SECMON1

Information Security Guideline

Security Overview

THIS PAGE INTENTIONALLY LEFT BLANK

This guide is an overview of security measures all organisations can do to best protect themselves from threats to the security of their business and customer information and systems. It contains a list of security mitigations that organisations can use to assist in securing their data to prevent data breaches and other events that could damage their organisation financially, operationally and reputationally. It is in no way a complete or exhaustive list, but includes some of the most important measures documented by the Australian Signals Directorate (ASD). They are ranked in an order from the most to the least important.

None of the below recommendations is an ultimate security solution in and of itself, but should be used in conjunction with other measures to take a defence-in-depth security stance.

A lot of these may be of limited value without the appropriate information security and acceptable use policies in place. This guide discusses the 'what' and 'why' of security measures recommended for organisations. For information on the 'how', please refer to the specific guide which provides information on implementing them. All guides are available at the SECMON1 blog page at www.secmon1.com.

Essential

Application Whitelisting

Application whitelisting restricts users from accessing any applications other than the ones explicitly allowed by your company's Acceptable Use Policy. This can include programs, software libraries, scripts and installers.

Application whitelisting can protect against code that is unauthorised (malicious or not) executing on a system regardless of where it was obtained (e.g., website download, email attachment, removable storage, etc).

Application whitelisting can be controlled by the vendor-provided security product your company chooses or has in place (e.g., firewall, access control solution, endpoint security solution), configuration settings and permissions controlling which directories a user and malware can write to and execute from. Some endpoint protection or anti-malware software solutions include application whitelisting functionality.

Note: Application whitelisting products may conflict with anti-malware software from a different vendor. Application whitelisting solutions are not meant to be a replacement for antivirus or other security software in place. Using multiple security solutions together is an effective defence-in-depth approach to mitigating system compromise.

The process of application whitelisting will be easier with detailed visibility of what software is installed on computers across the organisation. This can be accomplished by maintaining an inventory of software installed and implementing a robust change management process.

Potential User Resistance: Medium
Upfront Cost (Staff, Equipment, Technical Complexity): High
Ongoing Maintenance Cost (Mainly Staff): Medium

Patching Applications

Application patching is another way of referring to applying updates to applications, operating systems, and devices. It is absolutely critical for ensuring system security. Patching protects networks from consistently emerging vulnerabilities which enable adversaries to execute malicious code. Exploits for these vulnerabilities are so common that they can be bought and sold online.

Time is of the essence in patching. It is ideal to apply patches within 48 hours of release. When installing new applications, always use the latest version which is typically will include the latest patches. For some vendor applications, upgrading to the latest version is the only way to patch a security vulnerability.

Note: To maintain visibility of what software requires patching, keep a consistently up-to-date 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.

Potential User Resistance: Low
Upfront Cost (Staff, Equipment, Technical Complexity): High
Ongoing Maintenance Cost (Mainly Staff): High

Restrict Administrative Privileges

Restricting administrative privileges makes it difficult for an adversary to spread malicious code inside your network. Administrative accounts are the keys to the kingdom. If malicious code is activated using an administrative account, it can elevate its privileges, spread to other hosts, hide from detection, persist after reboot, obtain sensitive information and IP, and resist removal efforts.

Administrative privileges allow users 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 have low privileges instead. 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.

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

Potential User Resistance: Medium
Upfront Cost (Staff, Equipment, Technical Complexity): High
Ongoing Maintenance Cost (Mainly Staff): Medium

Patching Operating Systems

Operating system and firmware patches (also referred to as interim software upgrades) is critical to ensuring system security. It significantly reduces the risks from zero-day threats which take advantage of exploits to install malware into your networks.

Maintaining streamlined patch management strategy positions organisations to act quickly upon security bulletins or patch releases. This can dramatically reduce the time between noticing information on new security vulnerabilities, assessing them and applying patches or temporary workarounds where appropriate.

It is essential to patch security vulnerabilities as quickly as possible (within 48 hours is recommended). An exploit can be created within as little as a few hours of discovery.

Note: Always use the latest version of operating systems since they typically incorporate additional security technologies like anti-exploitation capabilities. Do NOT use operating system versions that are no longer vendor-supported with patches for security vulnerabilities.

Potential User Resistance: Low
Upfront Cost (Staff, Equipment, Technical Complexity): Medium
Ongoing Maintenance Cost (Mainly Staff): Medium

Disable Microsoft Office Macro Settings

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

Macros are embedded code written in the Visual Basic for Applications (VBA) programming language. They are easily-created tools that can greatly improve productivity. However, adversaries can also create and distribute macros that perform a variety of malicious activities. Out-of-date macros or macros downloaded from the Internet may contain vulnerabilities that

can be exploited and result in unauthorised access to sensitive information as part of a targeted cyber intrusion.

To manage the use of macros, 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 them in their IT environment.

Note: 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.

Potential User Resistance: Medium
Upfront Cost (Staff, Equipment, Technical Complexity): Medium
Ongoing Maintenance Cost (Mainly Staff): Medium

Harden User Applications

While useful for many business operations, applications like Flash, Java, Adobe Acrobat and certain features in Microsoft Office (e.g. OLE), can allow malware or intruders to enter your network. Disabling these applications and blocking online ads can remove any opportunity for adversaries to exploit these potentially disruptive tools. If your organisation uses these applications, you can restrict which users may access them.

Hardening user applications can significantly help 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. They can be blocked using web browser software and web content filtering at the gateway.

Note: 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.

Potential User Resistance: Medium
Upfront Cost (Staff, Equipment, Technical Complexity): Medium
Ongoing Maintenance Cost (Mainly Staff): Medium

Multi-Factor Authentication

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. It 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 (e.g., a physical token, smartcard or software-based certificate) or are (e.g., 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 an option. 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 network has been remotely compromised.

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

Potential User Resistance: Medium
Upfront Cost (Staff, Equipment, Technical Complexity): High
Ongoing Maintenance Cost (Mainly Staff): Medium

Daily Backups

Data is your most important digital asset. Protect it 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. Test as appropriate. Backups will contain undamaged copies of files.

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. Implement a backup strategy that minimises (or even eliminates) dependencies so that a version of files can be restored even if other versions have been encrypted, corrupted or deleted. Finally, ensure the organisation's incident response process identifies and restores all files that have been maliciously modified or deleted.

Note: Encourage users to avoid storing data on local storage media such as their computer's hard disk or USB storage, which is unlikely to be backed up. Instead, use corporate file servers and ASD certified cloud services.

Potential User Resistance: Low
Upfront Cost (Staff, Equipment, Technical Complexity): High
Ongoing Maintenance Cost (Mainly Staff): High

Excellent

Disable Local Administrator

The Administrator account (NT AUTHORITY\Administrator) exists by default on all Microsoft Windows (Windows NT-based) systems and Active Directory domains. It is typically used as a setup and disaster recovery account. Many organisations have standard build scripts that set a particular password for these accounts. As a result, all systems on the network will have the same Administrator password. This leads to significant problems should one of those systems become compromised.

If you must use the account, only use it during setup and to join the machine to the domain. After this, it should no longer be needed so should be disabled. If the account is needed for recovery or to boot into safe mode, the account will be automatically re-enabled for use only in troubleshooting. Once the system is booted again normally, it is disabled.

Conversely, you could assign passphrases that are random and unique for each computer's local administrator account. This would prevent propagation using shared local administrator credentials.

Potential User Resistance: Low
Upfront Cost (Staff, Equipment, Technical Complexity): Medium
Ongoing Maintenance Cost (Mainly Staff): Low

Protect Authentication Credentials

Protection of authentication credentials (e.g., network, local computer, e-mail, etc) is an excellent way to secure data.

This can be done be removing CPassword values (MS14-025), configuring WDigest (KB2871997), using Credential Guard (in Windows Defender), and changing default passphrases. Passphrase policies should be in place requiring long, complex passphrases as well as changing them at specified intervals. Some organisations require a yearly change whereas others require it every 90 days.

Note: NEVER leave passphrases out where they can be seen (e.g., sticky note on the monitor or under keyboard) and ideally don't store them in a file on your local machine. It is also a

good rule of thumb to not use passphrases across accounts (e.g., passphrase for your local e-mail is also the passphrase for logging into your organisation's network).

Potential User Resistance: Medium
Upfront Cost (Staff, Equipment, Technical Complexity): Medium
Ongoing Maintenance Cost (Mainly Staff): Low

Continuous Incident Detection and Response

Continuous incident detection and response, while reactive, can prevent further damage to an organisation's network and data.

Automated immediate analysis of centralised time-synchronised logs of permitted and denied computer events, authentication, file access, file movement and network activity is necessary for successful continuous incident detection and response. Vendor solutions are available to make this task quicker and more accurate. Manual review can be very time-consuming, subject to human error, and can mean the difference between one or two compromises and an organisation's entire network being compromised.

Potential User Resistance: Low
Upfront Cost (Staff, Equipment, Technical Complexity): Very High
Ongoing Maintenance Cost (Mainly Staff): Very High

Very Good

Server Application Hardening

Server application hardening mainly refers to securing of Web applications. Databases, as well as applications that access important (sensitive or high-availability) data are also included. The most important aspect of this is building security into the application in the first place as well as providing secure application development guidance for the organisation's developers. Programmers who are fluent in secure coding practices can avoid common security flaws in programming languages and follow best practices to help avoid the increasing number of targeted attacks that focus on application vulnerabilities.

Testing of existing applications should also be conducted to identify (and patch) any security vulnerabilities. Secure coding practices, in conjunction with pre-production and ongoing testing help to ensure applications are developed and maintained with a minimum exposure to known security vulnerabilities.

Developers should use the OWASP Top Ten list to guide their secure coding efforts. This list details the most common web application security vulnerabilities, including basic methods to protect against these vulnerabilities.

Applications, especially Internet-accessible Web applications need to sanitise input and use TLS not SSL.

Potential User Resistance: Low
Upfront Cost (Staff, Equipment, Technical Complexity): Medium
Ongoing Maintenance Cost (Mainly Staff): Medium

Operating System Hardening

Ideally, a system should serve a minimum amount of purposes. For example, a web server should not also function as a file server and/or workstation and/or domain controller. It should be a Web server, DNS or Exchange server, etc and nothing else. Typically, you won't harden a file and print server, a domain controller, or a workstation to this extent because those types of systems need too many functions to be properly hardened.

Generally, if a hardened system is what you need, Microsoft is not the place to look. It's much easier to harden a Linux or Unix system. Not only is there less work involved, but there is better documentation available on how to do it. Some exceptions to this, though, are if you are running a Check Point firewall on an NT-based system, the system will be as secure as its Unix counterpart. Vendors of these products tend to catch things a user might miss when hardening the systems on their own.

Some advantages of operating system hardening on a Windows server include having fewer patches to apply, you'll be less likely to be vulnerable to the average exploit, and you'll have fewer records to review in the logs. Attention can be focused on what the server is doing, not on the unnecessary services it may have running.

Important steps to hardening a Windows server include the following:

- Disable all unnecessary services: This can be more difficult than it seems as it needs to be determined which services can be disabled. Unfortunately, little documentation exists to identify which services are required for different purposes. Some examples of unnecessary functions are RDP, AutoRun, LanMan, SMB/NetBIOS, LLMNR and WPAD.
- Remove all unnecessary executables and registry entries: If this is not done, this may allow an adversary to invoke something that had previously been disabled
- Apply appropriately restrictive permissions to files, services, end points and registry entries: Inappropriate permissions could give an adversary an opening. For example, the ability to launch CMD.EXE as "LocalSystem" is a classic backdoor for attack.

Potential User Resistance: Medium

Upfront Cost (Staff, Equipment, Technical Complexity): Medium
Ongoing Maintenance Cost (Mainly Staff): Low

Antivirus

Antivirus software (AV), which is also referred to as anti-malware, is software that is used to prevent, detect and remove malicious software. While originally designed to detect and remove viruses, AV has evolved to provide protection from other computer threats like hijacks, ransomware, keyloggers, backdoors, rootkits, Trojans, worms, adware, and spyware. Some even go so far as to protect from infected and malicious websites, spam, phishing, social engineering, botnets, and advanced persistent threat (APT).

AV software that uses heuristics (dynamic behaviour-based detection) and reputation ratings to check a file's prevalence and digital signatures before execution is important. Using AV software from different vendors for gateways versus computers is another defence-in-depth strategy to employ.

Potential User Resistance: Low
Upfront Cost (Staff, Equipment, Technical Complexity): Low
Ongoing Maintenance Cost (Mainly Staff): Low

Control Removable Storage Media

Block any unapproved CD/DVD/USB storage media as well as connectivity with unapproved smartphones, tablet, and Bluetooth/Wi-Fi/3G/4G devices.

As there is often a business need to this type of connectivity, put a policy in place outlining use of these types of devices and institute an exception process. This means that only the people who have a business need for this functionality will be allowed to use it. This activity should also be monitored to prevent misuse of these exceptions (data leakage) as well as potential infections from malware that somehow may end up on the connected device.

Business approved removable storage media should be encrypted when possible. If the device itself is not an encrypted device, then at the minimum the data should be in the event the media is lost or stolen.

Potential User Resistance: High
Upfront Cost (Staff, Equipment, Technical Complexity): High
Ongoing Maintenance Cost (Mainly Staff): Medium

Software-Based Application Firewall

Software-based application firewalls (web application firewalls) filter, monitor, and block HTTP traffic to and from an application. They differ from a regular firewall in that they are able to filter the content of specific applications while regular firewalls serve as a safety gate between servers. By inspecting the HTTP traffic, it can prevent attacks stemming from application security flaws, such as SQL injection, cross-site scripting (XSS), file inclusion and security misconfigurations.

A software-based application firewall can serve a dual main purpose. It can block incoming network traffic that is malicious or unauthorised as well as deny network traffic by default (e.g., unneeded/unauthorised RDP and SMB/NetBIOS traffic. It can also block outgoing network traffic that is not generated by approved/trusted programs as well as deny network traffic by default.

Software-based application firewalls may come in the form of an appliance, server plugin, or filter. Customization of these may prove to be a significant effort and needs to be maintained as the application is modified.

Potential User Resistance: Medium
Upfront Cost (Staff, Equipment, Technical Complexity): Medium
Ongoing Maintenance Cost (Mainly Staff): Medium

Outbound Web and Email Data Loss Prevention

One potentially disastrous method of data loss can be through Web upload as well as email transfer and tends to be geared more toward the insider threat (can be malicious or non-malicious/inadvertent) as opposed to the external adversary.

To mitigate this vector, block unapproved cloud computing services. Log recipient, size and frequency of outbound emails. Block and log emails with sensitive words, classifications or data patterns. This activity should be continuously monitored and any concerns immediately addressed. There are a number of data loss prevention (DLP) vendor solutions out there to make this task less daunting. Generally, logs of this type can generate a lot of noise so it is helpful to have a solution in place that sifts through the noise for you and find the truly concerning activity.

Heuristics can also play an important role in this. By monitoring anomalous data movement, one can identify risky behaviour that might normally go unnoticed.

It is also important to make sure there are appropriate policies in place, as well as user awareness, to minimize this risk. Concerning activity can often be remediated through user education (reminding users of the policies).

Potential User Resistance: Medium
Upfront Cost (Staff, Equipment, Technical Complexity): Medium

Ongoing Maintenance Cost (Mainly Staff): Medium

Host-Based Intrusion Detection/Prevention

A Host-Based Intrusion Detection/Prevention System (or HIPS/HIDS) is a system or program used to protect critical computer systems containing crucial data against malware and active intrusions. They protect from and detect known and unknown malicious attacks by regularly checking the characteristics of a single host and the various events that typically occur for suspicious activities. A HIPS will take active measures to prevent compromise whereas a HIDS only detects and alerts on it.

They are used to identify anomalous behaviour during program execution (e.g., process injection, keystroke logging, driver loading and persistence). It monitors all or parts of the dynamic behaviour and the state of a computer system

Potential User Resistance: Low
Upfront Cost (Staff, Equipment, Technical Complexity): Medium
Ongoing Maintenance Cost (Mainly Staff): Medium

Endpoint Detection and Response

Endpoint Detection and Response (EDR) is an emerging technology. It focuses on detecting, investigating, and mitigating suspicious activities and issues on hosts and endpoints.

Advanced persistent threats (APTs) and customized targeted malware attack toolkits have the ability to bypass traditional signature-based antivirus solutions. EDR supplements signature-based technologies with richer behaviour-based anomaly detection and visibility across endpoints. They provide greater visibility into endpoint data that's relevant for detecting and mitigating advanced threats, limiting sensitive data loss, and reducing the risk of data breaches that can occur on endpoints.

Placing endpoint detection and response software on all computers will assist with centrally logging system behaviour and facilitate incident response. Microsoft's free SysMon tool is an entry-level option.

Potential User Resistance: Low
Upfront Cost (Staff, Equipment, Technical Complexity): Medium
Ongoing Maintenance Cost (Mainly Staff): Medium

Business Continuity and Disaster Recovery

Business continuity and disaster recovery planning are processes that help organisations prepare for disruptive events (e.g., hurricane, fire, power outages, etc). Disaster recovery is the process by which an organisation can resume business after a disruptive event. Business continuity suggests a more comprehensive approach to making sure an organisation can keep making money, not just after a disruptive event but also in the event of smaller disruptions (e.g., illness or departure of key staff, supply chain partner problems, etc).

It is important for organisations to have business continuity and disaster recovery plans in place which are tested, documented and printed in hardcopy with a softcopy stored offline. The highest priority systems and data should be the focus for recovery.

Potential User Resistance: Low
Upfront Cost (Staff, Equipment, Technical Complexity): High
Ongoing Maintenance Cost (Mainly Staff): Medium

System Recovery Capabilities

Virtualisation with snapshot backups, remotely installing operating systems and applications on computers, approved enterprise mobility, and onsite vendor support contracts are just a few examples of system recovery capabilities.

Virtualisation with snapshot backups are copies of a virtual machine's disk file and are used to restore a virtual machine (VM) to a particular point in time before a failure or system error occurred. They provide a method of backup. Any data that was writable on a VM becomes read-only when a snapshot is taken. When a VM reverts to a snapshot, current disk and memory states are deleted and the snapshot becomes the new state for that VM.

Remote install of an operating system uses pre-boot state of operating system or application and eliminates the need for a technician to be physically present on site for install. This can assist with organisations that have locations scattered across the country or even globe.

Enterprise mobility is the trend toward a shift in work habits, with more employees working out of the office and using mobile devices and cloud services to perform business tasks. This not only refers to mobile workers and devices, but also the mobility of corporate data. An employee may upload a corporate presentation from their PC to an approved cloud storage service, then access it from an iPad to show at a client site. While this can improve employee productivity, it can also create security risks. Enterprise mobility management products (e.g., data loss prevention technologies) and strong Acceptable Use Policies can contribute to successful implementation of enterprise mobility.

Vendor support contracts (with clearly defined SLA times) can aid in the timeliness of system recovery. The vendor would possess the best knowledge around how to repair a failure and get the product back to an optimum operating level.

Potential User Resistance: Low
Upfront Cost (Staff, Equipment, Technical Complexity): High
Ongoing Maintenance Cost (Mainly Staff): Medium

Personnel Management

Ongoing vetting especially for users with privileged access, immediately disabling all accounts of departing users, and reminding users of their security obligations and penalties are some examples of personnel management.

It is important for an organisation to justifiably be able to trust their employees in general, but especially those employees charged with access to and protection of privileged data, systems, and intellectual property. While most organisations conduct pre-employment screening, that is where it ends. Employees going into a role may have no malicious intentions when they start, but their loyalties could evolve over time. At the very least, employees moving from a low-risk role into a high-risk (or higher-risk) role should be re-screened.

Disabling all accounts and access of departing employee is also necessary whether they are leaving on amicable terms or not. This closes any potential risk of unauthorised access to sensitive data or systems by employees who are no longer with that organisation.

Yearly and ad hoc reminders to employees of their security obligations and penalties helps to reinforce security and acceptable use policies in place. Yearly reminders can consist of awareness training and sign-off. Ad hoc reminders can consist of periodic email reminders/tips sent to all employees as well as in response to minor violations that prove to be more of an education opportunity than resulting from malicious intent.

Potential User Resistance: High
Upfront Cost (Staff, Equipment, Technical Complexity): High
Ongoing Maintenance Cost (Mainly Staff): High

Good

User Education

User education aids an organisation in informing its employees of what they need to do or be aware of to protect the organisation and its data. This can consist of training and reminders around security and acceptable use policies, emails offering tips on how to keep their systems and data secure and avoid malware and phishing emails, tips on creating a strong passphrase as well as how often to change and not to reuse them, and unapproved removable storage media, devices and cloud services.

Potential User Resistance: Medium

Upfront Cost (Staff, Equipment, Technical Complexity): High
Ongoing Maintenance Cost (Mainly Staff): Medium

Limited

Antivirus Software with Up-to-Date Signatures

These should be used in conjunction with Antivirus software that utilises heuristics to identify malware-related threats. Signature-based AV needs to come from a vendor that rapidly adds signatures for new malware. Different AV software should be used for gateways versus computers and as part of a defence-in-depth strategy.

Potential User Resistance: Low
Upfront Cost (Staff, Equipment, Technical Complexity): Low
Ongoing Maintenance Cost (Mainly Staff): Low