ITSEC™

SECURITY DELIVERED

A Guide To

'ESSENTIAL EIGHT' CYBERSECURITY CONTROLS

A SOLID FOUNDATION OF SECURITY

Essential Reading for CEO's, CISO's, COO's, CIO's and CFO's.

ITSEC Australia | ITSEC.com.au | +61 1800 512 191 |info@itsec.com.au

ABOUT

Essential Eight

In organisations across Australia, IT and information security teams are implementing proactive cybersecurity measures in order to reduce their exposure to cyber risks. By taking a proactive, rather than a reactive, stance your organisation can mitigate against the vast majority of common cyberattack, simply by removing the most common threat vectors. Common sense dictates that trying to deal with a cybersecurity problem when it happens tends to be far more expensive than proactively mitigating against the problem before it can occur.

With this in mind, the Australian Signals Directorate (ASD) has created a new cybersecurity baseline titled 'The Strategies To Mitigate Cybersecurity Incidents' which has been nicknamed The Essential Eight. The baseline is designed to help organisations reduce their exposure to cyber risk in a proactive way and the essential eight are the elements which underpin their list and which have the biggest impact for the least investment. More than anything, the essential eight represents good security habits and helps your business protect yourself against a wide range of attack vectors. These guidelines should be used as a security baseline which you should then adapt to your own business's needs. Some of these guidelines are technical in nature, whereas others are geared towards operational guidance, let's outline each of these in more detail so that we can get a better understanding of them individually:

The Essential Eight

The Essential Eight is divided into three main objectives which are then further divided into eight essential strategies for ensuring that these objectives are implemented effectively.

- Preventing malware attacks
- Limiting the extent of cybersecurity incidents
- Recovering data and system availability

Let's break these objectives down into the eight strategies and take a look at them in more detail so that we can better understand them and get to grips with their goals:

Application Whitelisting -
When you whitelist an application you only allow 'trusted' applications to run on your network which stops malware and untrusted software from doing damage to your IT infrastructure. ITSEC can help by running an audit on the applications your business uses so that you can black/white list them, any applications which should not be running on your networks can easily be disabled and blacklisted.

Patch Your Applications -
Patching means making sure that your applications are up to date with the latest releases so that they do not contain any known security vulnerabilities and this is the simplest way to ensure good cybersecurity for your IT infrastructure. You should patch applications every time their vendor releases a new update and these updates provide you with essential security features, meaning they should be installed in a timely manner. ITSEC can help you in this regard by helping you identify unpatched applications in your IT infrastructure so that you can prioritise the systems where there is a risk.

Disable Macros -
Microsoft Office documents can be full of macros and while automating your tasks can be good for productivity, macros can contain malicious automation or malware which can mean unauthorised access to data or that your data could be manipulated in some way. You need to restrict the use of macros and only trust signed macros that you trust, it is also good practice to routinely audit your macros to work out if they are still needed.

User Application Hardening -
If you allow web browsing in your IT infrastructure then you expose yourself to malicious webpages, emails with malicious attachments and bad advertisements which could infect your machine (malvertising). If you harden your user's web browser or give them a remote browser to isolate their browsing activity away from your IT infrastructure, you can help reduce the risks associated with web browsing. You should also disable flash and java applications in the browser and any browser plugins that you do not trust, implementing an adblocker solution in your web browsers is also a good practice.

Restrict Admin Privileges -

When you conduct an account audit, you may find that you have administrator accounts which enable too much access or privileges that can then be used to install untrusted software, make system changes or bypass security settings. In general, administrator privileges should be restricted to the users who actually need them and admin accounts should be used to manage systems when installing trusted software or patching operating systems and applications. It is best practice to regularly audit your admin accounts and their rights and privileges, it is also best practice to put into place account security controls for employee changes, either when someone leaves or a new person starts.

Multi-Factor Authentication (MFA) -

Multi-factor authentication is a security mechanism that requires a user to provide two or more credentials in order to authenticate their identity and can prevent an attacker from compromising your systems even if they have the password. With MFA each user must provide multiple and separate pieces of information in order to verify their identity to the system before they are allowed to log in. This information typically consists of something you know like your password or PIN, something you have like an SMS code sent to your mobile, or even something you are like biometric data such as your fingerprint. MFA is the single most important measure for stopping unauthorised access to your systems.

Backup Your Data -

Because ransomware is so prevalent and because the only way to recover from ransomware (without paying the ransom) is to recover your data from backups, it is essential that you back up your critical data on a daily basis and store that data offline to ensure that your business can recover if you are ever attacked by ransomware. Backups can also save your skin with other kinds of cybersecurity incidents too and enable you to restore lost data. Just make sure that your backups have integrity, meaning that you can properly restore the data if you should ever need to, we often see situations where backups are kept but corrupt or incomplete making it much more difficult to restore any lost data in an emergency.

ABOU

The Philosophy Behind Essential Eight

This list of the essential eight security practices that you should be following is not meant to be a checklist, it is a cybersecurity philosophy that you need to implement and maintain in order to maintain the cybersecurity of your IT infrastructure and protect your businesses from the most common kinds of cyber threats. If you can follow each of these eight essential steps then you create a fantastic foundation upon which you can build a more robust cybersecurity defence for your organisation. ITSEC can help you accomplish and achieve compliance with these essential eight steps, practice good cybersecurity and manage your cybersecurity in order to help you reduce your businesses attack surface and minimize the chance of your business being disrupted by a crippling cyberattack against it by organized cyber criminals.

Achieving Essential Eight Maturity - ITSEC can help your business work out the maturity of your cybersecurity approach based on three maturity levels which have been clearly defined for the essential eight strategies we discussed above. These levels are defined as:

1. Partly aligned with the intent of the essential eight.
2. Mostly aligned with the intent of the essential eight.
3. Fully aligned with the intent of the essential eight.

If your organization finds itself in the category of maturity level one or two, then ITSEC can certainly help you mature your cybersecurity to the point where you can achieve a level three maturity in your cybersecurity posture. The good news is that achieving this level is not an arduous task and once achieved sets a fantastic baseline upon which we can build more robust cybersecurity controls. If all you do is achieve the essential eight then your business is ahead of most in terms of its cybersecurity and ITSEC can help you get there.

If you have any questions at all about any aspect of your cybersecurity or the Essential Eight, get in touch with us for a conversation today by calling us on +61 1800 512 191.