Essential Eight - Cyber Security Solution

Protect your business from known & emerging Cyber Security threats

Cyber threats are constantly evolving and becoming more complex.
The traditional approach of relying on antivirus software and firewalls is no longer enough to protect against these threats.

The Essential 8 security framework, developed by the Australian Signals Directorate (ASD), provides a more comprehensive approach, which focuses on eight key mitigation strategies.

Application control

To control the execution of unauthorised applications / software

Patching applications

To remediate known security vulnerabilities

Configure Microsoft Macro Settings

To block untrusted macros and only allow checked macros from trusted locations

User application hardening

Configure web browsers to block and disable potential malware

Restrict Admin privileges

To limit powerful access to important business information and systems

Patch Operating Systems

To remediate known security vulnerabilities

Multi-Factor Authentication

To protect against unauthorised access

Daily Backups

To maintain the availability of critical business data

The Essential 8 security framework provides a comprehensive set of mitigation strategies that have been proven to effectively defend against advanced persistent threat (APT) actors. By adopting these strategies, organisations can protect themselves from cyber threats and ensure the security of their sensitive information.

Essential Eight Features

1. Application Control

This strategy ensures that only approved applications are allowed to run on an organisation's systems. This reduces the risk of malware and other malicious software infecting systems and programs.

2. Patching Applications

This strategy ensures that all applications are kept up-to-date with the latest security patches to prevent attackers from exploiting known vulnerabilities.

3. Configure Microsoft Macro Settings

This strategy helps to prevent macro-based malware attacks by configuring Microsoft Office to disable macros from untrusted sources.

4. User Application Hardening

This strategy involves configuring user applications to reduce their attack surface and make them more secure.

5. Restrict Admin Privileges

This strategy involves restricting administrative privileges to only those who need them, reducing the risk of attackers using these privileges to compromise systems and steal sensitive information.

6. Patch Operating Systems

This strategy ensures that all operating systems are kept up-to-date with the latest security patches to prevent attackers from exploiting known vulnerabilities.

7. Multi-Factor Authentication

This strategy involves applying security controls to operating systems to prevent attackers from compromising systems and stealing sensitive information.

8. Daily Backups

This strategy helps to maintain the availability of critical business data.

Benefits

- **Heightened data security**
- **Reduced risk of human error**
- **Increase operational control**
- **Cost savings due to reduced risk**
- **Improved productivity & efficiency**

Want to learn more about New Era's Cyber Security Solutions?

Visit our website: https://www.neweratech.com/au/cybersecurity