THE ESSENTIAL EIGHT

Strategies to Mitigate Cyber Security Incidents

This concerns all businesses

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.

Essential Eight is spilt into three categories

- Mitigation Strategies to Prevent Malware Delivery and Execution
  To prevent the execution of unwanted applications, patch /mitigate computers with high-risk vulnerabilities, block unvetted macro's and disable unneeded features
- Mitigation Strategies to Limit the Extent of Cyber Security Incidents
  Restrict administrative privileges, know the benefit of using up to date operating systems and making it harder for adversaries to gain access
- Mitigation Strategies to Recover Data and System Availability
  Ensure data and business recovery after a cyber security incident

Suspect your current I.T. is holding you back?

Get in contact with us to review your options.

02 4337 0700

PROFESSIONAL.
RELIABLE.
LOYAL.

THE ESSENTIAL EIGHT

Strategies to Mitigate Cyber Security Incidents

Prevent, limit and recover

While no single mitigation strategy is guaranteed to prevent cyber security incidents, organisations are recommended to implement these eight mitigation strategies as a baseline. This baseline 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.

MITIGATION STRATEGIES TO PREVENT MALWARE DELIVERY AND EXECUTION

Application control

Why: All non-approved applications(including malicious code) are prevented from executing.

Patch applications

Why: Security vulnerabilities in applications can be used to executemalicious code on systems.

Configure Microsoft Office macro settings

Why: Microsoft Office macros can be used to deliver and execute malicious code on systems.

User application hardening.

Why: Flash, ads and Java are popular ways to deliver and executemalicious code on systems.

MITIGATION STRATEGIES TO LIMIT THE EXTENT OF CYBER SECURITY INCIDENTS

Restrict administrative privileges

Why: Admin accounts are the 'keys to the kingdom'. Adversaries use these accounts to gainfull access to information and systems.

Patch operating systems

Why: Security vulnerabilities in operating systems can be used to further the compromise of systems.

Multi-factor authentication

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

Why: To ensure information can be accessed following a cyber security incident (e.g. a ransomware incident).

LEARN MORE

Go to the Cyber Security Business Connect and Protect portal **www.loyalit.com.au/cybersecurity**

and see our videos, Q&A sessions and podcasts on this and other topics.

LOYAL
I.T. SOLUTIONS

PROFESSIONAL. RELIABLE. LOYAL.

02 4337 0700 | www.loyalit.com.au 370 Mann Street North Gosford NSW 2250