Daily Backups

Ensure important information such as new/changed data, software and configuration settings can be accessed following a cyber security incident (e.g. a ransomware incident).

20% of small to medium sized businesses will suffer a major disaster causing loss of critical data every 5 years

93% of companies that lost their data for 10 days or more filed for bankruptcy within one year of the disaster, and 50% filed for bankruptcy immediately

20% of all small businesses will be hacked within one year

Multi-factor Authentication

Stronger user authentication, including for VPNs, RDP, SSH and other remote access, and for all users when they perform a privileged action or access an important/sensitive data repository, makes it harder for adversaries to access sensitive information and systems.

81% of breaches are due to weak or stolen passwords such as common phrases or repeated words/numbers.

Phishing emails are successful nearly half of the times they are carried out.

An average employee has to remember approximately 27 passwords.

Redpoint
Cybersecurity LLC

ESSENTIAL EIGHT

Of all the attacks organizations experience, 99.9% of those exploiting a known vulnerability occur more than a year after the publishing of the associated CVE (Common Vulnerabilities and Exposures).

In 2019, 34% of data breaches involved internal actors.

Admin accounts are the ‘keys to the kingdom’. Adversaries use these accounts to gain full access to information and systems. Privileges to operating systems and applications should be restricted based on user duties and regularly revalidated based on the need for privileges.

Restrict Admin Privileges

57% of data breaches are attributed to poor patch management.

80% of companies who had a data breach or failed audit could have prevented it with patching or configuration updates.

20% of all vulnerabilities caused by unpatched software are classified as High Risk or Critical.

Vulnerabilities in operating systems can be used to further the compromise of systems. Patch/mitigate computers (including network devices) with 'extreme risk' vulnerabilities within 48 hours, use the latest OS, and do not use unsupported versions.

Patch Operating Systems

Application Control

To prevent the execution of malicious programs (including .exe, DLL, scripts) and installers, all unapproved applications are prevented from executing.

Whitelisting application allows protection against ransomware and other types of malware attacks. Traditional antivirus software tends to be signature-based. Whitelisting also helps decrease help desk costs, giving IT staff the ability to make sure that users are running application versions that are known to be stable and reliable.

The top malicious email attachment types are .doc and .dot which make up 37%. The next highest is .exe at 19.5%.

Patch Applications

Security vulnerabilities in applications (e.g. Flash, web browsers, Microsoft Office, Java) can be used to execute malicious code on systems.

92% of web applications with security flaws or weaknesses that can be exploited

82% of employers report a shortage of cybersecurity skills, and 71% believe this talent gap causes direct and measurable damage to their organizations

18% of all network-level vulnerabilities are caused by unpatched applications

Redpoint Cybersecurity LLC

ESSENTIAL EIGHT

Despite periodic lulls, infections for the top 20 most detected macro-based malware were high over the past three months.

In the enterprise, recent data from our Office 365 Advanced Threat Protection service indicates 98% of Office-targeted threats use macros.

Macros can be used to deliver and execute malicious code on systems. The right settings can block macros from the internet and only allow vetted macros in 'trusted locations' with limited access or trusted certificates.

Configure Microsoft Office Macro Settings

Nearly 90% of usage on mobile phones and tablets occurs through apps. The prevalence of the Internet of Things and increasing use of personal devices in vulnerable sectors have made the need for application hardening urgent.

61% of organizations have experienced an IoT security incident, with IoT devices experiencing an average of 5,200 attacks per month.

Flash, ads and Java are popular ways to deliver and execute malicious code on systems. Web browsers can be configured to block or uninstall all three, and unnecessary features (e.g. OLE and PDF viewers) can be disabled.

User Application Hardening