Computer Security Notes

Found at: benjaminshaw.uk

1 Basics

1.1 A Definition of Security

Confidentiality

Ensure that assets are accessed only by authorised parties.

Integrity

Assets can only be modified by authorised parties, or by authorised means.

Availability

Assets are only accessible to authorised parties at the appropriate times.

Accountability

Actions are traceable to those responsible

Authentication

User/data origin accurately identifiable

1.2 Security Countermeasures

Prevention

Stop security breaches via system design and defences

Detection

If a breach does occur, detect it.

Response

A plan utilised when a breach is detected.

1.3 Denial of Availability

A user will expect that services be available to them. A common attack is denying users this privilege. Denial of Service (DOS) attacks or malware are two common ways of attacking availability.

2 Cyber Security Essentials

2.1 Secure Configuration

Principles:

Devices on a network should be configured such that they minimise the number of inherent vulnerabilities.

Default settings can *often* be insecure, which includes default passwords.

Actions:

- Remove unnecessary user accounts, such as the *Admin* account found on Windows XP installs.
- Changing the default password
- Removal of unnecessary software
- Firewall software should regulate the incoming/outgoing connections on a device

2.2 Boundary Firewalls & Internet Gateways

Principles:

Devices should be protected against unauthorised access and disclosure.

Firewalls are the first line of defence and can stop attacks before they even reach the network.

Actions:

- Change default passwords
- Rules should be scrutinised before they are applied
- Unapproved services should be blocked by a rule
- Obsolete rules should be purged
- Firewall administration tools should not be accessible from outwith the network

2.3 Access Control and Privilege Management

Principles:

User accounts should have the minimum amount of privileges, with extended privileges awarded upon authorisation.

A compromised account with high levels of access can lead to a lot of damage.

Actions:

- Account creation should be subjected to an approval process
- Administration accounts should only be used for legitimate administration purposes and not activities that can be achieved with a standard account
- Elevated privilege accounts should require password changes periodically
- Users should be authenticated before being granted access to devices and applications
- Elevated accounts should be used when no longer required

2.4 Patch Management

Principles:

Remove unnecessary vulnerabilities by keeping software up-to-date.

Actions:

- Software should be kept up-to-date and fully licenced
- Out-of-date software removed
- Updates when made available should be installed in a timely manner

2.5 Malware Protection

Principles:

Internet-facing devices should make use of malware protection software that continuously monitor for known-malware instances.

Actions:

- Install anti-malware software
- Keep said software up-to-date
- Regularly scan all files
- Prevent connections to known malicious website