**Module 2 Technologies & Tools**

**2.3 Security Troubleshooting**

**Asset Management**

* Asset inventory step #1 for both NIST & CIS controls
* You can’t secure something you don’t know
* Use automated tools to maintain asset list
* Issue – assets lost/stolen

1. Mobile computers (Laptops, tablets, smartphones)
2. Removable storage media (USB drives)

* Includes software management – employees installing apps they shouldn’t

**Access Violations**

* People – occur when someone accesses/attempts to access data they shouldn’t be accessing

1. Insiders or external attackers

* Separation of duties
* Systems – system calls/automated access
* Solution – auditing, reporting & response

**Permission Issues**

* Least privilege violations
* Privilege creep – employee adding permissions over time
* Inherited permissions allowing access – files & folders, groups
* Write & execute allowed instead of read-only
* Other side – insufficient permissions
* Solution – auditing, reporting & response

**Authentication Issues**

* Common authentication issues

1. Incorrect username & password
2. Expired password
3. Disabled/deleted account
4. Restricted user rights
5. Authentication server unavailable/visible
6. TFA (2 Factor Authentication)/MFA (Multi-Factor Authentication) not enabled
7. Users choosing poor passwords

* Solutions

1. Account verification
2. Check connectivity
3. Review logs
4. User education

**Unencrypted Credentials/Clear Text**

* Password rules not enforced
* Systems configuration – app/service stores/sends clear text password
* People storing clear text passwords

1. Online – spreadsheet, document or database
2. Offline – writing it down

* User types password into User ID field
* Solutions

1. Automated password policies
2. Proper system configuration/application development
3. Use of password vaults
4. User education

**Certificate Issues**

* Certificate warnings (Eg. “There’s a problem with this website’s security certificate”)
* Causes

1. Date/time not set correctly
2. Expired certificates
3. Certificate revoked

* Use of SSL instead of TLS on web server
* Self-signed certificates

**Data Exfiltration**

* Unauthorised transfer of storage/data

1. Malicious/data theft
2. Unintentional (use of personal storage)

* Solution – Data Loss Prevention (DLP)

**Security Configuration**

* Misconfigured devices/weak security configurations
* Not enabling security features (OS, devices, apps etc.)
* Firewall rules

1. Old rules
2. Ordering of rules
3. Not deny by default

* Default passwords
* Missing updates/patches
* Baselines established by government mandate, regulatory bodies or industry requirements

1. PCI & HIPAA

* Issues

1. Configuration management not in place
2. Exceptions (system & people)

**Baseline Deviation**

* Normalisation establishes known baselines – system/network activity
* OS images
* Issues

1. Baseline not established
2. Baseline corrupted
3. Out of date (due to patches)

* Dynamic baselining more effective than static baselining

**Application Issues**

* Unauthorised software – users can install apps on end-point devices
* License compliance version – Business Software Alliance (BSA) fines
* Solutions

1. Implement policy for software acquisitions
2. Read all license agreements
3. Maintain inventory list
4. Audit for compliance

**Logs & Events Anomalies**

* Process of collecting data for monitoring & auditing purposes
* Logging standards for platforms, apps & servers
* Balancing too much & too little
* Log monitoring
* Solution

1. Centralised logging
2. Use of SIEM (Security Information & Event Management)
3. SOC (Security Operations Centre)

**Personnel Issues**

* Policy violation
* Insider threat
* Social engineering
* Social media
* Personal email
* Solutions

1. Policies
2. Security Awareness Training