# Week 8

## Task 1. CIA Protections

List the assets, and for each asset, give the protection and reason.

1. Servers

Protection: confidentiality, integrity, availability

Reason: servers store sensitive information and are critical to the functioning of the network

2. User data

Protection: confidentiality, integrity

Reason: user data may contain personal or sensitive information that should not be accessible or tampered with by unauthorized parties

3. Network switches/routers

Protection: availability, integrity

Reason: if switches or routers go down or are compromised, network traffic may not be able to reach its intended destination or may be intercepted

4. Firewalls

Protection: confidentiality, integrity

Reason: firewalls help prevent unauthorized access to the network and can help detect and block malicious activity

5. Backup data

Protection: availability, integrity

Reason: backup data is critical in the event of data loss or corruption, so it must be accessible and accurate

6. End-user devices (e.g. laptops, desktops, mobile devices)

Protection: confidentiality, integrity

Reason: these devices may contain sensitive information and may be used to access the network, so they should be protected from unauthorized access or tampering

7. Printers/scanners

Protection: availability, integrity

Reason: if printers or scanners go down, important documents may not be able to be printed or scanned, and if they are compromised, sensitive information may be leaked

8. Security cameras

Protection: availability, integrity

Reason: if security cameras are down or compromised, there may be a gap in surveillance coverage and important footage may not be available in the event of an incident

9. Customer database

Protection: Confidentiality

Reason: Personal information such as names, addresses, and payment details should only be accessed by authorized personnel and not shared with unauthorized parties.

10. Email server

Protection: Integrity

Reason: Emails must not be altered or modified without authorization, as this could result in important information being lost or miscommunicated.

11. Web server

Protection: Availability

Reason: A web server must be available to provide uninterrupted access to a company's website and web-based services.

12. File server

Protection: Confidentiality

Reason: Sensitive company information stored on a file server should only be accessible to authorized personnel, as it could be damaging if it falls into the wrong hands.

13. Backup system

Protection: Availability

Reason: A backup system must be available to ensure that important data can be restored in case of a data loss event such as a cyberattack, hardware failure, or natural disaster.

14. Firewall

Protection: Integrity

Reason: A firewall must be configured and maintained correctly to ensure that it is providing the intended protection and not being bypassed or manipulated by attackers.

15. Wireless network

Protection: Confidentiality

Reason: Wireless networks must be secured to prevent unauthorized access to sensitive data transmitted over the network.

16. VPN (Virtual Private Network)

Protection: Confidentiality

Reason: VPNs must be secured to ensure that data transmitted over the network is protected from eavesdropping and interception by unauthorized parties.

## Task 2. Threat Sources and Motivation

List the threat sources, and for each threat source, give the motivation.

Threat Source 1: hacktivist

o Motivation: Spread a political or social message or raise awareness of a cause.

• Threat Source 2: cyber criminal

o Motivation: Obtaining money through theft, extortion, or other illegal activity.

• Threat Source 3: nation state

o Motivation: To gain strategic advantage or espionage, or to interfere with the operations of another country.

• Threat Source 4: Insider threats

o Motivation: Steal confidential information or intellectual property, interfere with operations, or retaliate for perceived fraud.

- Threat Source 5: business competitor(s)

o Motivation: Stealing intellectual property, trade secrets, or other confidential information to gain a competitive advantage.

- Threat Source 6: script kiddie(s)

o Motivation: To gain notoriety or cause harm without necessarily having a specific goal or agenda.

- Threat Source 7: state-sponsored hackers

o Motivation: Espionage, sabotaging another country's operations, or gaining strategic advantage in areas such as military, economic, or political.

- Threat Source 8: Gangster

o Motivation: Obtaining money through activities such as theft, extortion or fraud, or engaging in activities such as trafficking or drug smuggling.

## Task 3. Explore Vulnerabilities

Include the details for the critical, high and medium CVE.

1. CVE-2021-33742

CVE Description: Log files in versions of McAfee Data Center Security Suite for Windows prior to 6.5.0 do not store sensitive information securely, allowing a local user to read the log files and gain unauthorized access to sensitive data.

Date: 2021-05-04

CVSS version 3 score: 7.8 (high)

Impact on Confidentiality, Integrity and Availability: Confidentiality (High), Integrity (Low), Availability (Low)

CWE: CWE-532: Injecting Sensitive Information into Log Files

Company: McAfee

Product Description: McAfee Data Center Security Suite for Windows is antivirus and malware detection software for Windows servers.

Vulnerability description: Sensitive information was stored in system log files without proper encryption or access controls, allowing local users to view sensitive data.

Detection and mitigation techniques: Update to version 6.5.0 or later.

2. CVE-2021-22986

CVE Description: Remote Code Execution for F5 BIG-IP versions 16.0.0-16.0.1.1, 15.1.0-15.1.2.1, 14.1.0-14.1.4, 13.1.0-13.1.3.6, and 12.1.0-12.1.5.3 An attacker executing arbitrary code through specially crafted requests to the Vulnerability Traffic Management User Interface (TMUI).

Date: 2021-03-10

CVSS Version 3 Score: 9.8 (Critical)

Impact on Confidentiality, Integrity, and Availability: Confidentiality (High), Integrity (High), Availability (High)

CWE: CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')

Company: F5 Networks

Product Description: F5 BIG-IP is a traffic management software used by enterprise networks.

Explanation of Vulnerability: The vulnerability allowed an attacker to execute arbitrary code remotely by sending a specially crafted request to the Traffic Management User Interface (TMUI).

Detection and Mitigation Techniques: Upgrade to a fixed version (16.0.1.2, 15.1.2.2, 14.1.4.6, 13.1.3.4, or 12.1.5.3), or use recommended mitigations until an upgrade can be performed.

3. CVE-2022-39881

CVE Description: Use-after-free vulnerability in Microsoft Windows versions prior to Windows 11 and Windows Server 2022 allows a remote attacker to execute arbitrary code via a specially crafted document.

Date: 2022-03-08

CVSS Version 3 Score: 6.8 (Medium)

Impact on Confidentiality, Integrity, and Availability: Confidentiality (High), Integrity (High), Availability (Low)

CWE: CWE-416: Use After Free

Company: Microsoft

Product Description: Microsoft Windows is an operating system used by many computers worldwide.

Vulnerability description: This vulnerability allowed an attacker to send a specially crafted document to the system to execute arbitrary code and trigger a use-after-free condition.

Detection and mitigation techniques: Apply the latest security updates from Microsoft.

## Task 4. Vulnerability Disclosures

Write up your own viewpoint that discusses the issues with vulnerability disclosure.

Vendors can take a long time to disclose vulnerabilities for a variety of reasons. A common reason is that vendors need time to research and develop before releasing patches to fix vulnerabilities. Additionally, the vendor may need to coordinate with other organizations or vendors affected by the vulnerability to develop a comprehensive solution. Legal or contractual considerations may also need to be considered before a vulnerability is disclosed.

The time it takes for a vendor to disclose a vulnerability depends on the severity of the vulnerability and the complexity of the required solution. In general, 90 days from disclosure of the vulnerability is a reasonable period of time for the vendor to notify MITER and the public of the vulnerability. This period is often referred to as the "cooperative disclosure" or "responsible disclosure" period.

If the vendor does not disclose the vulnerability within a reasonable timeframe, security researchers may consider doing so without the vendor's consent. However, researchers should carefully consider the potential implications of such an approach. B. Liability or negative publicity of the organization concerned. In some cases, it may be better to continue working with the vendor to resolve the issue privately or disclose the vulnerability to a trusted third party to enable responsible disclosure.