Week 1 revision notes

IFB240 Cyber Security - Comprehensive Revision Notes

Overview

These notes are designed to help understand key concepts in Cyber Security, focusing on definitions, real-world examples, and how to apply the knowledge effectively. These are ideal for someone who missed classes or needs a deeper understanding of the material.

1. Introduction to Cyber Security

Definition

- **Cyber Security** involves measures to protect systems, networks, and data from cyber threats. It ensures the **Confidentiality**, **Integrity**, and **Availability** (CIA) of information and systems.
- These concepts are critical for protecting data from unauthorised access and ensuring systems function reliably.

Why It Matters

- **Example**: The **QUT Ransomware Attack (Dec 2022)** disrupted university operations, affecting both the data (compromising **confidentiality**) and systems (affecting **availability**). This was an example of both a **cyber security** and an **information security** incident 25.

2. Information Security

Definition

- **Information Security** focuses on safeguarding **information assets** from unauthorised access, use, disclosure, modification, or destruction. It ensures data integrity and confidentiality.

Difference from Cyber Security

- **Information Security** protects the information itself, regardless of format (digital or physical).
- **Cyber Security** protects the systems and infrastructure that store, process, or transmit information.

Real-World Example

- **Red Cross Data Breach (2016)**:

- Sensitive personal information was leaked, leading to a **confidentiality** breach. This incident highlighted the importance of protecting personal data against unauthorized access 25.

3. Threats, Vulnerabilities, and Attacks

Key Definitions

- **Threat**: A potential cause of harm to an asset. For example, natural disasters, hackers, or internal bad actors.
- **Vulnerability**: A weakness in the system that can be exploited by threats, such as outdated software or weak passwords.
- **Attack**: A deliberate action that exploits a vulnerability, resulting in harm.

Example: Laptop Theft

- **Threat**: Theft of the laptop.
- **Vulnerability**: Poor physical security (e.g., an unlocked window).
- **Impact**: Compromises **availability** (loss of asset) and potentially **confidentiality** if sensitive information is accessed 24.

4. The CIA Triad (Security Goals)

Confidentiality

- **Definition**: Ensuring information is not disclosed to unauthorised individuals, entities, or processes.
- **Example**: The **Red Cross breach** compromised confidentiality as sensitive data was exposed to unauthorised parties 25.

Integrity

- **Definition**: Ensuring that information is accurate and cannot be modified without authorisation.
- **Example**: When attackers modify data in a phishing scam, it compromises **integrity**.

Availability

- **Definition**: Ensuring information and systems are accessible when needed by authorised users.
- **Example**: The **Optus Outage (2023)** disrupted services for 10 million Australians, severely impacting **availability** of communication services 25.

5. Additional Security Goals

Authentication

- **Definition**: Verifying the identity of a person or system before allowing access.

- **Example**: Authentication checks prevent unauthorised users from accessing systems, helping maintain **confidentiality** and **integrity**.

Non-repudiation

- **Definition**: Ensuring that actions taken cannot be denied by the actors. This is essential in legal contexts.
- **Example**: Digital signatures provide non-repudiation, preventing someone from denying that they sent a document 25.

6. Security Incidents and Control Measures

What is a Security Incident?

- A **security incident** occurs when a threat exploits a vulnerability, leading to harm to an asset. It is often an unplanned event with potentially severe consequences.
- If the incident is deliberate, it is called an **attack**.

Types of Control Measures

- **Preventive Controls**: Aimed at stopping incidents before they occur.
  - **Example**: Firewalls and encryption prevent unauthorized access.
- **Detective Controls**: Help identify and detect incidents while they are happening.
  - **Example**: Intrusion Detection Systems (IDS) monitor for unusual activity.
- **Corrective Controls**: Designed to fix the impact of an incident.
  - **Example**: Restoring data from backups after a ransomware attack.

Example: Phishing Attack

- **Phishing** involves attackers sending fake emails to trick users into sharing sensitive information.
- **Preventive Measures**: Employee training can help users recognize phishing attempts.
- **Detective Measures**: Monitoring systems for abnormal login activity can help detect compromised accounts 222324.

7. Real-World Security Breaches

ANU Data Breach (2019)

- Attackers gained unauthorized access to sensitive data over an extended period, highlighting the importance of constant monitoring and detective controls 23.

Colonial Pipeline Attack (2021)

- A ransomware attack led to critical fuel supply disruption in the U.S. Attackers demanded a ransom to decrypt the company's systems.
- **Control Measures**: Preventive controls like network segmentation could have helped reduce the attack's impact 23.

8. Information States

The Three Information States

1. **In Storage**: Data is being stored (e.g., files on a hard drive).
2. **In Transmission**: Data is being transferred between locations (e.g., emails, data packets).
3. **Being Processed**: Data is actively being used or modified by a program or system.

Importance

- **Context**: Understanding the state of information helps identify suitable **control measures**. For instance, **data encryption** is particularly crucial for **in transmission** data to ensure **confidentiality** 24.

9. How to Improve Security

Identify and Classify Information Assets

- Identify **what data you hold**, **where it is stored**, and **how critical it is** to your operations.

Implement Security Measures

- **Preventive**: Encryption, firewalls, and physical security like lockable storage.
- **Detective**: Monitoring systems, logging, and regular audits to detect any unauthorized activities.
- **Corrective**: Backup solutions and disaster recovery plans to restore data in case of incidents.

Security Controls

- **Technology**: Encryption, firewalls, IDS.
- **Policies**: Acceptable use policies and guidelines for handling sensitive data.
- **Training and Awareness**: Regular training sessions to ensure employees recognize phishing attempts and follow best practices 2325.

10. Common Cyber Security Terminology

Asset

- **Definition**: Anything of value, such as data, hardware, or intellectual property, that requires protection.
- **Context**: Properly identifying assets helps determine what needs the most protection and which controls are appropriate.

Attack vs Incident

- **Attack**: A deliberate attempt to harm an asset, usually by exploiting a vulnerability.
- **Incident**: An event that harms or threatens to harm assets. Incidents can be intentional (attacks) or accidental.

Real-World Example

- **QUT Cyber Attack (2022)**: A deliberate ransomware attack disrupted IT systems, impacting service availability. It exemplifies the overlap between **information security** and **cyber security** concepts 2225.

11. Summary

- **Security Goals (CIA)** are vital for protecting assets from threats and vulnerabilities.
- Understanding **threats**, **vulnerabilities**, and how they interact is key to defending against attacks.
- **Control Measures**: Combining **preventive**, **detective**, and **corrective** controls ensures a robust security posture.
- **Real-world incidents** illustrate the importance of these concepts and underscore the need for a proactive approach to cyber security.

Final Thought

- Remember, security is not just about technology; it's about understanding and mitigating risks through the right combination of tools, policies, and education. A solid understanding of what assets need protection and which threats and vulnerabilities could impact them is fundamental to building a resilient security strategy.