Week 2 Revision notes

IFB240 Week 2 - Threats, Vulnerabilities, Incidents, and Attacks

Overview

These notes provide a comprehensive understanding of **Threats, Vulnerabilities, Incidents, and Attacks** in cybersecurity. You'll learn the key definitions, relationships between these concepts, types of attacks, and practical real-world examples, along with strategies to prevent or mitigate them. These notes are written to help you understand not only the theory but also its application in real-world scenarios.

1. Threats, Vulnerabilities, and Attacks

Definitions

- **Threat**: A potential event or action that could cause harm to an asset by compromising its security. This can be something natural (like a storm) or human-made (like a hacker exploiting a weakness).
  - **Analogy**: Think of a threat as a storm cloud forming over your house—it has the potential to do harm.
- **Vulnerability**: A weakness or flaw in your system that makes it susceptible to threats. Vulnerabilities can exist in **people** (human error), **property** (physical weaknesses), **procedures** (flawed processes), **software**, or **hardware**.
  - **Analogy**: A vulnerability is like an unlocked door—if someone tries it, they might gain access.
- **Attack**: A deliberate attempt to exploit a vulnerability to cause harm. If a threat actor tries to open the unlocked door and steal something, it becomes an attack.

Relationships Between Threats, Vulnerabilities, and Attacks

- **Intersection of Threats and Vulnerabilities**: A **security incident** happens when a threat exploits a vulnerability. An **attack** occurs if this exploitation is deliberate.
  - **Example**: A poorly configured server (vulnerability) exposed to the internet may attract a hacker (threat), leading to an attack that compromises sensitive data.
- **Threats and Vulnerabilities Coinciding without Attacks**:
  - Vulnerabilities can exist without being exploited. For instance, a software vulnerability might exist without being known to threat actors, meaning no attack occurs.
- **Real-World Example**:

- **Misconfigured Database**: A database left open to the internet is vulnerable. It becomes an incident if a cybercriminal gains unauthorised access. However, if no one attempts to access it, the vulnerability still exists, but there's no attack.

2. Threat Actors and Threat Actions

Types of Threat Actors

- **External Actors**:
  - **Cybercriminals**: Motivated by financial gain, often carrying out ransomware or phishing attacks.
  - **Hacktivists**: Driven by ideological beliefs, seeking to make a political statement.
  - **Nation-State Actors**: Attackers backed by governments, aiming for strategic benefits, often targeting critical infrastructure.
  - **Script Kiddies**: Novice attackers using pre-made tools for thrills.
- **Internal Actors**:
  - **Negligent Employees**: Those unaware of the security impact of their actions, such as misplacing sensitive documents.
  - **Malicious Insiders**: Individuals inside an organization intentionally causing harm, often for revenge or monetary gain.

Threat Actions

- **Human Actions**:
  - **Accidental**: Examples include configuration errors, misplacing sensitive information, or accidentally deleting important files.
  - **Deliberate**: Includes activities like **espionage**, **fraud**, **sabotage**, and **malware deployment**.
- **Natural Events**: Threats that arise from natural phenomena like earthquakes, floods, storms. These often impact the **availability** of systems by causing power outages, communication failures, etc.

Real-World Context

- **Brisbane Floods (2022)**: Flooding in the Brisbane CBD led to data centers being submerged, impacting the availability of information systems. This incident highlighted how **physical vulnerabilities** to natural events can lead to major disruptions 40.

3. Types of Attacks

Passive Attacks

- **Objective**: To gather information without altering the data or system.
- **Examples**:
  - **Eavesdropping**: Listening to network communications to steal sensitive information.
  - **Shoulder Surfing**: Observing someone inputting sensitive data, like watching an ATM PIN being entered.
  - **Network Monitoring**: Using packet sniffers to capture data moving across the network.
- **Why It's Dangerous**:
  - **Undetectable**: Passive attacks are hard to detect because they don't change anything within the system. Preventive measures like **encryption** are the best defence.
  - **Example**: Capturing login credentials on a Wi-Fi network without encryption is a classic form of a passive attack.

Active Attacks

- **Objective**: To alter data, disrupt services, or gain unauthorized access.
- **Examples**:
  - **Denial of Service (DoS)**: Overloading a system so that legitimate users cannot access services.
  - **Distributed Denial of Service (DDoS)**: An attack similar to DoS but conducted using multiple devices, often part of a botnet.
  - **Spoofing**: Impersonating a trusted entity, such as faking an email address to deceive the recipient.
  - **Man-in-the-Middle (MITM)**: Intercepting communication between two parties to alter or steal information.
  - **Phishing**: Social engineering technique where attackers masquerade as a legitimate entity to trick individuals into revealing sensitive information.
- **Case Example**:
  - **Mirai Botnet Attack (2016)**: The Mirai malware transformed IoT devices into bots, leading to a massive DDoS attack that targeted Deutsche Telekom, impacting 900,000 routers and affecting internet availability 38.

4. Vulnerabilities in Information Systems

Types of Vulnerabilities

- **Property (Physical Assets)**:
  - **Location Risk**: Assets located in areas prone to **natural disasters** (e.g., floods, earthquakes) are vulnerable.
  - **Lack of Security**: Inadequate physical barriers such as **missing fences, locks, or guards** can lead to increased risks.
- **ICT Hardware and Software**:

    - **Obsolete Systems**: Unsupported systems like Windows XP pose significant vulnerabilities as no security patches are available.
    - **Environmental Susceptibility**: Hardware exposed to conditions like dust, heat, or moisture can fail. Backup power and environmental controls are crucial.
    - **Configuration Weaknesses**: Systems left in **default configurations** or without regular patches are highly vulnerable.
- **People**:
    - **Social Engineering**: Employees manipulated into providing sensitive information due to a lack of awareness.
    - **Insufficient Security Training**: Employees unaware of proper security protocols may unwittingly expose the system to attacks. Training is essential to prevent phishing and social engineering attacks.
- **Processes**:
    - **Access Control Issues**: Poor management of access rights can lead to unauthorised access.
    - **Backup and Recovery Gaps**: Lack of proper data backups or not storing them securely can lead to total data loss in the event of an incident.
    - **Communication Practices**: Carelessly sharing passwords or using unsecured communication channels creates vulnerabilities .

Real-World Example

- **Ryuk Ransomware Attack**: A student downloaded pirated software, which led to a **Ryuk ransomware** infection. This incident demonstrates how a seemingly small vulnerability—unauthorized software downloads—can lead to a full-blown ransomware crisis 39.

5. Security Incidents and Chains of Events

What is a Security Incident?

- A **security incident** occurs when a **threat exploits a vulnerability**, resulting in harm. When the action is deliberate, it's termed an **attack**.
- **Example**: The **University of Tasmania** suffered a data breach in August 2020, affecting 20,000 students. A misconfigured database allowed unauthorized individuals to access personal information, showing how vulnerabilities in configuration can lead to major incidents 38.

Chain of Events in Incidents

- Security incidents often lead to a **chain reaction**:
    - **Event 1**: Misconfigured database exposes student data.
    - **Event 2**: Phishing campaigns target students, using the stolen data.

- **Event 3**: Phishing leads to installation of keylogger malware.
- **Event 4**: Attacker uses captured data to access and steal money from student bank accounts

6. Real-World Attack Examples

- **UnitingCare Queensland Ransomware Attack (2021)**:
  - **Threat Actor**: REvil ransomware targeted hospitals and aged care centers, leading to restricted access to systems.
  - **Lesson**: Healthcare infrastructure must ensure **resilience** and **response plans** to mitigate such attacks .
- **German Airports DDoS Attack (2023)**:
  - **Target**: German airports experienced a DDoS attack, claimed by 'Anonymous Russia,' which disrupted airport services.
  - **Impact**: The attack compromised the **availability** of airport websites and critical systems, showcasing how political motivations can lead to targeted disruptions .

7. Summary and Protection Strategies

Understanding Threats and Vulnerabilities

- To **protect information assets**, understand:
  - **What assets need protection** (data, hardware, systems).
  - **Potential threats and vulnerabilities** that could impact these assets.

Mitigation Strategies

- **Preventive Measures**:
  - Physical security (**locks, surveillance**).
  - Technical defenses (**firewalls, encryption, regular updates**).
- **Detective Controls**:
  - **Monitoring and Logging**: Use **IDS (Intrusion Detection Systems)**, **auditing**, and **CCTV**.
- **Corrective Actions**:
  - **Incident Response Plans**: Defined plans to restore systems after incidents.
  - **Regular Training**: Employees should understand how to identify phishing attempts and other social engineering tactics .

Consequences of Security Incidents

- The impact depends on the **value of the asset** and **severity of compromise**.
- Incidents may happen in isolation or escalate into **chains of cascading failures**, which can be devastating to an organization .

Key Takeaways

- **Threats, Vulnerabilities, and Attacks** are core concepts in understanding cybersecurity incidents. Knowing how they interact helps in creating effective security measures.
- **Different types of attacks**, both passive and active, require **different strategies** to detect and defend against.
- **Real-world incidents** illustrate the importance of combining preventive, detective, and corrective controls for a comprehensive security strategy.

These notes provide a thorough understanding of Week 2's topics, using practical examples and in-depth explanations to ensure you're well-prepared to tackle any security scenario.