Day 3 - Explore the term Threat, Vulnerability, Attack, Risk, Exploit, Asset, Impact (05/08/2024)

1) Threat

- A threat refers to any **potential danger or harmful event** that can exploit a vulnerability and cause harm to a system, organization, or individual.
- There are two ways threats attack -
  - ➔ **Intentional threats** - Attacks carried out by threat actors with **malicious intent.** These can include cyberattacks, such as malware infections, malicious code or SQL injection attacks, ransomware, phishing attempts, and distributed denial-of-service (DDoS) attacks.
  - ➔ **Unintentional threats** - These attacks originated from **human error or accidental actions** that can lead to security breaches. These threats include accidental disclosure of sensitive information or falling victim to social engineering tactics.

2) Vulnerability

- A vulnerability is a **weakness or flaw** in an operating system, network, or application.
- A threat actor tries to exploit vulnerabilities to **gain unauthorized access** to data or systems.
- Common vulnerabilities include software vulnerabilities, easily guessable passwords, unpatched systems, lack of encryption, insecure network configurations, and human error such as falling for phishing scams or sharing sensitive information unintentionally.

3) Attack -

- An attack is a deliberate **unauthorized action** on a system or asset. Attacks can be classified as active and passive attacks. An attack will have a motive and will follow a method when the opportunity arises.

Types of Attack

- **Active Attack:** Active attacks aim to **manipulate** system resources or impact their operation.
- **Passive Attack:** Passive attacks aim to **extract sensitive information** from a system **without affecting** its resources.

4) Risk -

- Risk is the likelihood of a threat exploiting a vulnerability and causing harm. It represents the **potential loss or damage** associated with a specific threat.
- Organizations employ **risk management** processes and methodologies to identify, evaluate, and prioritize security risks.
- Risk assessment is the systematic **identification of potential cybersecurity threats,** vulnerabilities and their associated impacts; and risk assessment is one of the most important parts of risk management. It helps organizations to understand their security posture, prioritize resources, and make informed decisions regarding risk mitigation.

5) Exploit -

- An exploit is a **piece of software,** data, or sequence of commands that **takes advantage of a vulnerability** to cause unintended or unanticipated behavior in software or hardware.
- Common exploits include zero-day exploits, buffer overflow exploits.

6) Assets -

- Assets are **anything of value** to an organization that needs to be protected, including data, software, hardware, and personnel.
- Examples: Customer data, intellectual property, servers, employee information.

7) Impact -

- Impact is the **effect or consequence** of a threat exploiting a vulnerability. It is a measure of the potential damage or loss to the assets such as financial loss, reputational damage, legal consequences, operational downtime.

Analyzing the Pegasus Airline data breach -

- **Threat -** The threat here includes unauthorized individuals or groups who could access the misconfigured AWS bucket. These could be hackers, cybercriminals, or even malicious insiders.
- **Vulnerability -** The vulnerability in this case was the misconfigured security settings on the AWS bucket used by Pegasus Airline. This misconfiguration left the data exposed to the internet without proper access controls.
- **Attack -** The actual attack was the unauthorized access to the exposed data in the AWS bucket. This could include downloading, modifying, or even deleting the data.
- **Risk -** The risk involved the potential exposure of sensitive data, which could lead to financial loss, reputational damage, and operational disruptions for Pegasus Airline, as well as the two other airlines using the software, Turkish IZ Air and Kyrgyzstani Air Manas.
- **Exploit -** The exploit in this scenario was the use of web scanners by researchers (and potentially malicious actors) to identify and access the misconfigured AWS bucket, taking advantage of its lack of security controls.
- **Asset -** The assets at risk included 6.5 terabytes of data comprising 23 million files. This data included personal information of the flight crew, flight charts, navigation materials, plain text passwords, secret keys, and source code for the EFB software.
- **Impact -** The impact of this data breach included potential unauthorized access to sensitive information, which could lead to identity theft, intellectual property theft, financial fraud, and compromised safety procedures. The exposure of nearly 400 files with plain text passwords and secret keys could allow further attacks on the systems and databases of Pegasus Airline and its clients.

Conclusion - The Pegasus Airline data breach is a classic example of how a vulnerability (misconfigured AWS bucket) was exploited by a threat (unauthorized access), resulting in an attack (data breach). The risk involved was significant due to the value of the assets (sensitive data) at stake. The impact of this breach could have severe repercussions, including financial loss, reputational damage, and potential legal consequences for Pegasus Airline and the other affected airlines. This incident underscores the importance of proper configuration and security controls in cloud services to protect valuable data assets.