Cyber Security Vulnerabilities

Outline

- Overview
- Types
  - Software Vulnerabilities
  - Network Vulnerabilities
  - Human Factors
  - Physical Vulnerabilities
  - Organizational Vulnerabilities
- common exploitation techniques
  - SQL Injection
  - Cross site scripting (XSS)
  - Buffer overflow
- Management strategies
  - Regular scanning and Testing
  - Patch Management
  - User Training and Awareness

Cyber security Vulnerabilities : An Overview

- what is cyber security vulnerability?
- A vulnerability is known as a weakness that can be exploited by anyone to gain unauthorized access to computer.[1]
- a cyberattack can run malicious code, install malware, and even steal sensitive data.

Cyber security Vulnerabilities : An Overview

- Difference between Vulnerability and Risk[1]:
- Think of risk as the probability and impact of a vulnerability being exploited.
- If the impact and probability of a vulnerability being exploited is low, then there is low risk. Inversely, if the impact and probability of a vulnerability being exploited is high, then there is a high risk.
- Generally, the impact of a cyber attack can be tied to the CIA triad or the confidentiality, integrity, or availability of the resource. Following this train of reasoning, there are cases where common vulnerabilities pose no risk. For example, when the information system with the vulnerability has no value to your organization.

Cyber security Vulnerabilities : An Overview

- When Does a Vulnerability Become an Exploitable?[1]:

- A vulnerability with at least one known, working attack vector is classified as an exploitable vulnerability. The window of vulnerability is the time from when the vulnerability was introduced to when it is patched.
- If you have strong security practices, then many vulnerabilities are not exploitable for your organization.
- For example, if you have properly configured S3 security, then the probability of leaking data is lowered. Check your S3 permissions, or someone else will.
- Likewise, you can reduce third-party risk and fourth-party risk with a Third-Party Risk Management framework and Vendor Risk Management strategies.

Types of Vulnerabilities

- **Software Vulnerabilities :**
  - Outdated or Unpatched Software : Software that is not regularly updated or patched presents significant vulnerabilities. Attackers exploit these weaknesses to launch malware, ransomware, and other cyber attacks. Implementing a rigorous process for prioritizing and automating software updates and patches can mitigate this risk.
  - Zero-day Vulnerabilities : Zero-day vulnerabilities are previously unknown flaws that are exploited before developers have a chance to address them. These vulnerabilities require a proactive defense strategy, including advanced threat detection systems and a comprehensive endpoint security solution.
  - Hardware Vulnerabilities : Hardware vulnerabilities arise from physical or design flaws in hardware components. Mitigating hardware vulnerabilities can be challenging and may require physical modifications or firmware updates. Default usernames and passwords, Outdated firmware and Unsupported legacy devices are just some examples of hardware vulnerabilities.

Types of Vulnerabilities

- **Software Vulnerabilities :**

  - Network Vulnerabilities : Network vulnerabilities exist in the infrastructure and protocols that govern internet and network communications. Weaknesses in network architecture, such as unsecured Wi-Fi networks or outdated encryption protocols, can allow attackers to intercept or alter data in transit. Effective network security measures, including the use of VPNs and updated encryption methods, are vital for protection against these vulnerabilities
  - Unsecured APIs : Application Programming Interfaces (APIs) serve as bridges between different software applications, facilitating their interaction. Unsecured APIs are a prime target for attackers due to their accessibility over the internet and inherent security risks. Securing these requires encryption, proper IT hygiene during development, and regular key rotation.

Types of Vulnerabilities

- Network Vulnerabilities[3] : There are plenty of network vulnerabilities a hacker can exploit to access valuable information, but the four most common types are:
- Malware: Malicious software includes worms, Trojans, and viruses that can infiltrate a device or host server. People unknowingly buy or download malware that will exploit a network vulnerability.
- Outdated or Bugged Software: Systems running an application without adequate patching can potentially infect an entire network if someone finds and manipulates the flaw.
- Social Engineering Attack: Network intruders can use various methods to fool workers into unintentionally giving up confidential data like passwords or login information.
- Misconfigured Firewalls or Operating Systems: Default settings are easy to guess and are well known.

Types of Vulnerabilities

- Human Factor[4] : The human factor in cybersecurity refers to the influence of human behavior on the security of information systems.
- Human Error as a Major Contributor: A 2023 study by Verizon found that 74% of security breaches involved human error, often stemming from innocent mistakes rather than malicious intent.
- Common Human Errors :
  - Phishing and social engineering
  - weak password practices
  - System misconfiguration
  - software updates failure
- Lack of security awareness : Employees who are unaware of potential threats are less likely to recognize and respond appropriately to security incidents

Types of Vulnerabilities

- Physical Vulnerabilities[4] : mostly it affects to cloud infrastructure vendors and large organizations operating in-house data center systems. It may include :
  - The ability to access server rooms
  - Camera blind spots
  - Inadequate documentation
  - Recording of physical activities performed in the data center, such as replacing storage devices
- To address physical vulnerabilities, organizations must enforce strict policy controls governing the use of business information on BYOD devices. They should also regulate access to corporate apps, services, and networks from outside the organization's physical premises.

Types of Vulnerabilities

- Organizational Vulnerabilities

Types of Vulnerabilities

- Insider Threats : According to research, the human element is responsible for 95% of all cyber security incidents.
- The vulnerability of an insider threat is a challenging case : at the outset an employee is trusted with sensitive business information and access to mission-critical technology systems. If the employee becomes dissatisfied or disgruntled and intentionally chooses to harm their organization, the risk exposure comes down to two things:
  - The access privileges assigned to them
  - Their ability to gain unauthorized access

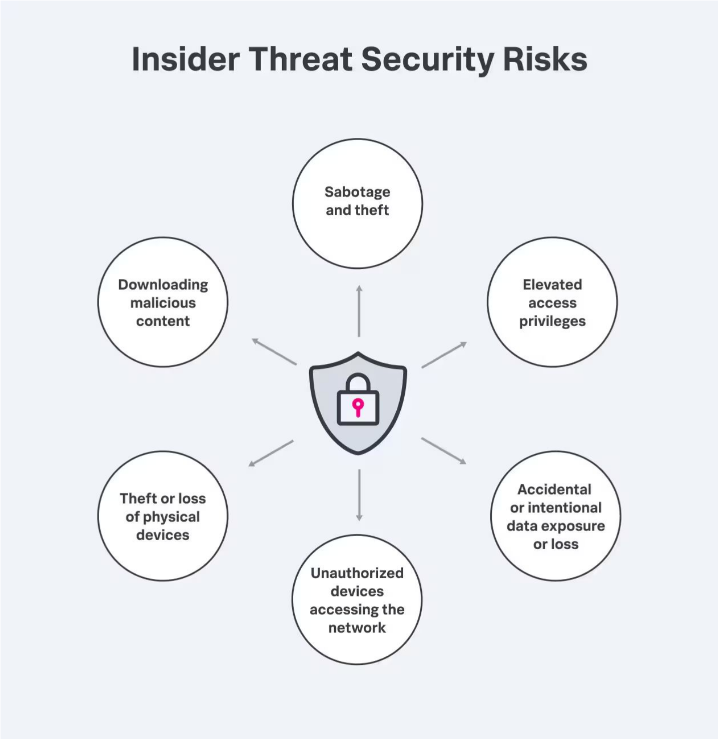
Insider Threat Security Risks
Sabotage and theft
Downloading malicious content
Elevated access privileges
Theft or loss of physical devices
Accidental or intentional data exposure or loss
Unauthorized devices accessing the network

Fig:Insider threat [5]

Common Exploitation techniques

- SQL Injection

Common Exploitation techniques

- cross site scripting(XSS)

Common Exploitation techniques

- Buffer Overflow

Management Strategies

- Regular scanning and Testing

Common Exploitation techniques

- Patch Management

Common Exploitation techniques

- User Training and Awareness

References

1. https://www.upguard.com/blog/vulnerability
2. https://insights.integrity360.com/what-are-the-types-of-vulnerability-in-cyber-security
3. https://www.digitaldefense.com/blog/what-are-the-most-common-types-of-network-vulnerabilities/
4. https://www.crowe.com/insights/the-human-factor-in-cybersecurity
5. https://www.splunk.com/en_us/blog/learn/vulnerability-types.html
6.
7.
8.