Topic 1 Discussion 1

What is the definition of a vulnerability? What are some key characteristics and how are they classified according to industry standard? What are the root causes of vulnerabilities, motivations, and techniques utilized from threat actors? What mitigations could be used to secure them? Provide an example.

Hello Class,

A vulnerability is defined as a weakness in an information system, system security procedures, internal controls, or implementation that a threat source can exploit to gain unauthorized access or cause harm (CSRC, 2015). Key characteristics of vulnerabilities include their exploitable nature, which allows attackers to compromise systems, and their variety, which can range from software bugs to misconfigurations. Vulnerabilities are typically classified using the Common Vulnerability Scoring System (CVSS), which assesses their severity and categorizes them into levels such as Informational, Low, Medium, High, and Critical (Imperva, 2024).

Root causes of vulnerabilities often stem from several factors, including complexity in system design, poor coding practices, and human error (Spacey, 2013). Vulnerabilities can also come from lack of security updates and misconfigurations. Threat actors are motivated by various factors, including financial gain, espionage, and ideological beliefs (Sophos, 2024). They utilize techniques such as phishing, exploiting software flaws, and social engineering to exploit these vulnerabilities. A common one used that I see nearly every day is phishing.

To mitigate vulnerabilities, organizations can implement several strategies. These strategies include : Regular vulnerability assessments to identify and prioritize weaknesses, patch management to ensure that software is up-to-date and secure, access controls to limit user permissions and reduce exposure , employee training to raise awareness about security best practices and phishing attacks, and incident response planning to prepare for potential breaches.

Example:

A common vulnerability would be the use of SQL injection. SQL injection is where attackers exploit input fields to execute arbitrary SQL code, potentially compromising the database. By employing input validation and prepared statements, organizations can significantly reduce the risk of such vulnerabilities (Goodman, 2022).

References:

CSRC. (2015). *vulnerability - Glossary | CSRC*. Nist.gov. https://csrc.nist.gov/glossary/term/vulnerability

Goodman, C. (2022, September 23). *What is a vulnerability? Examples, Types, Causes*. Balbix. https://www.balbix.com/insights/what-is-a-vulnerability/

Imperva. (2024). *What is CVE and CVSS | Vulnerability Scoring Explained | Imperva*. Learning Center. https://www.imperva.com/learn/application-security/cve-cvss-vulnerability/

Sophos. (2024). *Threat Actors Explained: Motivations and Capabilities*. SOPHOS. https://www.sophos.com/en-us/cybersecurity-explained/threat-actors

Spacey, J. (2013, March 5). *The 10 Root Causes Of Security Vulnerabilites*. Simplicable. https://arch.simplicable.com/arch/new/10-root-causes-of-security-vulnerabilites