TALENTO TECH

REGIÓN 3
CAUCA - NARIÑO
LESSON 4 -UNIT 2

TIC

Universidad Tecnológica de Pereira

faceIT

Lesson 4: Introduction to Vulnerability and Risk Management: Identifying, Evaluating, and Prioritizing Threats

1. **Reading: Vulnerability, Threat,and Risk Management**

Vulnerability, threat, and risk management represent fundamental cybersecurity practices capable of shielding both systems and data belonging to an organization. Below is an explanation of these terms, redefined and illustrated to maximize their potential understanding.

What Is Meant by Vulnerabilities?

Vulnerability is defined as a weakness in a computer system that can be exploited by an attacker. This includes software bugs, inappropriate settings, and missing updates. For example,if the program has a glitch that allows the hacker to access it without permission, that is termed as vulnerability.

Vulnerability Management Processes

The vulnerability management process is a continuous functionin multiple steps. As mentioned by the authors, these are:

- Vulnerability Identification: Automates the process,may involve tool scanning of the system, identifying vulnerabilities, etc. For example, software can verify insecure settings or pending updates.
- Evaluation: After identified vulnerabilities, they should be evaluated on the basis of their severity, which will further help to decide which vulnerabilities should be preferred to be fixed first—for instance, a vulnerability that lets you gain full access to a system versus one that only targets a small feature.
- Prioritization: Vulnerabilities are classified on the basisof the risk associated with them for the organization; this helps channel resources to the most critical areas.
- Correction: A solution is implemented to fix or reduce the vulnerabilities. This could include applying software patches or changing settings.
- Monitoring: Continuous monitoring is done to find new vulnerabilities as they arise.

What Are Threats?

A threat is any eventor situation that has the potential to cause harm to computersystems. Threats can be intentional, such as cyberattacks, or unintentional, like natural disasters.

Example: A phishingattack, where a hacker triesto trick a user into revealing sensitive information, is a common threat in the digital world.

Threat Management

Threat management involves identifying, evaluating, and responding to potential threats:

- Identification: Recognizing what types of threats can affect the organization.
- Evaluation: Determining the likelihood and potential impact of each threat.
- Response: Creating plans to reduce the impact if a threat happens.

What Are Risks?

- Risk is the combination of the likelihood of a harmfulevent happening and the impactit would have on the organization. In cybersecurity, this refers to how vulnerabilities and threats could affect the confidentiality, integrity, and availability of data.
- Example: If a company doesn’tupdate its softwareregularly (vulnerability) and gets attacked (threat), the risk is high because there’s a high chance the data will be compromised.

Risk Management

Risk management in cybersecurity includes:

- Risk Identification: Figuring out what risks exist.
- Analysis: Evaluating the severity and probability of each risk.
- Control: Taking stepsto reduce or eliminate the risks.
- Monitoring: Continually checking how effective the control measures are.

Practical Example

Let’s imaginea high school that uses computers for online classes:

- Vulnerability: The computers have outdated software.
- Threat: A hacker tries toaccess the school system to steal personal information.
- Risk: If the hacker is successful, they could compromise sensitive data like addresses and phone numbers.

To manage this,the school shouldregularly update the software (correction), teach students how to spot suspicious emails (threat management), and evaluate how likely an attack is (risk management).

Conclusion

Effective management of vulnerabilities, threats, and risks is crucial to protecting any organization in today's digital world. By understanding these concepts and how they are related, young peoplecan be better prepared to face the challenges of the digitalworld and contribute to cybersecurity in their future careers and daily lives.