Bootcamp PPT#5

Session 2.2 Governance, Risk, and Compliance II

Sunday September 13, 2020 / 6:30-9:30 PM
Zoom Link: https://zoom.us/j/2246200754
Zoom Password: 508637

Class Objectives

- Identify threats, attacks, and vulnerabilities.
- Prioritize risks ased on likelihood.
- Choose and justify controls.

GRC: Risk Management and Threat Modeling

- Difference between **vulnerablity**, **threat**, and **risk**.
- **Vulnerability:** Lack of protection, asset that can be exploited.
- **Threats:** The actor or agent that will exploit a vulnerability.
- **Risks:** Outcomes and possibilites.

Risk Management

- Measured quantitatively.

Threat Modeling

- Results shared upwards, theoretical.
- **PASTA:** Process for Attack Simulation & Threat Analysis
- **STRIDE:** Spoofing tampering, repudiation, information disclosure, denial of service, elevation of privilege.
- **OWASP:** Open web application security project.
  - **Determine asset scope.** Developing inventory with priority.
  - **Identify threat agents.** Identifying ATP, Script Kiddies, Employees, and Incomptetence.
  - **Identify potential attacks.** Analyze each agent, identify **motivation**, **skill level**, and **funding**.
  - **Identify exploitable vulnerabilities.** Identify vulnerable points in the system or network.
  - **Prioritize identifies risks.**
  - **Mitigate risks.**

Risk Analysis

- **Qualitative:** identifying intuitive, unmeasurable factors.
- **Quantitative:** measuring expectation of risks with respect to data.
    - **Asset Value** *AV*
    - **Exposure** *EF*
    - **Annual Rate of Occurance** *ARO = AV x EF*
    - **Annual Lost Expectancy** *ALE = SLE x ARO*

Mitigating Risks

- **Control Types**
    - Physical, Administrative, Technical
- **Necessary Effectiveness**
- **Cost** / **Time** of Implementation

Practical Threat Modeling

- Answering the **4 Golden Questions**:
    - What are we working on?
    - What can do wrong?
    - What will we do about it?
    - Did we do a good job?
- Secure Coding Practices