Southern New Hampshire University

CYB 250 Stepping Stone One Template

Name: Juliano Alves de Souza

Professor: Taylor Bianchi

I. Threat Modeling:

Howard Threat Model			
Incident	Target Breach	Sony Breach	OPM Breach
Attackers	Cybercriminals possibly based in Eastern Europe.	The group is named 'Guardians of Peace', possibly with nation-state support.	Suspected state-sponsored actors (China).
Tools	Malware, including BlackPOS.	Malware, data wiping tools, data exfiltration techniques.	Advanced malware (PlugX, Sakula), remote access tools.
Vulnerability	Weakness in third-party vendor security, lack of robust network segmentation.	Inadequate security practices, lack of strong network defenses.	Poor security practices, lack of two-factor authentication.
Action	Intrusion via a third-party HVAC vendor, malware installation on POS systems.	Network infiltration, data destruction, data leaks.	Use of stolen credentials, escalation of privileges, data exfiltration.

Target	Credit and debit card information of customers.	Sensitive corporate data including emails, employee data, intellectual property.	Personnel records, background check data, fingerprint data.
Unauthorized Result	Theft of approximately 40 million credit/debit card records and 70 million customer records.	Public disclosure of sensitive data, reputation damage, financial loss.	Compromise of sensitive data affecting millions of individuals.
Objective	Financial gain through the sale of stolen card details.	Political motivations, reputational damage, and possibly financial extortion.	Espionage, gathering of sensitive information on U.S. government employees.

II. Incident Analysis:

→For Sony breach

A. For the Sony breach, The most applicable aspect of the CIA triad to the "Action" category is Confidentiality. The breach involved unauthorized access and disclosure of sensitive corporate data, including emails and intellectual property. This violation of confidentiality led to significant exposure of private information.

B. Using an adversarial mindset in analyzing the "Attackers" and "Objective" involves understanding the attackers' motivations and tactics. By acknowledging that the attackers (Guardians of Peace) were likely driven by political motives and aimed to cause reputational damage, a more informed response could include enhanced monitoring of indicators of politically motivated attacks and improved data encryption and segregation to protect sensitive information.

C. If I worked for Sony and used a threat model proactively, changes to avoid the incident could include:

- Strengthening network security and implementing robust access controls.
- Regular security training for employees to recognize phishing attempts and other social engineering tactics.
- Implementing more stringent data classification and encryption strategies.
- Increasing monitoring for unusual network activities and having a faster incident response plan.
- Conducting regular security audits and penetration testing to identify and fix vulnerabilities.

III. Threat Modeling Extension:

A- Threat modeling is not just a security exercise; it's a strategic tool that helps us understand and prepare for potential cyber threats proactively.

I. By identifying vulnerabilities early, we can tailor our security measures specifically to making defenses more effective and cost-efficient:

- **Identifies Potential Threats Early**: It uncovers vulnerabilities and potential attack vectors before they are exploited, reducing the risk of breaches and associated costs.
- **Improves Security Posture:** It helps tailor security measures to the specific risks an organization faces, enhancing overall security.
- **Cost-Effective:** Preventing attacks is typically more cost-effective than responding to them.
- **Compliance and Reputation:** It assists in compliance with regulatory requirements and protects the organization's reputation by demonstrating a commitment to security.

This proactive approach not only enhances our security posture but also supports compliance with regulatory standards, protecting our reputation. Beyond security, threat modeling fosters better decision-making, aligns security with our business goals, and enhances cross-departmental understanding. In IT roles, threat modeling provides unique insights – testers can focus on data mutations, designers on analyzing threats in system architecture, and developers on tracking data flow and code vulnerabilities.

Threat modeling is crucial for security practitioners as it provides a structured approach to identify, prioritize, and mitigate potential threats.

II- Beyond security, threat modeling can offer organizational benefits like informed decision-making, better alignment of security with business objectives, and improved communication and understanding across different departments.

B- Threat modeling differs across IT roles due to their distinct responsibilities:

- **Testers focus on data mutations.** They simulate attacks and test the system's responses to various threat scenarios, identifying potential vulnerabilities.
- **Designers** concentrate on analyzing threats against the system's architecture. They evaluate how the design choices might introduce or mitigate security risks.
- **Developers** are tasked with tracking data flow. They scrutinize the pathways through which data travels in the system, identifying spots where data might be intercepted or manipulated.

Each role applies its unique lens to threat modeling, ensuring a comprehensive approach to identifying and mitigating security risks.

Southern New Hampshire University

References:

1- Meyer, A. (2015, January 9). Lessons from the Sony breach in risk management and business resiliency. SurfWatch Labs. https://www.networkworld.com/article/2867313/lessons-from-the-sony-breach-in-risk-management-and-business-resiliency.html

2- Shu, X., Tian, K., Ciambrone, A., & Yao, D. (2017). Breaking the Target: An Analysis of Target Data Breach and Lessons Learned.

3- Fruhlinger, J. (2020, February 12). The OPM hack explained: Bad security practices meet China's Captain America. CSO Online. https://www.csoonline.com/article/3513899/the-opm-hack-explained-bad-security-practices-meet-china-s-captain-america.html

4-