Gagujas, Michael

CS405 – Secure Coding

June 30, 2024

8-2 Journal Reflection

“Adoption of a secure coding standard” and “not leaving security to the end” are two secure coding practices that ensure the reliability, integrity, and robustness of software applications. They foster a culture of security awareness that emphasizes a proactive approach for addressing potential vulnerabilities and implementing effective security measures. Adoption of a secure coding standard provides guidelines and best practices that help with writing code that is more resistant to attacks and less likely to have vulnerabilities. They address common mistakes, but more importantly, they cultivate a mindset of security consciousness that helps developers anticipate and mitigate potential threats. Similarly, not leaving security to the end cultivates a mindset of considering security from the start, where it becomes an integral part of the software development lifecycle process. Rather than waiting until the end of a project or reactively applying security, security is continuously thought of and applied to better identify and prevent potential vulnerabilities. Overall, the effective application of both processes prevents unnecessary refactoring for issues involving complications or legal compliance, and each practice leads to the development of software that is more secure, reliable, and efficient.

Other aspects to consider are the evaluation and assessment of risks and the cost benefit of their mitigation. Performing risk assessments helps to identify potential risks, estimate their chances for occurring, and evaluates their potential impact. They significantly improve the decision-making process for mitigating risks and enhancing the overall security of a system. A specific mitigation strategy or deciding if one is even necessary can vary depending on the constraints of a specific project, so understanding a project’s scope, resources, and objectives is crucial for effective and cost-efficient project management. It's important to consider that various mitigation strategies have tradeoffs where more security can also mean increased operational costs, the need for continuous monitoring, and the potential for reduced efficiency. Users may be inconvenienced by more security protocols, and implementation of more complex mitigation strategies can disrupt operations, potentially lead to downtime, and require employees to take additional training.

A common concept that many companies are adopting to adapt to the evolving nature of cybersecurity threats is the zero-trust policy where “no one is safe” since they aren’t trusted by default. By considering potential internal threats along with external threats, companies can create a more comprehensive and robust cybersecurity strategy that reduces the possibility and damages of breaches. Dividing a system’s network and implementing strict access controls makes it that much more difficult for attackers to gain unauthorized access and compromise sensitive data. When combined with continuous monitoring and logging, this approach can provide a real-time view of network activities, which allows for the swift detection and response to any potential threats.

Implementing security policies and performing gap analysis for recommendations towards its improvement are essential steps for maintaining a robust cybersecurity framework within an organization. Security policies outline the rules, procedures, and standards for establishing a secure environment that will protect a company’s assets and ensure they comply with regulatory requirements. Recommendations from gap analysis can pinpoint company weaknesses and allow companies to make informed decisions that align themselves with industry standards and their desired state. Ultimately, proactively addressing vulnerabilities significantly enhances the overall security of a system, and they allow organizations to more effectively identify, track, and prevent any potential threats.