Alex Walrond

Prof Mimi

CS-405

08/18/2024

8-2 Journal: Portfolio Reflection

The principle of integrating security from the outset of the software development lifecycle (SDLC) is crucial in preventing vulnerabilities that could be exploited by malicious actors. Adopting a secure coding standard ensures that developers follow best practices consistently, which reduces the likelihood of introducing security flaws. For example, incorporating input validation, proper error handling, and secure authentication mechanisms can prevent common attacks like SQL injection, cross-site scripting (XSS), and buffer overflows.

Risk assessment involves identifying potential security threats, evaluating their likelihood, and determining their potential impact on the organization. The goal is to prioritize risks and allocate resources to mitigate them effectively. In this context, the concept of "risk appetite" plays a critical role—organizations must decide how much risk they are willing to accept and what level of mitigation is appropriate.

The zero trust security model challenges the traditional notion of trusted internal networks and untrusted external networks. Instead, zero trust assumes that no user or device—inside or outside the network—should be trusted by default. This paradigm shift is increasingly necessary as organizations adopt cloud services, remote work, and other technologies that blur the boundaries of the corporate network. Zero trust emphasizes the continuous verification of identities and strict access controls based on the principle of least privilege. The readings on zero trust highlight how this approach can mitigate the risks posed by insider threats, compromised credentials, and advanced persistent threats (APTs). For example, the zero-trust model can prevent lateral movement within a network, a tactic often used by attackers to escalate privileges and access sensitive data.

Security policies provide the framework for how security is managed within an organization. These policies should be comprehensive, covering aspects such as data protection, incident response, access control, and compliance with regulatory requirements. The readings on policy development suggest that effective security policies must be clear, enforceable, and regularly reviewed to ensure they remain relevant in the face of evolving threats.When implementing security policies, it's important to balance security needs with business objectives. For example, a stringent access control policy might enhance security but could also hinder productivity if not implemented thoughtfully.