8-2 Journal: Portfolio Reflection

Unique Chambers

Southern New Hampshire University

CS-405-R3360 Secure Coding 24EW3

03/03/2024

Integrating security at the start of the software development lifecycle (SDLC) ensures that security considerations are not an afterthought but are embedded in the architecture, design, and implementation. Secure coding standards like OWASP Top 10, CERT Secure Coding Standards, and Common Weakness Enumeration (CWE) provide guidelines and best practices for writing secure code.

Secure coding standards are adopted to prevent common security vulnerabilities. They guide developers on how to write code that is resilient against attacks. Security is cheaper and more effective when addressed early in the SDLC.

Secure coding standards help in preventing vulnerabilities that could lead to security incidents. It is more cost-effective to address security early in the SDLC rather than fixing security issues after deployment, which can be expensive and damaging to the organization's reputation.

Zero Trust is a security concept centered on the belief that organizations should not automatically trust anything inside or outside its perimeters and instead must verify anything and everything trying to connect to its systems before granting access. This approach is increasingly relevant due to the increase in remote work and cloud computing.

Zero Trust architectures do not assume trust based on network location. They require continuous verification of the security status of assets and users. Implementation often involves multi-factor authentication, least privilege access, and micro-segmentation. In a zero-trust model, security is not a one-time thing but a continuous process. Each access request is evaluated, and the principle of least privilege is enforced, minimizing the potential impact of breaches.Highlight the importance of security policies.

Some suggested considerations for effective policy implementation are Security policies. They define how issues are handled, what behaviors are expected, and the framework within which the organization operates to secure its assets. Security policies should be clear, enforceable, and aligned with business objectives. They should be communicated effectively to all stakeholders. Regular training and awareness programs are crucial for policy adherence.

Effective security policies require that they are well understood and accepted by all members of the organization. Regular reviews and updates are necessary to keep the policies relevant to the evolving threat landscape.