Jorden Thomas

Southern New Hampshire University

12/22/2024Adoption of a secure coding standard, and not leaving security to the end

For this discussion, the approach would be to discuss the importance of integrating security within the development lifecycle. Integrating security at the start of the software development lifecycle ensures that security considerations are not an afterthought but are embedded in the architecture, design, and implementation. Secure coding standards like OWASP's top 10, CERT's Secure coding standards, and common weakness enumeration provide guidelines and best practices when writing secure code.

Secure coding standards help in preventing vulnerabilities that could lead to security incidents. This is more cost-effective when addressing security early in the SDLC rather than fixing security issues after deployment. As it can be expensive and damaging to the organization’s reputation.

Evaluation and assessment of risk and cost-benefit of mitigation

For this discussion, the approach would be to discuss the proof of identifying, evaluating, and prioritizing risks. While also analyzing how risk assessment influences the mitigation strategies. Risk assessment is a core component of any security program. It involves the identification of potential threats and vulnerabilities along with the assessment of the potential impact and likelihood of those risks. The cost-benefit analysis will then be used to determine whether the cost of mitigation is justified by the benefit of reducing risk.

The cost-benefit analysis in risk mitigation ensures that resources are allocated effectively, and the organization is not spending more on mitigating a risk than the potential loss that risk represents.

Zero trust

For this discussion, the approach would explain the concept of Zero Trust as well as discuss its relevance in modern security architecture. Zero Trust is a security concept that is centered around the belief that organizations should not automatically trust anything inside or outside its perimeter and instead must verify anything and everything trying to connect to the system before access is granted. This approach is increasingly relevant due to the rise in remote work and cloud computing.

Within the Zero Trust model, security is not a one-time gate but a continuous process. Each access request is evaluated, and the principle of least privilege is enforced. This will minimize the potential impact of breaches.

Implementation and recommendations of security policies

For this discussion, the approach would be to discuss the importance of security policies while suggesting consideration for effective policy implementation. Security policies form the backbone of an organization’s security posture. They define how issues are handled and what behaviors are expected. Effective implementation of security policies requires that they are well understood and accepted by all organization members. Regular reviews and updates are mandatory to keep policies relevant to the evolving threat landscape.