Mohamed Jaddour

CS-405 Secure Coding

8-2 Journal: Portfolio Reflection

06/30/2024

**Adopting of a secure coding standard, and not leaving security to the end:**

Secure coding standards ensure that security is integrated into the development process from the beginning, rather than the end. By adhering to established coding standards, developers can avoid common programming errors that lead to vulnerabilities such as SQL injection, and buffer overflows, thereby reducing vulnerabilities. These standards create a uniform approach to security across development teams, leading to more consistent and reliable code. Addressing security issues early in the development lifecycle is significantly cheaper than fixing them post-deployment, as the cost of fixing a bug discovered during the testing phase is much lower than one found after release. Early integration of security measures reduces the risk of vulnerabilities being exploited in production, thereby protecting the organization's data and reputation, which is essential for risk mitigation. Moreover, early adoption of security practices will ensure compliance with industry standards and regulations, to prevent any legal or financial penalties.

**Evaluation and assessment of risk and cost benefit of mitigation**

Identify potential security threats and vulnerabilities through threat modeling and risk assessments, which involves understanding the system, identifying potential attack vectors, and assessing the likelihood and impact of various threats. Compare the cost of implementing security measures against the potential impact of security breaches by calculating the potential financial, reputational, and operational costs of a breach versus the investment required for mitigation through a cost-benefit analysis.

**Zero trust**

Zero trust requires continuous authentication and authorization of all users and devices, regardless of their location within the network, ensuring that only legitimate users have access to resources. Implementing least privilege access means users only have the minimum necessary permissions to perform their tasks, reducing the potential impact of a compromised account. Operating under the assumption that the network is already compromised leads to the implementation of robust monitoring and incident response measures to detect and mitigate threats quickly.

**Implementation and recommendations of security policies**

Develop clear and comprehensive security policies that cover all aspects of information security, including access control, data protection, incident response, and employee training. Continuously review and update security policies to address evolving threats and technological advancements, ensuring policies remain relevant and effective. Conduct regular training sessions to ensure all employees understand and adhere to security policies, fostering a culture of security awareness within the organization. Implement mechanisms to enforce security policies and ensure compliance, which can include regular audits, monitoring, and disciplinary actions for policy violations. Develop and implement a robust incident response plan to quickly address and mitigate security breaches, including clear procedures for detecting, reporting, and responding to incidents.

**Sources:**

Bower, J. (n.d.). *Zero trust security | what is a Zero trust network? | cloudflare*. Zero Trust security | What is a Zero Trust network? <https://www.cloudflare.com/learning/security/glossary/what-is-zero-trust/>

Pryimenko, L. (2024, April 24). *8 steps for Data Breach Response and investigation | ekran system*. Liudmyla Pryimenko  Origin: https://www.ekransystem.com/en/blog/author/liudmyla-pryimenko © Ekran System. https://www.ekransystem.com/en/blog/data-breach-investigation-best-practices