Ryan G. Cooper

Professor Conlan

CS-405 Module 8 Journal

June 30th, 2024

**Reflection**

Having a consistent secure coding standard early in the development process is crucial to ensuring the overall security and robustness of software applications. Secure coding standards provide a set of best practices that developers can follow to avoid common vulnerabilities, such as SQL injection, cross-site scripting, and buffer overflows. By integrating these standards from the beginning, security becomes an integral part of the development lifecycle rather than an afterthought. This proactive approach reduces the risk of vulnerabilities and can significantly lower the cost and effort required for post-release fixes. Overall, addressing security early can prevent the compounding of risks and make the development process more efficient and reliable.

Evaluating and assessing risk, along with performing a cost-benefit analysis, are essential components of picking a security strategy. Risk evaluation helps in identifying potential threats and vulnerabilities, allowing developers to prioritize issues based on their severity and impact. By conducting a thorough cost-benefit analysis, organizations can make decisions about which security measures to implement, ensuring that resources are allocated effectively. This approach aligns with a Zero Trust model, which shows the importance of continuous verification and assumes that threats can come from both inside and outside the network. By implementing Zero Trust principles, organizations can minimize the risk of unauthorized access and limit the potential damage of security breaches. This model requires continuous monitoring, regular security assessments, and the adoption of least privilege access, ensuring that users only have access to the resources necessary for their roles. Recommendations for security policies should include regular employee training and the use of advanced security tools to monitor and protect against threats. Employee training programs are essential to ensure that all staff members are aware of the latest security practices, potential threats, and their role in maintaining security. By incorporating these recommendations into their security policies, organizations can create a robust and adaptive security framework that effectively protects against all threats.