Dhevie Miller

CS 405 - 10932

Module Eight Journal

August 19, 2024

Portfolio Reflection

Adopting a secure coding standard is crucial in building reliable and resilient software, especially in a world where cyberattacks are becoming increasingly sophisticated. We can significantly reduce vulnerabilities and prevent costly security breaches by integrating secure coding practices from the beginning of the software development lifecycle (SDLC). For instance, the MGM Resorts cyberattack in 2023 demonstrated how neglecting security can lead to severe operational and financial consequences. The attackers exploited social engineering techniques to breach MGM’s systems, emphasizing the need for robust security policies and practices. By adopting secure coding standards like those developed by CERT, organizations can ensure that security is baked into every step of the development process, reducing the likelihood of vulnerabilities being introduced (Seacord, 2013).

Leaving security to the end of the SDLC is risky, as vulnerabilities discovered late in the process or after deployment can be costly to fix and may have already been exploited by attackers. Secure coding standards should be an integral part of the development process, guiding programmers to follow consistent and safe practices. For example, using Role-Based Access Control (RBAC) early in developing platforms like Brightspace helps prevent unauthorized access and protects sensitive data, ensuring that security is not treated as an afterthought but as a core component of the system's design.

Evaluating and assessing risk is essential in determining the most effective security measures for an organization. The Zero Trust security model, which operates on the principle of "never trust, always verify," is a modern approach that addresses the shortcomings of traditional perimeter-based security models (Kueh, 2020). In today’s environment, where employees access applications from various devices and locations, Zero Trust provides a dynamic and flexible security framework that continuously verifies trust across every device, user, and application.

The five pillars of Zero Trust include device trust, user trust, transport/session trust, application trust, and data trust (Kueh, 2020). These form a comprehensive strategy for securing modern IT environments. For instance, device trust ensures that only known, managed devices can access company resources, reducing the risk of unauthorized access. By implementing technologies like multi-factor authentication (MFA) and endpoint detection and response (EDR), organizations can enhance their security posture while also considering the cost-benefit of these measures. While the initial investment in Zero Trust may be significant, the long-term benefits of preventing breaches and minimizing risks far outweigh the costs.

Effective security policies are the backbone of a secure IT environment. These policies should encompass core security values, coding standards, encryption, the Triple A framework (Authentication, Authorization, and Accounting), automation, and risk assessments. The MGM Resorts cyberattack serves as a real-world example of what can happen when security policies are inadequate or not enforced. To prevent similar incidents, organizations must implement strict access control policies, regular security training, and continuous monitoring.

A strong security policy should also include recommendations for adopting the Zero Trust model. By requiring continuous verification of trust and limiting access based on the principle of least privilege, organizations can greatly minimize the likelihood of data breaches and unauthorized access. Additionally, automating security processes, such as vulnerability assessments and incident response, ensures that threats are identified and addressed instantly, minimizing the potential impact on operations.

References

Abrams, L. (2024, January 1). *The biggest cybersecurity and cyberattack stories of 2023*. BleepingComputer. <https://www.bleepingcomputer.com/news/security/the-biggest-cybersecurity-and-cyberattack-stories-of-2023/>

Kueh, T. (2020, January 15). *A Practical Guide to Zero-Trust Security*. Threatpost.com. https://threatpost.com/practical-guide-zero-trust-security/151912/

Seacord, R. C. (2013). Secure Coding in C and C++ (2nd ed.). Pearson Technology Group.

https://mbsdirect.vitalsource.com/books/9780132981972