Bryce Cooperrider

CS-405

27 October 2024

Portfolio Reflection

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

Adopting a secure coding standard is vital for any organization and helps mitigate potential vulnerabilities. Organizations such as CERT stress the importance of integrating security measures from the start of development, rather than waiting until the end. Being proactive with security provides better integration and insight, leading to software that is more robust and secure. In the event of a breach, because security has been worked on from the start of development, it leads to reduced time on remediation, enabling the software to come back online faster.

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

Evaluation and risk assessment involves evaluating potential risks and assessing the cost-benefit of implementing risk mitigation strategies. One risk assessment tool such as static analysis, can identify vulnerabilities early on in the cycle, allowing the developers to weigh the cost of mitigation against the impact of a potential security breach. To give an example, while it costs a lot of time and resources to implement certain security features, the long-term investment may be worth it due to the increase of potential uptime due to already having features to mitigate against a breach. It is always important to keep in mind the consequences of a breach, with a major concern being public trust. Once the public trust is gone, it can be very difficult to build it back up.

***Zero Trust:***

Zero trust is a security model that by default trusts nothing and verifies everything. This is due to the many different devices and cloud applications that make up an organization. Traditionally, security models rely on a perimeter-based defense, meaning they only verify information going in and out of the perimeter. Zero trust instead implements multifactor authentication and continuous monitoring to ensure access to a system is controlled and limited to authorized users. Zero trust works well in a modern-day environment where users may be working from home, or want to access a system on their phone, or whatever device they’d like. It enables access as long as they are connected to the internet and provides better security than before.

***Implementation and recommendations of security policies:***

Implementing policies requires a definitive approach that encompasses clear guidelines and continuous evaluation. Each company should have security policies that are tailored to the organization’s specific needs, that address key areas such as data protection and access control. The best recommendations for implementing security policies invlude adopting best practices, implementing encryption protocols, training employees effectively, and regular security audits. Policies should also be constantly reevaluated due to the ever changing nature the technology landscape.