SNHU: CS-405 Secure Coding

Module 6 – Journal (Motivations)

Matthew Bandyk

The adoption of a secure coding standard is a fundamental aspect of any comprehensive security strategy. Waiting to address security concerns until the end of the development process is not only risky but also costly. Secure coding standards advocate for a proactive approach to security. By identifying and mitigating security vulnerabilities during the development phase, organizations can prevent security incidents before they occur.

Additionally, addressing security issues early in the development lifecycle is more cost-effective. The cost of fixing a vulnerability in production is significantly higher than addressing it during development. Introducing and implementing a security policy with coding standards provides the company with guidelines and expectations that can reduce the chances of those security issues occurring, thus, cost savings. On top of the reasoning already provided, utilizing a secure coding standard will typically integrate security into all aspects of the software development life cycle, meaning security is being considered from the planning phases through launch and maintenance.

Risk assessments are also critical components of effective security. Identifying and quantifying risks is essential for prioritizing security measures. By understanding the potential impact and likelihood of security threats, organizations can allocate resources where they are most needed. With all things though, cost will always be a concern, and not all security measures are created equal. Organizations should assess the cost of mitigation against the potential impact of a security incident. This analysis helps in making informed decisions about which security measures to prioritize. Due to this, a balancing act is created and It's about finding the right balance between security measures and the associated costs. Risk assessments and cost-benefit analyses guide organizations in finding this balance.

Zero Trust is a security model that assumes no trust, even among individuals and devices within the internal network. It's becoming increasingly important in today's interconnected and cloud-centric environments to ensure the safety of our systems and networks. It focuses on securing every user, device, and application, regardless of their location. At zero trust’s core, identity is the most important factor. Access is granted based on strict identity verification and continuous monitoring, reducing the risk of unauthorized access. Zero Trust involves continuous monitoring of network traffic, user behavior, and device health to detect and respond to threats in real-time. Users and devices are given the minimum level of access required to perform their tasks, letting this principle reduce the attack surface and limit potential damage in case of a breach.

When implementing a security policy, it should be developed in alignment with the organization's overall business objectives, compliance requirements, and risk tolerance, utilizing everything we have discussed prior when building it. It’s also not enough to just implement a security policy, as that policy isn’t what is completing the work. Policies are only effective if employees understand and follow them. Comprehensive training and awareness programs are essential. They are also not a one-and-done mechanism. They should be considered a living document that requires care and monitoring to ensure it remains effective and up to date with the changing landscape. They should be reviewed regularly and updated to address emerging threats and evolving business needs.