Jorge Torres

SNHU CS 405 Secure Coding

Journal Module 8

**Portfolio Reflection**

In my view, adopting a **secure coding standard** is essential for creating reliable and safe software right from the beginning. I believe that security should be integrated into every step of the development process, not just added as an afterthought. By building security into the code early on, we can prevent many common vulnerabilities and reduce the need for costly fixes later. This proactive approach makes the software much more robust and less likely to be exploited by attackers, which is a critical step in ensuring the overall security of our applications.

When it comes to **evaluating and assessing risks**, I think it's crucial to understand the potential threats and vulnerabilities that could impact our systems. By doing a thorough risk assessment, we can prioritize which risks need immediate attention and decide on the best ways to mitigate them. It’s important to weigh the costs of implementing security measures against the potential damage that a security breach could cause. This helps in making informed decisions that not only protect the organization but also make sense from a business perspective. Although the upfront costs of some security measures might be high, the long-term benefits, like preventing data breaches and avoiding regulatory penalties, often justify the investment.

I find the **Zero Trust** security model particularly compelling because it fundamentally changes the way we think about network security. Instead of assuming that anyone within the network is trustworthy, Zero Trust requires continuous verification of users and devices. This approach is much more effective in today’s threat landscape, where traditional perimeter-based security models are no longer sufficient. Implementing Zero Trust means adopting strict access controls and continuously monitoring activities, which helps in minimizing the risk of both internal and external threats. It’s a more rigorous and effective way to ensure that our systems and data are protected.

**Implementation and Recommendations of Security Policies**

In my opinion, having strong **security policies** is crucial for safeguarding an organization’s data and systems. These policies need to cover essential aspects like access control, data protection, and incident response. I believe it’s important to enforce the principle of least privilege, ensuring that users only have the access they need to perform their jobs. Regular updates and patches are essential for keeping systems secure and addressing any vulnerabilities that arise. Continuous monitoring is also key to detecting and responding to potential threats quickly. Providing ongoing security training for employees is another critical component, as it helps everyone stay aware of the latest threats and best practices.

Overall, I think integrating secure coding practices, conducting thorough risk assessments, adopting a Zero Trust model, and implementing comprehensive security policies are all vital for building a strong security framework. These practices not only help in protecting against various threats but also ensure that security is a fundamental part of the organization’s operations and culture.