Southern New Hampshire University

CS 405 Secure Coding

Module Eight Journal

Anaid Rodriguez

12/11/2023

**Adoption of a secure coding standard (Do not leave security to the end)**

Security is one of the most commonly overlooked steps in code development and has been consistently left “to the end” by developers. Not only is this severely bad practice, but it is highly risky to do. As the program is developed, it increases in size daily and keeping track of vulnerabilities become an increasingly harder task. Additionally, unit testing is not as simple when the source code is thousands upon thousands of lines of code. Aside from the bad practice of leaving security to the end, developers also fail to adopt a secure coding standard. A coding standard is yet another line of defense because although it itself does not provide physical defense to the system, it includes all the steps needed to add those lines of defense.

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

Mitigation is an important step in the development process once the vulnerabilities and security risks are identified. The main downfall of mitigation is the financial implications. However, if the budget is not an issue, there are not enough significant risks or issues with mitigation. In fact, mitigation can help reduce the existing damage and any future damage that might have occurred.

**Zero Trust**

Zero Trust is a modern security strategy which reinforces the idea that the system should not trust anything or anyone and should instead always verify and authenticate. This approach has proven effective because it eliminates the threat of attacks within the same network. Zero Trust also mitigates the severity of successful attacks and helps reduce the overall cleanup of those attacks.

**Implementation and recommendations of security policies**

It’s important to perform constant testing. We are increasingly becoming more dependent on technology which means innovations are not only expected but demanded. We must be prepared for new developments because with new developments come new, never before encountered threats. Additionally, do not leave any risks up to chance, always assume every single risk will be exploited and plan to defend it accordingly.