Ryan Hubbuck

10/22/2024

Prof. Alesso

CS 405

Module 8 Journal

Throughout this course, I have gained a greater understanding of the importance of adopting a secure coding standard and not leaving security to the end. Through the adoption of a secure coding standard, organizations can ensure that all security policies are defined, implemented, governed, and maintained over time. Together these factors can help reduce the chance of security vulnerabilities and improve the response effectiveness and time when situations arise. Furthermore, it is critical that security is considered in each phase of software development and is not left to the end. If security is considered during the gathering of requirements, design, development, testing, and deployment, the system will likely be far more secure, and vulnerabilities will be found and addressed quickly.

As mentioned above, considering security during requirement gathering and design will require evaluation and assessment of risk and cost benefit of mitigation. While developers can work tirelessly to reduce the likelihood of security breaches, there is always some risk of occurrence. Each security standard should be evaluated to determine the priority and likelihood of individual occurrence. By doing so, developers can then determine how to best spend their time and where to fucus efforts. Furthermore, if a breach does occur, the benefits of early reaction or waiting must be carefully considered. This includes factors such as the number of subsystems affected, the data at risk, and the potential time or money required to address the issue.

Another key element to consider is the policy of zero trust. Zero trust is a key aspect of security that can help reduce the likelihood of security breaches by restricting the number of users permitted to access specific portions of a system. In general terms, zero trust refers to a modern alternative to networks secured via firewalls in which the security perimeter is instead placed around individual users and their devices. This concept relies on the system trusting nobody and verifying everyone requesting access, regardless of their location inside or outside the network.

The final critical step is the implementation and recommendations of security policies. Every individual involved in the development and maintenance of a given system must be on the same page, and all must adhere to the same standards. Security policies are created with specific guidelines to address many aspects of the system, and it is critical that every developer is creating code with the same level of accuracy and security. Any and all recommendations outlined within the policy should be followed exactly, so that if and when a situation arises, the team can already have a plan of action to follow to reduce the potential cost.