CS405-R3362 Secure Coding

Module 8-2 Journal: Portfolio Submission

Jessica Giliam

March 3, 2024

Implementation and recommendations of security policies is paramount to running a safe environment and releasing quality products. It might seem boring, but when products are evaluated and thoroughly assessed, the number and type of vulnerabilities they can present are fascinating. There are multiple areas where developers would not think to look that can present a vulnerability. Frequently, there is also difficult to assign relevance to programs or products if they are not thoroughly understood. Thousands upon thousands of security policies exist, but it is a learned skill to know when and how to implement them for purposeful meaning to the product or company using them. A critical question to ask is if the policy is accomplishing a goal. Despite being commonly practiced, security implementations many times fall short of the goal. It is imperative to understand that there is never a “one size fits all’ security solution and each company and product require specific and unique contributions. Since the goal is often lost or not achieved, many might also believe security policies to be an obstacle or nuisance or sorts. They might have a different or faster way to do something and lose sight of why the security policy is in place. They might not understand why their way can present a problem or vulnerability. It is for this reason that security should be a constant and dynamic entity during the software development life cycle. When the environment fosters learning and betterment versus a blind rule following endeavor, the product will become only the better. Knowing the specific context in which policies take place opens doors to knowledge in all directions and allows better understanding (Karyda et al., 2005). It is also for this reason that security should be left to people with a high knowledge of security and the product or company they are working with. Managers or others with a lower technical skill set might have louder opinions of what security policies should be implemented and how, but those opinions must be met with evidence-based and intelligent responses to release a quality product. The desire to release a quality product and have a high-quality working environment is also why security must be considered during the planning phases and not left until the end. Working on a product until release only to find that no security has been implemented, coding standards were not practiced contribute to a stressful environment and force developers to go back and do redundant work that is time consuming and costly. Having security at the forefront with relevant contextualized policies and procedures can pave the road for a smooth development and release.

**References**

Karyda, M., Kiountouzis, E., & Kokolakis, S. (2005). Information systems security policies: a contextual perspective. *Computers & Security, 24*(3), 246-260. 10.1016/j.cose.2004.08.011