Andrew Laipple

Dr. Tam

CS-405

22 December 2024

Module Eight Journal: Portfolio Reflection

Today, security has to be a major concern for any company that stores information no matter how sensitive that data may appear to be. Data breaches are becoming more dangerous because we are in an age where most of our personal information is stored digitally. A single data breach can cause millions of people's personal information exposed to attackers and hackers looking to exploit that information (*The 18 biggest data breaches*, 2024). There are multiple ways for companies to combat the security issues they are facing. The first is to adopt a coding standard. SEI has put together a set of coding standards that when implemented can help to prevent common vulnerabilities within the code (*SEI CERT C Coding Standard*, 2024). As a company, a document should be drafted that should outline all of the coding standards that developers should use while creating projects and programs for the company. The SEI coding standards are great examples to use as inspiration for a company’s coding standard or implemented directly. Adopting a secure coding standard will drastically reduce the chances of data breaches happening because of code exploits.

Adopting a secure coding standard is great for the implementation phase of the software development lifecycle, but security should never be concentrated in just one phase. We are realizing more and more that security should be thought about and addressed at each phase (Seacord, 2013). One of the reasons for this is that the later in the development cycle a problem is found the more costly it is to fix (Hambling et al., 2019, p. 20). For example, if security is just focused at the end of the development cycle, if an issue is found a company may have to go back and update requirements and design documents as well as code. This will become very costly. But if security concerns were thought about at the requirements or design phase, the problem may have been found and corrected much earlier. Microsoft has developed a process called the security development cycle that provides guidance for companies to incorporate security into each cycle of the current software development cycle.

Even if programs are developed with security in mind and vulnerabilities are kept to a minimum, that doesn't mean that the program is secure. Once a program has been released there are other vulnerabilities to consider. Users that login to a system and use that system need to be authenticated so that an attacker or hacker is not let in. Once logged in, users need to be restricted in the operations they perform. Also, any actions that users perform while logged in need to be "accounted" or recorded in case a data breach does occcur the source of that breach can be investigated. These three A's make up the concept of triple-A security (Mylonas, 2018). An extension of the triple-A concept is the concept of zero trust. With a zero trust policy, instead of a more traditional view of "trust but verify" when it comes to users, the view of "never trust/always verify" is used (Kueh, 2020). This means that users need to have some form of multi-factor authentication and possibly re-verify who they are multiple times while using the system.

By adopting a secure coding standard, not waiting until the end to think about security, incorporating the triple-a strategy, and utilizing the concept of zero trust, a company can make sure they are doing everything possible to prevent security breaches in their system. These concepts should be developed and documented into a complete security policy. That way when new employees and developers are hired at a company, they can understand these concepts and incorporate them into their work. It cannot be stressed enough that companies need to focus on security today in order for our information to be protected in the future

Reference

Hambling, B., Morgan, P., Samaroo, A., Thompson, G., & Williams, P. (2019) *Software testing : An istqb-bcs certified tester foundation guide - 4th edition*. BCS Learning & Development Limited.

Kueh, T. (2020, January 15). *A Practical Guide to Zero-Trust Security*. ThreatPost. <https://threatpost.com/practical-guide-zero-trust-security/151912/>

Mylonas, L. (2018, November 27). *What is AAA security? An introduction to authentication, authorisation and accounting*. CodeBots. <https://codebots.com/application-security/aaa-security-an-introduction-to-authentication-authorisation-accounting>

Seacord, R. C. (2013). *Secure Coding in C and C++* (2nd ed.). Pearson Technology Group. <https://mbsdirect.vitalsource.com/books/9780132981972>

*SEI CERT C Coding Standard*. (2024, April 4). Carnegie Mellon University. <https://wiki.sei.cmu.edu/confluence/display/c/SEI+CERT+C+Coding+Standard>

*The 18 biggest data breaches of the 21st century*. (2024, September 12) CSO. <https://www.csoonline.com/article/534628/the-biggest-data-breaches-of-the-21st-century.html>