Jacob Griffin

CS 405 Module 8 Journal

Professor Tam

22 December 2024

**Adoption of secure coding standard and security not left until the end**

The coding standard that I would adopt is SQL Injection Prevention. The reason I would adopt SQL Prevention is because it is the easiest vulnerability for a hacker to identify. When coding, if we do not use parameters, it leaves a vulnerability that could easily be exploited by a malicious attack. For example, without having parameters for logging in, someone could use the 1 = 1 method and gain access to the account and database since 1=1 is always true. However, if we use parameters such as “username = input(“Enter username: “), the 1-1 will never be executed because it does meet the standards of the parameters identified. If SQL prevention is left until the end, the company is immediately at risk of a data breach and an attacker gaining access to the data. Furthermore, if we adopt a practice of ensuring we are always implementing parameters, we can prevent these attacks.

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

According to Bergmans, Crowdstrike, 2022, “SQL injections were the third most serious web application security risk in 2021”. The impact of an SQL attack could cause severe damage in the case of Data Breaches, Service disruption, data manipulation, etc. SQL injection is a very high probability of occurrence if the correct coding standards are not being implemented, and this raises the risk to high. As far as cost benefit of mitigation, if the code has not been written, then the correct policy just needs to be adopted to parameterize the code, but if the code is already written, it will be time consuming but not costly. However, implementing this mitigation will help prevent data breaches, and other security risks.

**Zero Trust**

Zero trust is a policy that must be implemented as it will help maintain the integrity of the system. Without zero trust, users are always at risk of an unauthorized user gaining access to their data and account, but with zero trust, it will impact users positively as it will give them the confidence that their data is secure as well as their account. Although it will positively improve security, it will impact users as far as having to use 2FA, periodically having them resign in, provide a pin to access certain data/files, but it is worth it due to the protection it provides. I think that Zero Trust is very crucial in today’s realm of cyber security due to the ever-advancing world of technology.

**Implementation and Recommendation**

Implementation of security policies is something that must be done to prevent malicious attacks. The security policy I think we should implement is input validation, sanitization of data, and lease privilege. With these three security policies we can prevent against a wide variety of attacks and deter a lot of attackers due to the complex security measures taken.

Resources

Lenaerts-Bergmans, B. (2022, October 10). *SQL Injection (SQLi): How to protect against SQL injection attacks*. Retrieved from <https://www.crowdstrike.com/en-us/cybersecurity-101/cyberattacks/sql-injection-attack/>