Ren Welck

SNHU

CS-405

6/28/2024

Journal Module 8

The adoption of secure coding is a very important step in a system and in your development of code it makes sure security is integrated in the development process from the very beginning rather than as an afterthought. The standards provide a guideline to follow that helps teams write code that has less security vulnerabilities and allow for better protections against common attack vectors like SQL injections and buffer overflows.

Risk evaluation and cost-benefit analysis are helpful and effective at helping determine an effective security strategy. It allows you to identify potential threats and assess the likelihood of them happening and the impact they would have on a business and determine the most cost-effective way to mitigate them. There is a balance between the cost of security measures and the cost of security breaches because if it isn’t likely to happen then why spend tons of money on protecting against it.

Zero trust is a security model based on the principle of “never trust, always verify.” This assumes threats can come from both outside and inside the network, therefore no user or device should be trusted by default. Instead access to resources is granted based on continuous verification of the user’s identity and the security of their device. Effective security policies for protecting an organization define the rules and procedures for managing and securing data, systems and networks and implementing them involved creating the police and making sure they are taught to all employees and following up with all employees to make sure they know them.

# References

Dunham, R. (2020, May 5). *Information Security Policies: Why They Are Important To Your Organization*. Retrieved from Linford and co: https://linfordco.com/blog/information-security-policies/

Murray, A. (2020, June 13). *Secure Coding: A Practical Guide*. Retrieved from mend.io: https://www.mend.io/blog/secure-coding/