Southern New Hampshire University

CS405 – Secure Coding

Tek Bista

Date: 04/24/2021

Journal: Portfolio Reflection

Secure coding is nothing but the development of highly secure software application capable of withstand vulnerabilities. Adoption of a secure coding standard is the way to find and remove vulnerabilities that could be exploited by cyber criminals. Developing secure code means reducing the probability of getting the system hacked or illegal access to the system and application. Leaving security at the end would be difficult to detect error, bugs and vulnerability in code and there might be the high possibility of causing damage to the system or application. So, it is critical to check security flaws, errors, and bugs at the early stage of software development.

Security risk assessment is the process to identifying and evaluating risks for assets that could be affected by cyber-attacks. Basically, risk assessment identifies both internal and external threats and evaluate their potential impact on data availability, confidentiality, and integrity. It also estimates the cost of suffering a cybersecurity incident. With this information, we can tailor our cybersecurity and data protection controls to match our organization’s actual level of risk tolerance. It measures the risk ranking for assets and prioritize them for assessment and also apply mitigating controls for each asset based on assessment results (Security Risk Assessment, 2021).

Zero trust is a security concept centered on the belief that organizations should not automatically trust anything inside or outside its perimeters. Instead, they must verify everything about the user while trying to connect to the system. Never allow access to IP address, machines, systems or applications until you know who the use is and whether he/she is authorized to use that system. It is the best approach to secure applications, networks, and data.

Implementation of security policy is harder than the creation of the policy itself because it involves coaching and educating the staff to behave in a secure manner, following each of the core elements listed in the security policy. As I understand from this course, Zero Trust is only the security policy that could protect your network, system, server, and data from being hacked. It relies on various existing technologies and governance processes to accomplish its mission of securing the enterprise IT environment (Pratt, 2018). It draws on technologies such as multifactor authentication, IAM, orchestration, analytics, encryption, scoring and file system permissions.

# References

Pratt, M. K. (2018, 01 16). *What is Zero Trust? A model for more effective security*. Retrieved from CSO: https://www.csoonline.com/article/3247848/what-is-zero-trust-a-model-for-more-effective-security.html

*Security Risk Assessment*. (2021, 04 22). Retrieved from Synopsys: https://www.synopsys.com/glossary/what-is-security-risk-assessment.html