Felicia Schenkelberg

Professor Moscon

CS-405-X6390

22 July 2021

8-2 Journal: Portfolio Reflection

In this assignment, I will reflect on and include a discussion of the following topics, using readings from throughout the course to support my views.

1. Adoption of a secure coding standard, and not leaving security to the end.

There are many things to consider When writing code. One main thing is the Adoption of a secure coding standard. Making sure the code is secure will

prevent many cyberattacks by removing vulnerabilities on which many exploits are based. a set of guidelines, as list by Robert Seacord is as follows:

* **“Validate input.**
* **Heed compiler warnings.**
* **Architect and design for security policies.**
* **Keep it simple.**
* **Default deny.**
* **Adhere to the principle of least privilege.**
* **Sanitize data sent to other systems.**
* **Practice** **defense in depth.**
* **Use effective quality assurance techniques.**
* **Adopt a secure coding standard” (**Seacord, 2018**).**

1. Evaluation and assessment of risk and cost benefit of mitigation

Threat and risk modeling procedures identify potential risks to the system. In this way, threat levels are reduced or even blocked. For example, sensitive data might be cached by proxies. As a principle, limit the information sent to what is necessary to mitigate risks.

1. Zero trust

“Never Trust/Always Verify.” In practice, this model considers all resources to be external. Once trust has been established, the decision can be made to grant or deny access. Once a decision has been made to grant access, it is necessary to monitor it continuously. If the level of trust changes, organizations must be able to act immediately.

1. Implementation and recommendations of security policies

The purpose of an information security policy is to guide the behavior of employees in relation to the security of company information. Without an information security policy, the organization's information assets are susceptible. It is important to consider the principles of the CIA triad when developing corporate information security policies. Security policies need to reflect the companies' risk tolerance. The policy should manage risk mitigation.

Citations

Seacord, R., & Schiela, R. (2018, February 5). Top 10 Secure Coding Practices. Carnegie Mellon University. Retrieved from https://wiki.sei.cmu.edu/confluence/display/seccode/Top+10+Secure+Coding+Practices?focusedCommentId=88044413