Richard Chang

Professor Demory

CS 405

4/17/2023

8-2 Journal: Portfolio Reflection

Throughout this course I have learned about the importance of secure coding practices and the need to adopt a secure coding standard from the beginning. I see that the lack of security brings security breaches, irreparable damage to businesses and organizations, economic loss, loss of trust, hack attacks, privacy infringement and more. Coding standards help to set guidelines and rules to reduce security vulnerabilities and errors during development. Not leaving security to the end means not adding security features at the final stages of the project. DevSecOps (security with DevOps) has two cycles: pre-production and production. Both cycles bring a standard of security that helps to design, build, test, maintain, and stabilize the application.

To build security measures, I need to assess the risk and cost benefit of mitigation. With consideration of any security incident that may occur, implementing different security measures is costly to the organization. I learned to balance a level of security with the number of resources and funds. I take consideration in defense in depth, which is a new term to me. Defense in depth means to build layers and layers of security measures. If one layer of security fails another one may prevent a threat.

Zero trust is a security model that assumes no user or device should be trusted by default and requires continuous verification of their identity and authorization. A negative impact of zero trust is that adding security brings more complexity and time-consuming factors to the organization. The world is constantly evolving in technology. Because times have changed, people can access confidential data and networks through various devices and away from corporate office spaces. Security is harder to protect these alternative approaches these days.

Implementation of security policies is critical to maintaining a secure environment. Policies must follow the needs of the organizations rules and regulation. Depending on what are the organization’s policies and where the Corporation Headquarters resides and how the overall business models, the type of security defenses varies from one to another. Some may want to incorporate firewalls and yet some want to track HTTP traffic load balancers. Overall, the most initiative-taking approach is to build an application with security with cooperation from the technology team and more.