Ashli Campbell

CS 405

Southern New Hampshire University

8-2 Journal: Portfolio Reflection

**This is your final course reflection as well as your portfolio submission. Reflect on and include a discussion of the following topics, using readings from throughout the course to support your views.**

* **Adoption of a secure coding standard, and not leaving security to the end**
  + Security is so important to each level of development that it should be factored into decision-making from the very start of the project. Best practices in programming and coding include utilizing security methods and keeping it top-of-mind every step of the way. For example, each programming language has its own set of security techniques to implement, but there are also practices that apply to any language that a programmer should use. Security of sensitive information and assets helps to guide developer’s choices and to follow best coding practices throughout development.
* **Evaluation and assessment of risk and cost benefit of mitigation**
  + Mitigating risks will ensure that the projects run smoothly. This will benefit the company by earning customer’s trust, staying within budget, which keeps the customer happy and continues to build trust, and staying within the allotted timeframe, which again keeps the customer happy, along with allowing the company to continue taking on projects and increasing revenue. Waiting to test for vulnerabilities or not taking acting can slow things down and cause the company to spend valuable resources and time that could be allotted to other projects.
* **Zero trust**
  + Zero trust essentially means that instead of deeming devices inside of the network as good and devices outside of the network as bad, you deem all devices untrustworthy to prevent a hacker from infiltrating someone’s device and gaining access to the network. This involves using multi-factor authentication (MFA) instead of just a username and password or two-factor authentication. This also includes safeguards like disconnecting after a certain length of inactivity, re-authentication for certain actions, and not allowing auto-logins. Another strategy that goes hand-in-hand with zero trust is the method of least privilege, where users are only granted access to the things they need to have. This ensures that a compromised account has a limited amount of potential damage.
* **Implementation and recommendations of security policies**
  + It is critical that everyone remains in sync with the principles and best practices in their company’s security policies. This applies to all staff that create, deploy, or support custom software. Software development requires consistent implementation of secure principles to all applications. Not only should developers adhere to the principles and standards in the security policy, but they should make use of unit testing to catch vulnerabilities and weaknesses in their code early and often.