Alex Bevz

Module 8 Journal – Portfolio Reflection

CS-405-T4538 Secure Coding 22EW4

Southern New Hampshire University

April 24, 2022

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

It is important to adopt a secure coding standard so that there is consistency in how security is handled among team members and projects. It is much more beneficial to add in the security aspect concurrently as the code is being developed. The development team should constantly test and improve how their program performs to ensure that there is a low risk of the program being compromised by hackers. Adopting a secure coding standard at the foundation level shows that the company takes security very seriously, which will help to uphold the security standards from the top executive level and down to the staff level employees. If staff level employees see that their senior management are large proponents of security, then the staff level employees will also be more inspired to follow suit.

* **Evaluation and assessment of risk and cost benefit of mitigation**

It is important to know what kinds of risks to anticipate and ways to mitigate them so that you can handle them better when incorporating security into your code. Running through the various security breach scenarios and staying up to date on all latest news will help the company be better prepared against the types of attacks the current hackers are implementing and will help the company to identify possible weak spots much easily in their security architecture. There is also the cost aspect where fixing a potential breach down the road is going to cost a lot more as opposed to catching the issue before the release of the software. If a company discovers a major security flaw in their software after deployment then it will probably require more teams and resources to fix the problem, not to mention the downstream impact to the end users of the software, who will likely experience some down time while the security patch is being deployed. This may hurt the company’s reputation and may result in users switching to a competitor’s product if they are dissatisfied with the security performance of the software.

* **Zero trust**

It is important for a company to adopt a zero-trust security policy to maximize its overall security effectiveness. This security approach assumes that no user can be trusted and will verify credentials for all users the same way to ensure consistency and authenticity of users. It doesn’t matter if the user has accessed the system a hundred times previously. The zero-trust policy will look at this user as though they are accessing the system for the first time. This type of policy is beneficial to both the company and the user. It protects the company from any unauthorized access while protecting the user from having their credentials stolen and used to access a user’s personal account and information. Companies should implement zero-trust protocols in their cybersecurity policies and procedures to ensure that its vital infrastructure is secure from any malicious users.

* **Implementation and recommendations of security policies**

A company should have an effective and up-to-date security policy that outlines the expectations that the company has for its employees. This way both the leadership and staff level employees are on the same page. The company should have security policies and procedures for its software development, for its operations, and for its employees. The software development security policies will list the security principles and the coding standards specific to the coding language being utilized by the company. The operational security policies should outline defense in depth policies on how the company intends to protect itself both physically and in terms of its cybersecurity. The employee security policy should outline how the company’s employees should conduct themselves to promote security, such as to not let unauthorized individuals into the building and to not open attachments of a suspicious email. Together these policies will promote an effective security atmosphere within the company and will ensure that any potential breaches are minimized.