Jonathan Ramirez

Module 8 Journal: Portfolio Reflection

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

As a best practice in secure coding, the phrase “Don’t leave security to the end.” means that security coding practices should be implemented from the start of the software development life cycle. It should not be something that should be ignored until the very end or even worse, something that should not be ignored until a breach happens and the harm is done.

The first step I can take to prevent threats is by starting with the requirement. What type of threats can arise from going through the requirements. Are they financial threats, user data threats, company data threats or threats that could cause harm to human life. After finding the type of threats that can arise from unsecure software based on the requirements, unit tests should be created and be performed on the code from the start of development of code until the very end. Also, more unit testing should be done on areas where it may cause the highest level of threats like human lives.

One example of how to I plan to ensure that security is addressed intrinsically and not left until an issue is discovered is by having everyone working on the project to adhere to the company’s coding standards to increase consistency and readability of code. This will make everyone write consistent code quality that will be easier to find errors, reduce complexity and maintain the code.

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

Leaving security to the end or even failing to implement security throughout the life cycle is a top reason why identify theft happens as well as fraud and data leaks. The costs to mitigate these vulnerabilities, especially when they have already happened, are very high compared to if secure practices were implemented throughout the life cycle. To make matters worse, some of these costly incidents are caused by simple vulnerabilities that could have easily been fixed.

**Zero trust**

Zero trust is the idea of logging and inspecting all network traffic within an organization, limiting, and controlling access to the network, and verifying and secure resources like data and user login information. This ensures that everything that happens within the organization is being monitored and checked for any suspicious activity. There really is no one to trust when it comes to protecting a company’s data and intellectual property.

I feel like knowing a hacker’s motivation will help me adopt more secure coding standards. This will also enforce the concept of Zero Trust. With the many reasons why hackers hack, for money, make a point, disrupt services, steal information, etc. Makes me realize that no one should really be trusted either from outside a company or within. It is not about trusting your most trusted colleague, it is about keeping the data secure and with zero trust, this can be accomplished.

**Implementation and recommendations of security policies**

No program is 100% protected from vulnerabilities. There are always new threats emerging, so emerging threats should be analyzed and provide mitigation strategies accordingly. One example is to keep updating a company’s security policy. Also, software teams should be educated in what security is and how to apply best practices such as security principles into their code.

**References**

* IBM.What is zero trust?.IBM. <https://www.ibm.com/topics/zero-trust>
* Agarwal, H. (May 2018).5 Key Reasons Why Do hackers Hack?.appknox. <https://www.appknox.com/blog/why-do-hackers-hack>
* ACM Code 2018 Task Force. 20218.ACM Code of Ethics and Professional Conduct. Association for Computing Machinery. <https://www.acm.org/code-of-ethics>
* Sweet, C.(2007).Dont’s Leave Security for Last. Software Test Professionals. <https://www.softwaretestpro.com/dont-leave-security-for-last/#:~:text=Failing%20to%20integrate%20security%20throughout%20the%20lifecycle%20is,defacements%20and%20fraud%20we%20read%20about%20almost%20daily>.
* Kleidermacher, D.(March 2012). Enhance system security with better data-at-rest encryption.Enbedded. <https://www.embedded.com/enhance-system-security-with-better-data-at-rest-encryption/>