Evelyn Pinarello

CS405-T4240

Module Eight Journal

April 17, 2023

As technology continues to develop and evolve, technological security must also develop and evolve to protect increasingly vulnerable data and systems. Implementing the secure best coding methods in the first venture in securing vulnerable data and mitigating security risks. SEI CERT has ten main secure coding practices that should be implemented into every coding project or program (Seacord, 2018). Some of these practices, such as “validate input” and “heed compiler warnings” suggest that security measures should be implemented throughout the creation of the project and not left at the end of the project development. Using secure methods throughout the coding process creates a more cohesive and secure code with less vulnerabilities because it enables a programmer to implement security measures as they are writing the program as opposed to trying to find issues and vulnerabilities as an afterthought.

With any technology, there are vulnerabilities and security risks. Evaluating the security risks and vulnerabilities of each project is the strongest method to mitigate said project’s risk. Using the risk assessment of each SEI CERT rule or recommendation is a beneficial tool to determine the risk and mitigation methods of each vulnerability. It is also important to determine the cost benefit of mitigation security vulnerabilities. Overall, the cost of implementing proper security measures will be miniscule compared to the financial damage these vulnerabilities can pose.

Another security measure that should be implemented is the zero trust security method, which is a framework that authorizes the user to access the organization’s systems and data regardless of whether they are currently in the organization’s secure network (What is Zero Trust?, n.d.). This helps support the Triple A framework of security and ensures that those accessing data have authorization to do so.

Overall, implementing various security measures would be the most effective method to creating a secure project. The Defense in Depth, Triple A framework, and Zero trust security methods will work together to create cohesive and balanced security measures that provide as much risk mitigation as possible. These methods, coupled with adopting the secure best coding methods and implementing security throughout, and not as an afterthought, will help ensure an organization’s data and users are protected and secure.

References

Seacord, R. (2018, May 2). *Top 10 secure coding practices*. Top 10 Secure Coding Practices - CERT Secure Coding - Confluence. Retrieved April 17, 2023, from https://wiki.sei.cmu.edu/confluence/display/seccode/Top+10+Secure+Coding+Practices

*What is Zero trust?* IBM. (n.d.). Retrieved April 17, 2023, from https://www.ibm.com/topics/zero-trust