Laynie Tierney  
CS-405-R4888

28 April 2024

8-2 Journal: Portfolio Reflection

Introduction:

Throughout this course, I have delved into various aspects of cybersecurity, including the adoption of secure coding standards, risk assessment, the concept of zero trust, and the implementation of security policies. In this reflection, I will discuss these topics and provide insights based on the readings and discussions I have had in the course.

Adoption of Secure Coding Standards:

One of the key takeaways from the course is the importance of adopting secure coding standards right from the beginning of the software development lifecycle. Secure coding practices are essential for mitigating vulnerabilities and reducing the risk of security breaches. By incorporating security into the development process from the outset, organizations can proactively address potential threats and ensure that security is not an afterthought.

Evaluation and Assessment of Risk:

Risk assessment plays a crucial role in cybersecurity strategy. It involves identifying potential threats, assessing their likelihood and impact, and implementing mitigation measures to reduce risk to an acceptable level. Throughout the course, I have learned about various risk assessment methodologies and tools that can help organizations evaluate and prioritize security risks effectively. By conducting thorough risk assessments, organizations can make informed decisions about allocating resources for security measures and implementing cost-effective mitigation strategies.

Zero Trust:

The concept of zero trust represents a paradigm shift in cybersecurity, advocating for the principle of "never trust, always verify." In a zero trust model, access to resources is granted based on continuous authentication and authorization, regardless of the user's location or network. Zero trust architecture helps organizations strengthen their security posture by minimizing the attack surface and mitigating the risk of insider threats. By implementing zero trust principles, organizations can better protect their assets and data from unauthorized access and cyberattacks.

Implementation of Security Policies:

Effective implementation of security policies is essential for maintaining a strong security posture within an organization. Security policies define the rules, procedures, and guidelines that govern how security measures are implemented and enforced. Throughout the course, I have discussed the importance of developing comprehensive security policies that address various aspects of cybersecurity, including access control, data protection, incident response, and compliance. By establishing clear security policies and procedures, organizations can ensure consistency in security practices and mitigate the risk of security breaches.

Conclusion:

In conclusion, the adoption of secure coding standards, effective risk assessment, implementation of zero trust principles, and the development of robust security policies are critical components of a comprehensive cybersecurity strategy. By integrating these elements into their cybersecurity practices, organizations can better protect their assets, data, and infrastructure from evolving cyber threats.

References:

Amarasinghe, H. (2022, August 1). *SSDLC - tryhackme walkthrough*. Medium. <https://hasanka-amarasinghe.medium.com/ssdlc-tryhackme-walkthrough-1a22960cae0b>

Irei, A., & Shea, S. (2022, October 20). *What is the zero-trust security model?*. Security. <https://www.techtarget.com/searchsecurity/definition/zero-trust-model-zero-trust-network>

Sotnikov, I., & Ilia Sotnikov

Ilia Sotnikov is Security Strategist & Vice President of User Experience at Netwrix. He has over 20 years of experience in cybersecurity as well as IT . (n.d.). *The importance of security risk assessments and how to conduct them*. The Importance of Security Risk Assessments. <https://blog.netwrix.com/2023/08/04/it-risk-assessment/>

Squirrel, S. the S. (2024, February 9). *What is information security governance in cybersecurity?*. Kiteworks. <https://www.kiteworks.com/cybersecurity-risk-management/security-governance-in-cybersecurity/>