Jacob Casas

CS-405

03/03/24

8-2 Journal: Portfolio Reflection

Ignoring security is like constructing a house on flimsy foundations: eventually, weaknesses will show through and require expensive repairs. Using secure coding practices from the start lays a solid basis for reliable systems. Susan Morrow, a tech journalist for vpnoverview states “The adoption of secure coding practices is important because it removes commonly exploited software vulnerabilities and prevents cyberattacks from happening.” These standards minimize possible vulnerabilities and promote secure coding methods by offering advice for typical errors. They also promote efficiency and uniformity throughout the development team, which enhances communication and makes the process of developing software safer.

But there is a cost associated with security measures. A comprehensive risk assessment is necessary to strike a balance between resource allocation and security effectiveness. In this process, possible risks and vulnerabilities are identified, their effect is estimated, mitigation strategies are assessed, and a cost-benefit analysis is carried out. Setting risk priorities according to likelihood and severity is essential to make sure resources are allocated to the most important areas.

Conventional security models frequently depend on trust boundaries, presuming that everything is secure inside a perimeter. On the other hand, Zero Trust follows the tenet of "never trust, always verify." Regardless of the user or device, this method necessitates constant authorization and access verification. Zero Trust minimizes the attack surface, provides quicker detection and reaction to security problems, and continually verifies requests. Zero Trust implementation, however, can be difficult and necessitate adjustments to network architecture, infrastructure, and access controls. Furthermore, striking a balance between improved security and a flawless user experience is critical.

Lastly, thorough security regulations offer a precise foundation for safe actions and judgment. These policies provide appropriate system usage, password management techniques, incident reporting methods, and data handling protocols. They include appropriate Use, Password, Incident Response, and Data Security policies. Robust security postures are eventually achieved through a culture of security compliance that is fostered by clear and succinct policies, continuous communication, and enforcement.

Resources

Morrow, S. (2023, August 22). *What is secure coding and why is it important?*. VPNOverview.com. https://vpnoverview.com/internet-safety/business/what-is-secure-coding/#:~:text=Secure%20code%20will%20help%20to,Software%20vulnerabilities%20are%20rampant.