8-2 Journal: Portfolio Reflection

CS-405

Grant Sorenson

6/30/2024

Security is extremely important to the success of a product because it ensures data is secure and users are protected. The adoption of a secure coding standard improves security by increasing the quality of code created and maintaining a consistent level of security across the system. Not leaving security to the end relates to this because the development team should have security in their mind while developing the entire product. Security must be implemented throughout the system at a consistent quality in order to maximize its effectiveness. In an article titled “Shifting Left on Security”, DORA describes how high performing teams spend %50 less time remediating issues than low performing teams because the optimize security by implementing it early(2024). While looking for vulnerabilities, it’s important to evaluate and assess the risk it poses to the system. Organizing risk by priority will make it easier to examine the cost benefit analysis for fixing a vulnerability. high risks that severe ramifications will be prioritized over lower risk vulnerabilities. Having accurate evaluation techniques provides the security team with a direction on where security components could be added or improved. Zero trust is an important policy that should be applied to the system. Every user should be considered a possible attacker, and the system should be built around that mentality. For example, if the system wants evaluate the trust level of a user, what components are needed? A few popular ones include password based authentication, multi factor authentication, and certificates. Once these have been established the system can trust that the user is legitimate. Policies like Zero Trust are important to implement because they actively protect the system from attackers and give developers areas in which to advance security systems and expand their functionality(Kueh, 2020). The implementation and recommendations for security policies can be difficult at times. If security will cost money through labor or services, the individuals in charge of providing that money may not understand why they are needed. Creating an effective security policy presentation that makes it easy for them to understand is essential to maintaining transparency. Security policies should be updated as new vulnerabilities are found or common attack vectors located. Overall this course has taught me a lot about secure coding and the various ways it can be implemented correctly. I hope to use some of these practices in my career and work to uphold and improve security standards.

Sources:

*DORA | DevOps Capabilities: Shifting Left on Security*. (n.d.). Dora.dev. Retrieved June 30, 2024, from <https://dora.dev/devops-capabilities/process/shifting-left-on-security/>

Kueh, T. (2020, January 15). *A Practical Guide to Zero-Trust Security* [Review of *A Practical Guide to Zero-Trust Security*]. Threat Post; Threatpost. https://threatpost.com/practical-guide-zero-trust-security/151912/

‌

‌