8-2 Journal

Paloma Rodriguez

CS-405 Secure Coding

December 12th, 2023

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

Our foundation is built on the practice of secure coding, ensuring that the software we create is safe, strong, and protected. When we adopt a secure coding standard, it means we include security practices throughout the entire process of creating the software. We move away from thinking about security only at the end, and instead we make it a part of the whole development process. This method fits well with the idea of "shift left," which means we pay attention to security issues early on and work on fixing them. The idea of including security early on is supported by widely accepted practices in the industry and frameworks like OWASP. OWASP highlights how important it is to think about security right from the start of the software development process. Security isn't something we think about just once, it's an ongoing thing. Training and awareness programs for developers, along with resources like secure coding guidelines are crucial in making sure everyone prioritizes security. Secure coding standards are made to deal with common issues that could make software vulnerable, like injection attacks, buffer overflows, and insecure dependencies.

Evaluation and assessment of risk and cost benefit of mitigation:

Managing risks includes the steps of identifying, assessing, and prioritizing potential problems. Methods like FAIR help us in measuring risk, making it simpler to prioritize efforts to minimize risks based on how likely they are to happen and how impactful they might be. Analyzing the costs and benefits is crucial for deciding if security measures are practical and effective. Economic models and frameworks for assessing risks, as discussed in literature, offer guidance on wisely allocating resources to reduce specific risks. Successful risk management means connecting security investments with the goals of the business. By understanding how security incidents might affect the business, organizations can better prioritize and justify their spending on security measures.

Zero Trust:

The zero trust model questions the traditional way we secure things by having a strong boundary. zero trust stresses the idea that we should always check and never assume anything is safe in today's environment. In zero trust, keeping a constant eye on what's happening is crucial. Readings emphasize the need to always know what's going on in the network and having plans ready to deal with any problems quickly.

Resources:

https://books.google.com/books?hl=en&lr=&id=0cuNAgAAQBAJ&oi=fnd&pg=PP1&dq=security+development&ots=MIRlqzphaw&sig=9w6A3nyJddoUeS2aEHgCwpQVEL0#v=onepage&q=security%20development&f=false

https://www.cloudflare.com/learning/security/threats/owasp-top-10/

https://www.cio.com/article/643767/whats-the-state-of-zero-trust-security.html

https://www.exabeam.com/explainers/information-security/defense-in-depth-stopping-advanced-attacks-in-their-tracks/