Carmen Kingery

Secure Coding

Olga Mill

Module 8 – Journal

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

Reflecting on the course, the adoption of a secure coding standard from the start of a project is fundamental to software development. This preemptive approach, where security is an integral part of the development lifecycle, greatly reduces the chances of vulnerabilities. It also cultivates a security-first mindset among developers. By embedding security practices from the beginning, we ensure that security isn't just a final checklist item but a core aspect of the development process.

*Evaluation and assessment of risk and cost benefit of mitigation*

The course also highlighted the importance of evaluating and assessing risks, coupled with a cost-benefit analysis of mitigation strategies. This process is key to understanding the potential impacts and likelihood of security threats, which in turn helps in making informed decisions about where to invest in security measures. Effective risk management is not about eliminating all risks but rather managing them in a way that balances security with functionality and usability. It's a strategic approach to prioritize and allocate resources effectively, focusing on the most critical areas first.

*Zero trust*

Discussing the Zero Trust model revealed its growing relevance in today's security landscape. This model, based on the principle of “never trust, always verify”, is a shift from traditional perimeter-based security. It recognizes that threats can arise from anywhere and that trust should not be implicit. Implementing Zero Trust involves rigorous identity verification, least-privilege access, and continuous monitoring, which are essential in a world where security perimeters are no longer defined by physical locations.

*Implementation and recommendations of security policies*

Finally, the course underscored the significance of implementing and regularly updating security policies. These policies provide a framework for action and decision-making within an organization, setting clear guidelines and expectations. They should be comprehensive, enforceable, and adaptable to new threats and organizational changes. Effective security policies cover various aspects, including data protection, incident response, user access, and more, ensuring that an organization's security practices are robust and responsive to the evolving digital environment*.*