Monticia Dunn

CS-405 Module Eight

4/22/23

**Module Eight Journal: Portfolio Reflection**

An essential practice for building secure software applications is adopting a secure coding standard. Something that has been reiterated throughout this course is the importance of not making security an afterthought, therefore developing a secure coding standard ensures from the beginning that security will be integrated in the development process. This has many benefits including preventing security flaws, improving system quality, and protecting against emerging cyberthreats.

It's important for an organization to perform a risk evaluation and assessment so they know what kind of cyberthreats to anticipate and prepare for. Along with this the organization must weigh the cost benefits of risk mitigation to evaluate if the cost of implementing mitigation techniques is worth the potential benefits. Not every potential threat I worth the time and money investment to mitigate it, which is why it’s important to perform these assessments so resources are allocated appropriately.

Another concept used throughout the course was the Zero Trust policy, the assumption that every user, device and connection to the system is a threat and the system should be prepped accordingly. This also goes hand-in-hand with the Defense-in-Depth policy, that covers multi-layered security. It’s important to have multiple layers of security and one of the most crucial layers is within the authorization and authentication process. If we’re going to have zero trust of anyone/anything accessing the system then we must verify their identity and only allow the most minimal authorization necessary for the user based on the verified identity. This helps reduce the impact of any potential security breaches and makes it much harder for an attacker to gain access to more sensitive data.

All in all, the security policy can only provide recommendations for how a system should implement security measures, it’s up to the company to enforce the implementation for the system. Implementing a security policy is only the start, security policies must also be amended and adapted over time as cybersecurity is an ever-growing field with new cyberthreats introduced daily.