Module Eight Portfolio Reflection

CS 405

Miranda Putnam

The statement “Don’t leave security to the end” means that security should be considered in all aspects of a software, program, business, or organization from the very beginning so as to avoid any security blunders down the line when it’s too late. Secure coding uses this best practice to ensure that security is always at the forefront when designing anything from code, new software or programs, or a business. If the system is secure from the get-go, it can avoid costly and damaging security risks and breaches down the line had security not been considered and implemented in every aspect. It is also more difficult to implement secure practices later on once the system has already been put together, so it’s best to not leave security to the end. There are many steps you can take to prevent security threats within a system. First and foremost, follow the best practice of considering and implementing security from the start. Next, don’t collect any unnecessary personal information, as it poses a risk that could simply be avoided by not collecting and keeping this information. “No one can steal what you don’t have”, says the FTC (*Start with security: A Guide for Business*, 2021). Another step to prevent security threats is to limit accessibility and administrative use, as well as implementing authentication practices (*Start with security: A Guide for Business*, 2021). Companies should also keep sensitive information secure throughout its lifecycle and during transmission (*Start with security: A Guide for Business*, 2021).

It is also vitally important to create and adopt a secure coding standard to follow as you create and build code and systems. This ensures that all personnel who are responsible for creating and maintain code have standard with which to measure by and follow, which in turn creates consistent and secure code and systems.

It is also important to assess potential security risks to your system, and what it will cost to mitigate those risks. One main risk to every system is the threat of breaches and hackers. It is important to understand their motives and strategies in order to best protect your system. Some of these motives include money, challenge, revenge, and infamy, among others (Khagram, 2017). First, money is a primary motivation for many hackers, as they can gain access to and hold data and information hostage until ransom is paid. Second, some hackers attack for the challenge of it, trying to prove they can break into an unbreakable system and gain notoriety for it (Khagram, 2017). Next, revenge is often a motivation of some hackers; They use their anger and retaliate against individuals, a group, or a company in order to get revenge (Khagram, 2017). Lastly, many hackers are motivated by the prospect of infamy and ability to boast about their achievements to others (Khagram, 2017).

While it might cost more money, time, and resources to implement security from the start and to maintain a highly secure system, the pros outweigh the cons. Ignoring security best practices and failing to implement them can lead to attacks later on that will then be more difficult to mitigate, likely leading to more money spent and more time spent to then implement security later on. Attacks due to lack of security may also lead to damage of reputation and loss of clients and business.

Zero trust is also an important security measure to adopt when creating and maintaining a system. This approach ensures that no one user is 100% trusted, and implements multiple layers of authentication and verification to ensure the system remains secure even when a user is given access to a system. This also may require more time and resources to implement and maintain, but in the long run will avoid disastrous attacks and ramifications from those attacks. This policy may also change user experience by requiring more authentication methods throughout the use of their account, but as long as the user understands it is all being done to protect their data, this should not deter anyone from utilizing the zero trust approach.

Overall, I highly recommend creating, adopting, and adapting a security policy, implementing security from the start, understanding and adapting to security risks, and implementing the zero trust policy. Each of these will ensure that a business is doing everything in their power to ensure their system remains secure, as well as their customers data. This will lessen and even prevent attacks from occurring, as well as gain consumer trust and build the company a reputation that is based on security.

**References**

Khagram, A. (2017, March 2). *The motivations of a Hacker*. swcomms. Retrieved February 12, 2022, from https://www.swcomms.co.uk/blog/article/the-motivations-of-a-hacker

*Start with security: A Guide for Business*. Federal Trade Commission. (2021, December 1). Retrieved February 7, 2022, from https://www.ftc.gov/tips-advice/business-center/guidance/start-security-guide-business