Throughout this course, I have learned a great deal about the importance of making security a priority instead of leaving security to the end. Adopting a secure coding standard is essential to ensure you’re a developing code that is as secure as it can possibly be. It is essential to be compliant with secure coding standards from the start because if you leave security to the end, you are leaving your software and systems vulnerable to security threats.

It is important to note that each security threat is not created equal and the security threats of today are not necessarily the security threats of tomorrow. When a new security threat is identified it should be analyzed to get as much information as possible before creating a plan to combat the threat. By assessing the level of risk a certain security threat may pose to your software or system and weighing it against the benefits of mitigation, you can organize threats by levels of severity. The security threats that pose the most severe risks should be mitigated first and the rest should follow. Also, as time goes on, new threats are identified as technology changes and hackers develop new methods. It’s important to regularly check for security threats and develop a plan for dealing with them as soon as possible.

Zero trust as a security best practice is an excellent security policy that will help maintain the security of software and systems. By not trusting anyone, users are required to regularly authenticate their credentials using multiple factors of authentication. Also, by implementing zero trust, all users are treated like untrusted individuals until proper authentication has been performed. This means avoiding creating and assigning roles to users with different levels of access since everyone is treated the same. As a user, I sometimes get slightly annoyed by repeatedly authenticating my credentials using multiple factors of authentication, but it truly is a small price to pay in order to protect your software and systems from unauthorized access.

Creating, maintaining, enforcing, and reviewing a comprehensive security policy is absolutely essential in today’s digital world. Software development regularly involves the implementation of new frameworks and technologies, and a strong security policy will adapt to include these updates. Also, as technology continues to advance, cyber criminals are developing new methods to gain unauthorized access to software and systems and a strong security policy will address these new methods.

References

Kueh, T. (2020, January 15). *A practical guide to zero-trust security*. Threatpost English Global threatpostcom. Retrieved December 17, 2021, from https://threatpost.com/practical-guide-zero-trust-security/151912/

Cisco Netherlands. (2019). *How Zero Trust improves security and the user experience*. *YouTube*. Retrieved December 17, 2021, from https://www.youtube.com/watch?v=-Why\_ZjJUhg.