Zachary Nicholas

August 21, 2024

CS-405 Secure Coding

Module Eight Journal

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

This is an important topic to consider, especially during the development of a program or app as if planned out beforehand the cost of integration for security is much less than what it would be if it had to be reconfigured later to incorporate the security necessary.

* Evaluation and assessment of risk and cost benefit of mitigation

Looking at different breaches that have happened can give us a sense of what we should be thoughtful of, for instance the Yahoo data breach that saw 3 billion accounts be compromised over the span of 3 years, the breach included the names, email addresses, date of birth, and telephone numbers, one of the good things that happened with this breach is that none of the passwords were revealed as they were hashed. The thing that we should look at from this is making sure that our data from users and data that the application uses is properly encrypted and protected against potential breeches, another thing that was important was SQL injection which would provide all or a lot of this same information if not properly protected against.

* Zero trust

With zero trust, it assumes that all connections that are made are bad until they are fully verified, this is especially important as more workplaces move to work from home and cloud based computing as a lot of different connections are made and need to be properly verified so that a potential bad actor(s) from gaining access to a company’s secure system.

* Implementation and recommendations of security policies

Security policies are important to consider as they are the backbone of how security will be implemented and how each developer will use them to make a secure app or program. This comes with identifying the risks that our company or app would face by potentially leaving security till last or making it not as important as it should be, it also allows us to make sure we are meeting regulatory requirements if they are needed such as HIPAA and Sarbanes–Oxley. Another main thing to consider when choosing and implementing a security policy is to make sure that they are being adhered to and trained on often.

References:

Grimmick, R. (2023, April 6). *What is a security policy? definition, elements, and examples*. Varonis. https://www.varonis.com/blog/what-is-a-security-policy#definition

Information security policies: 10 examples, features, and benefits | ekran system. (n.d.-a). https://www.ekransystem.com/en/blog/information-security-policies

Online, B. (2020, November 23). *Yahoo Data Breach: What actually happened?*. Medium. https://bpbonline.medium.com/yahoo-data-breach-what-actually-happened-54cf8f3f7c93

Selyukh, A. (2017, October 3). *Every yahoo account that existed in mid-2013 was likely hacked*. NPR. https://www.npr.org/sections/thetwo-way/2017/10/03/555016024/every-yahoo-account-that-existed-in-mid-2013-was-likely-hacked

Thurmond, T. (2024, February 6). *15 information security policies every business should have*. KirkpatrickPrice. https://kirkpatrickprice.com/blog/15-must-have-information-security-policies/

Yahoo says all three billion accounts hacked in 2013 Data Theft | Reuters. (n.d.-b). https://www.reuters.com/article/technology/yahoo-says-all-three-billion-accounts-hacked-in-2013-data-theft-idUSKCN1C82NV/