Module 8 Journal

Abby Farnsworth

CS405- Secure Coding

October 22, 2021

Adoption of a secure coding standard is a must-have for every development team. Foster (2020) explains, “Secure coding standards are rules and guidelines used to prevent security vulnerabilities. Used effectively, these security standards prevent, detect, and eliminate errors that could compromise software security”. Software security is not something that can be left for the very end of a project. It might not even be possible to fix all errors if an entire project is finished, then found to contain large amounts of insecure code. Bellairs (2019) writes, “Don't leave security until the end of development. Adding a deadbolt to a door made out of cardboard won’t make it more secure. In the same way, an insecure device or application may require extensive redesign to become secure”. Insecure code is not something that can be overlooked. It is a gateway for hackers to enter your system and steal data, release malware, trigger a denial-of-service attack, and more.

Security breaches can be extremely damaging for businesses. A breach is likely to be an expensive event for the company. As of 2020, the average cost of a cyber breach in the US was $3.86 million (4 Serious, 2021). Part of this financial loss comes in because the business may have to shut down while the situation is being straightened out. It is therefore in a company’s best interests evaluate risks and address them before something happens.

There are four steps to the risk evaluation process: identification, assessment, mitigation, and prevention (Security Risk, n.d.). First, identify your critical assets and consider what sensitive data is associated with those assets. Assess the risks presented by your assets and think about the resources needed to mitigate those risks. Determine your mitigation approach and what the security controls will be. Implement the chosen tools and controls to prevent the risk of threats and vulnerabilities compromising your company’s security.

Raina (2021) explains, “Zero Trust is a security framework requiring all users, whether in or outside the organization’s network, to be authenticated, authorized, and continuously validated for security configuration and posture before being granted or keeping access to applications and data”. The five pillars of zero trust are device trust, user trust, transport/session trust, application trust, and data trust (Keoh, 2020). Device trust means that devices are inventoried, managed, and monitored by IT. User trust says that user authentication can involve a username and password, but it should have another component to it, such as MFA. Transport trust means that users can only access internal apps if certain conditions are met. Session trust uses the principle of least privilege to ensure that users do not have too much access. When users need to access multiple applications, it can be useful to isolate the apps to a virtual desktop, which is where application trust comes in. For data trust, Keoh (2020) writes, "Technologies such as data loss prevention (DLP) ensure unwanted exfiltration or destruction of sensitive data. Although data classification and integrity are, for the most part, handled by the application itself, we should enhance the trust level wherever we can when building a zero-trust architecture".

Having a strong security policy is a good first step, but a company must actually follow its own recommendations and implement the necessary security controls. It is not enough to just have good intentions around security--there must be follow-through. If a business is having trouble figuring out how to create a more secure environment, they can hire a security expert to come in, do an evaluation, and provide their recommendations. The important thing is for a company to take consistent steps towards stronger security.

References

Bellairs, R. (Jul 2019). What Is Secure Coding?. Retrieved from <https://www.perforce.com/blog/sca/what-secure-coding>

Foster, S. (Oct 2020). What Are Security Standards? Secure Coding Standards Overview. Retrieved from <https://www.perforce.com/blog/qac/secure-coding-standards>

4 Serious and Damaging Consequences of Data Breach. (Mar 2021). Retrieved from <https://triadanet.com/consequences-of-data-breach/>

Kueh, T. (Jan 2020). A Practical Guide to Zero-Trust Security. Retrieved from <https://threatpost.com/practical-guide-zero-trust-security/151912/>

Raina, K. (May 2021). Zero Trust Security. Retrieved from <https://www.crowdstrike.com/cybersecurity-101/zero-trust-security/>

Security Risk Assessment. (n.d.). Retrieved from <https://www.synopsys.com/glossary/what-is-security-risk-assessment.html>