Chris Bull

2/23/2025

CS-405

8-2 Journal: Portfolio Reflection

Throughout the CS-405 course, I have learned the importance of not leaving security to the end. According to the federal trade commission, “Experts agree on the key first step: Start with security” (Federal Trade Commission, 2015). Starting with security means that it should be factored into decision making across every department. With this proactive approach, a lot of time and money can be saved by reducing breaches and reducing compliancy violations. Shifting to the security-first mindset also increases trust with customers as they will feel secure with providing their personal information and sensitive information to the company. If security is left to the end, major breaches can occur that can be very expensive to fix and will cause customers to lose trust in the company’s security.

I have also learned the importance of adopting a secure coding standard. Without a standard, different departments and teams will operate in their own “silos” and have their own agendas and standards (Vijayan, 2017). When the teams collaborate and combine each of their unique standards, it can create a messy program riddled with security vulnerabilities. A secure coding standard eliminates the possibility of this happening. It will unify the style of coding across the company and help train developers who may have been unaware that they were coding insecurely in the first place (Vijayan, 2017).

To evaluate and assess potential risks in your code, it is important to run the code through a static analysis program. A great example of a static analysis program that we used in this course is Cppcheck. Static analyzers help developers write consistent code, perform maintenance on their code, get more performance out of their code, and prevent bugs and undefined behavior in their code (Verhagen, 2020). While they aren’t as “smart” as a developer who is extremely familiar with the libraries that they are working with, they are a great second layer of defense to run your code through before pushing it to a production environment.

Mitigation is another important topic within the field of secure coding. When security threats are proactively mitigated in early development phases, a company can save large amounts of money with remediation costs in any future breaches. An example of a mitigation technique in cybersecurity is encrypting sensitive user details like password and personal information about users. Encrypted data costs less to remediate and often is required by compliancy standards like HIPAA, GDPR, and FISMA (Patrick, 2019).

Zero Trust is a newer model in the cyber security field and has changed the way that companies handle their security. Traditionally, companies defended themselves by considering everything in their network as trustworthy and everything outside of the network as untrustworthy. Now that many employees working from personal devices and being outside of the “protected” network, the zero trust model is used. In the zero trust model, no users are trusted and every user is verified when they try to login or access a resource (Okta, 2019). Verifying users may come in the form of biometric verification, requesting that the user sign in again, or using multi-factor authentication (MFA) methods such as one-time passcodes, security keys, or push notifications to the user’s trusted device.

Security policies are crucial for any business and provide employees with a set of policies that protect the user and the company’s organization’s legal and ethical responsibilities (Dunham, 2020). They should include policies about access control, data classification, encryption, remote access, physical security, change management, etc… (Dunham, 2020). For example, in the company’s access control section of their policy, it may state that only authorized individuals have access to company systems. To uphold this policy, all users must have unique login credentials and new accounts must be approved by HR and the IT security team. When implementing a company-wide security policy, it is important to ensure the policies are enforceable, explain how policy exceptions are handled, and make the policies brief and clear (Dunham, 2020). An ideal security policy is one that protects an organization and its employees while also being followed and understood by the employees.

**References**

Dunham, R. (2020, May 5). *Information Security Policies: Why They Are Important to Your Organization*. Linford & Company LLP. https://linfordco.com/blog/information-security-policies/

Federal Trade Commission. (2015, June 29). *Start with Security: A Guide for Business*. Federal Trade Commission. https://www.ftc.gov/business-guidance/resources/start-security-guide-business

Okta. (2019, January 7). *What is Zero Trust Security?* YouTube. https://www.youtube.com/watch?v=d-Jk3GzjwlM

Patrick, S. (2019, June 28). *Why Encrypt Data in an Application? Save money in a data breach*. Tozny. https://tozny.com/blog/why-encrypt-data/

Verhagen, B. (2020, February 14). *Things I learned from the static analyzer - Bart Verhagen - Meeting C++ 2019*. YouTube. https://www.youtube.com/watch?v=\_\_Wz2DG1t24

Vijayan, J. (2017, December 13). *6 DevSecOps best practices: Automate early and often*. TechBeacon. https://web.archive.org/web/20240117143629/https://techbeacon.com/security/6-devsecops-best-practices-automate-early-often