**Module Eight Journal**

Andres Sanchez

Southern New Hampshire University

CS-405-13379-M01 Secure Coding

October 27, 2024

Throughout our course with secure coding practices, I’ve engraved the importance of having a security first mind set and how it’s not just a best practice but instead a necessity. In today’s ever-evolving world, understanding the tools and information to fight a growing threat of cyberattacks is crucial. Personally, it has been particularly impactful to learn about tools I can use to stay secure, such as using Automation Tools, Assert()’ and 'Unit Testing. Moreover, I’ve realized the importance of thinking more through vulnerabilities during the planning phase of projects, rather than addressing them later.

In Module Six, we focused on the adoption of secure coding standards and not leaving security to the end. We read and discussed how security does not have to be complicated and can be seamlessly integrated into existing infrastructure. As developers, this means shifting towards a DevSecOps model from the traditional DevOps framework, encouraging programmers to follow a uniform set of rules and guidelines set by the organization. Its key to think through principles, policies & standards early in pre-production to provide pre-determined guidance and training, ensuring code remains consistent and common errors are prevented. For me, this is an area I could improve as I tend to focus on methods that just work functionally & efficiently, often not considering security until the review process. That said, adopting this proactive approach can help me catch vulnerabilities earlier. For post-production practices, this includes performing health checks, continuous monitoring and having a response process in place in case of a breach. This is particularly relevant to a various set of real-world incidents such as the Target incident from 2013. In this breach, attackers compromised the company’s POS systems, exposing to over 40M credit card records. While the security in place flagged this intrusion, the alerts were ignored, and no proper process was in place to respond quickly which ultimately cost the company over $200M.

In this course, we also explored how to evaluate and assess risks using a cost-benefit analysis of mitigation. This involved determining whether the cost of mitigating a risk justified the reduction in risk. Fundamentally determining risk can consist of three questions: What can happen? How likely is it to happen? And what are the consequences if it does? In a hypothetical, a company might evaluate a certain network segmentation as a strategy. This could involve estimating the cost of hardware upgrades, software tools and ongoing maintenance, then comparing those costs to the potential impact of breach based on similar incidents or industry trends.

In our current module we took a dive into Zero Trust, a security framework where internal and external users are authenticated and authorized before accessing a company’s data, systems and resources. As mentioned in my discussion, this aligns with the ‘Default Deny’ principle & ‘Least Privilege Access’ where no device or user is trusted by default and instead granted access only after verification. A real-world example that failed to follow Zero Trust principles was a 2023 Tesla’s insider breach, where two former employees were able to misappropriate sensitive information, gaining access to over 100GB of confidential data including information about 75 thousand of current and former employees. An effective Zero Trust Model could have prevented this by enforcing offboarding processes where access is revoked upon an employee leaving an organization. Additionally, monitoring data and movement, especially for sensitive data, could have minimized the damage.

Finally, one of the most important topics we covered was the implementation and recommendation of security policies which we did for Project One. Security and policies ultimately protect an organization’s assets and information by outlining a clear set of expectations, guidelines and procedures for security practices. In our project, we identified potential threats to Green Pace , defined principles & standards to address those risks and provided examples on how developers could apply these to their work. Most importantly we discussed the importance of creating a security aware culture, encouraging employees to implement effective security policies. This is a valuable skill that I will carry with me as I develop projects for myself and future organizations.

**Citations**

Kohen, I. (2023, November 27). *Data Breach: What Tesla’s biggest insider threat in 2023 can teach us going into 2024*. HackerNoon. <https://hackernoon.com/data-breach-what-teslas-biggest-insider-threat-in-2023-can-teach-us-going-into-2024>

Jones, C. (2022, May 3). *Warnings (& lessons) of the 2013 target data breach*. Red River | Technology Decisions Aren’t Black and White. Think Red. https://redriver.com/security/target-data-breach