**Southern New Hampshire University**

**8-2 Journal: Portfolio Reflection**

**Cassidy Yohn**

The adoption of SEI CERT C++ Coding Standard ensures that specific rules are followed during the development of an application that help keep code as secure as possible. The standard can be used as a guideline of how to implement secure coding throughout development. Without adhering to these rules and recommendations, applications are more vulnerable to an attack by a threat agent. Bugs, defects, and flaws in code can be easily overlooked if secure coding practices are not implemented during production and adding a safe lock at the end of a system or program does not guarantee security. Therefore, it is necessary to apply layers of security within code to prevent penetration, rather than leaving security to the end.

There are many risks involved with coding and costs benefits to mitigating them. Some of the risks include privacy violations, insecure storage, insecure transport, insecure deployment, and poor logging practices. All these code flaws are susceptible to ransomware, phishing, data leakage, hacking, and more. These problems cause businesses a lot of money due to putting business at a standstill, a decrease in sales, and a loss of business. Mitigation of these issues can save companies millions of dollars considering the average cost of a data breach is US$4.24 million on an annual basis (Owaida, 2021).

According to Threat Post, the term zero trust “is a phrase first coined by John Kindervag of Forrester in 2010 to describe the need to move security leaders away from a failed perimeter-centric approach and guide them to a model that relies on continuous verification of trust across every device, user and application” (Kueh & Kueh, 2020). The zero-trust approach focuses on five areas which include device trust, user trust, transport/session trust, application trust, and data trust. Zero trust policies are implemented into these areas to enforce the never trust, always verify concept (Kueh & Kueh, 2020). The zero-trust security model “considers all resources to be external and continuously verifies trust before granting only the required access” (Keuh & Keuh, 2020). Since, modern problems require modern solutions, the zero-trust policy is considered the best method of security to implement due to rising remote positions and users needing to access many different apps, from many different devices, both internally and externally from their companies’ network.

There are many different recommended security policies and ways to implement them. Some of the most popular among cyber security specialists include employee awareness and training, password management, remote access, bring your own device, acceptable use, regular backup, and disaster recovery polices. These policies help establish and maintain the confidentiality, integrity, and availability of information, applications, and systems. The policies can be implemented through teaching employees of the importance of security, enforcing the need for strong, unique passwords that should be updated frequently, implementing security procedures for accessing data over remote networks, specifying how and where data can be accessed, explaining the correct use of a company’s technical resources, implementing regularly scheduled back-ups, and creating a plan for how to recover from an unexpected disaster. The implementation of security policies will help ensure the safety and security of an organization’s and their user’s data.

**References**

Owaida, A. (2021, December 31). *22 cybersecurity statistics to know for 2022*. WeLiveSecurity. Retrieved April 23, 2022, from https://www.welivesecurity.com/2021/12/30/22-cybersecurity-statistics-know-2022/

Kueh, I. S. I. T., & Kueh, T. (2020, January 15). *A practical guide to zero-trust security*. Threatpost English Global threatpostcom. Retrieved April 23, 2022, from https://threatpost.com/practical-guide-zero-trust-security/151912/