**8-2 Journal Portfolio Reflection**

The adoption of secure coding standards is one of the most important aspects of software development. This approach integrates security from the initial phases of the software development life cycle. Secure coding standards serve as preventative measures against common vulnerabilities and security flaws by establishing guidelines that developers must follow. This is fundamental in reducing the risk of security breaches and ensuring the integrity of software applications. For instance, practices such as input validation, proper error handling, and adherence to principle of least privilege in AAA security, are used to prevent unauthorized access and data leakage.

The evaluation and assessment of risks is essential in security decision-making. You must balance the potential impacts of security threats against the expenses involved in implementing security measures. The adoption of AAA security frameworks exemplifies how risk assessment shows the configuration of authentication, authorization, and accounting protocols, align security expenditures with actual threat landscapes. This alignment ensures that security measures do not overly encumber the usability or performance of any given system.

The shift towards a Zero Trust model reflects a fundamental change in security philosophy from "trust but verify" to "never trust, always verify." This transformation is driven by the need for more dynamic security mechanisms in increasingly complex IT environments, where traditional security models are no longer sufficient. Zero Trust advocates for continuous verification of all entities including users, devices, and applications within an organization's network. This approach minimizes attacks by ensuring that access is strictly authenticated and authorized on a per-session basis and is dependent upon compliance with security policies.

The effective implementation of security policies is integral to the governance of IT infrastructures. These policies dictate the security posture of an organization and guide the implementation of security measures, such as those outlined in the AAA security model and the Zero Trust framework. To be effective, these policies must be clear, comprehensive, and enforceable with technological solutions that enable automation and scalability. For example, the deployment of technologies like multi-factor authentication (MFA) and conditional access systems are practical implementations that reinforce policy directives.

**Resources**

Mylonas, L. (2018, November 27). *What is AAA Security? an introduction to authentication, Authorisation and Accounting*. Codebots. https://codebots.com/application-security/aaa-security-an-introduction-to-authentication-authorisation-accounting

Kueh, I. Insider                                      Tony, & Kueh, T. (n.d.). *A practical guide to zero-trust security*. Threatpost English Global threatpostcom. https://threatpost.com/practical-guide-zero-trust-security/151912/