8-2 Journal: Portfolio Reflection

Chris Marrs

06/25/2024

Secure Coding Standards are an indispensable element of any development project, helping ensure security isn't an afterthought but built directly into applications from day one. Adherence to such standards allows developers to avoid vulnerabilities like SQL Injection and Cross-Site Scripting from entering their code, thus decreasing risk and saving both time, money and resources in later repairs.

Secure development processes incorporate cost-benefit analyses and risk evaluation. Developers can prioritize critical issues by conducting in-depth risk evaluation, while more efficiently allocating resources. It is also crucial that costs associated with implementation be balanced against possible security breach costs (financial loss, damage reputation damage liability).

Zero trust models don't entail implicit trust between entities in and outside an organization's networks, following the principle of giving users and devices only minimal permissions for tasks they need to accomplish. Such models help organizations reduce risks such as security breaches, data leakage and other hazards; it requires shifting attitudes while being committed to ongoing authentication processes but can result in tangible benefits in terms of resilience and asset protection.

Implementation of security policies is integral in creating and maintaining a safe development environment. For maximum effectiveness and relevance, policies must address issues like access control and data handling - while at the same time providing accountability through regular reviews. Enforcing policies also promotes teamwork - key qualities needed in today's complex threat landscape.