Concepción Ardon

CS 405

15 Dec 2022

8-2 Journal

Portfolio Reflection

Adopt a secure coding standard. Create and/or implement a secure coding standard for your development language and platform. Secure coding methods and standards are critical since coding errors generate up to 90% of software security issues. Software security is vital because it helps to protect software from potential vulnerabilities, faults, or flaws. The usage of secure coding standards is a critical component of such protection. Don’t leave security until the end of development, because any potential coding error could cause a glitch or, worse yet, a significant security breach. Cyberattacks are becoming more frequent and sophisticated, so it's critical to identify vulnerabilities and prevent attacks as early in the development process as possible. The steps to preventing these threats are by following the 10 secure coding practices. A security risk assessment finds, evaluates, and applies important application security controls. It is also concerned with preventing application security flaws and vulnerabilities. A risk assessment enables an organization to see its application portfolio comprehensively from the perspective of an attacker. The application of security policies and processes to lower the total risk or impact of a cybersecurity threat is known as risk mitigation. Risk mitigation in cybersecurity can be divided into three components: prevention, detection, and remedy. As hackers' approaches get more sophisticated, your organization's cybersecurity risk mitigation strategies will need to evolve in order to keep the upper hand. Zero Trust is a security framework that requires all users, both inside and outside an organization's network, to be verified, approved, and continually validated for security configuration and posture before being permitted or maintaining access to applications and data. Zero Trust presupposes that there is no traditional network edge; networks can be local, in the cloud, or a combination or hybrid of the two, with resources and workers located anywhere. This framework's implementation combines advanced technologies such as risk-based multifactor authentication, identity protection, next-generation endpoint security, and robust cloud workload technology to verify a user's or system's identity, take into account access at that time, and maintain system security. Zero Trust also necessitates the consideration of data encryption, email security, and the hygiene of assets and endpoints before they connect to apps.

Any security policy has two components. One is concerned with preventing external threats to the network's integrity. The second addresses internal hazards by establishing proper network resource use. Implement the 10 principles of secure coding and secure coding practices. Implement triple-A policy and defense-in-depth policy. Train everyone in the company about security risks and how to detect them. Run multiple tests to detect any flaws in the code. Assess the impact of organizational issues on information security policy. Policy and standards should be reviewed and modified as needed, but at least once a year.