8-2 Journal

CS 405

Ma24rtin Richardson

10/24/2024

Security is a fundamental part of modern software development, and to protect systems against evolving cyber threats, organizations must integrate security into every stage of development. This paper addresses four critical concepts: secure coding standards, risk evaluation, Zero Trust, and the implementation of security policies.

Adopting secure coding standards early in the software development lifecycle (SDLC) is essential. Relying on security measures at the end of development often leads to vulnerabilities that are harder and more expensive to address. Using frameworks like OWASP's Secure Coding Practices helps developers mitigate risks such as SQL injection and cross-site scripting (XSS) through techniques like input validation and secure authentication. By incorporating threat modeling early, teams can identify and address security concerns before they become critical issues, reducing overall remediation costs.

Risk evaluation helps prioritize threats and assess how best to mitigate them. Frameworks such as STRIDE or NIST allow organizations to categorize risks based on their potential impact and likelihood. A cost-benefit analysis helps determine when mitigating certain risks, such as encrypting sensitive data, is worth the investment. Proper risk assessment ensures that resources are spent wisely, focusing on the most significant threats.

The Zero Trust model assumes that no one, whether inside or outside the network, can be trusted by default. This model requires continuous verification and least privilege access, ensuring that users have only the permissions they need. With the rise of cloud computing and remote work, Zero Trust offers critical protection by minimizing the risk of insider threats and preventing lateral movement within networks. Identity and Access Management (IAM) and role-based access controls (RBAC) are key components of this approach.

Strong security policies provide a clear framework for consistent security practices across the organization. Policies should include password management, data encryption, and incident response protocols, and be continuously updated to reflect evolving threats and regulations. Regular employee training is vital, as human error is a common cause of breaches. Enforcing policies through monitoring, audits, and incident response ensures compliance and strengthens the organization’s security posture.

By adopting secure coding standards, performing thorough risk evaluation, implementing Zero Trust, and enforcing strong security policies, organizations can build more secure systems. These practices work together to reduce vulnerabilities, improve response to threats, and protect sensitive data in an increasingly complex cybersecurity landscape.