Mod 8 Journal George Kaline III

Adopting a secure coding standard means utilizing a set of best practices and guidelines that guide developers in coding applications that are immune to vulnerabilities and protected from exploits. Instead of security as an afterthought, it should be integrated into the software development lifecycle (SDLC) right from the early stages.

Preventative security avoids vulnerabilities instead of having to fix them after the fact, reducing risk. Cost Efficiency reduces the cost of fixing security vulnerabilities early and is significantly cheaper than doing so after deployment. Regulatory Compliance is used in most sectors that must meet security standards. Defense against attacks reduces exposure to common exploits like SQL injection, XSS, and buffer overflows. Security has long been considered an afterthought in development, usually addressed during penetration testing or after a breach.

Risk evaluation and appraisal entail the process of identifying likely threats, quantifying their occurrence, and understanding their effects on an organization's operations, resources, and goodwill. The activity assists in categorizing risks depending on their probability and severity, thereby assisting organizations in prioritizing risks. Having identified risks, a cost-benefit analysis can be done to identify the most efficient measures for mitigating identified risks. The objective is to balance security expenditure with business effectiveness so that the cost of implementing a security control is no more than likely losses in the event of a security breach. Organizations choose among risk avoidance, mitigation, transfer, or acceptance based on this. An effectively designed risk assessment framework facilitates decision-making, optimizes security spend, and optimizes overall cyber threat resilience.

Zero Trust is a security design that operates on the "never trust, always verify" principle, in which no user, device, or system is automatically trusted whether inside or outside the network. Instead of trusting traditional perimeter security, Zero Trust continuously verifies, enforces least-privilege access, and anticipates that breaches will happen at any time. It also employs multi-factor authentication, network segmentation, real-time monitoring, and strict access control to minimize risk. By eliminating the notion of implicit trust and emphasizing verification at every level, Zero Trust improves security, prevents unauthorized access, and limits the impact of cyberattacks.

Security policies provide systematic rules to protect systems, data, and users against cyberattacks. Establishing security needs in the process of conducting risk assessments and adhering to standards like NIST, ISO 27001, and GDPR. Security Policies will establish access control, data protection, incident response, and acceptable use olicies. Implementation of security controls using MFA, encryption, network segmentation, and endpoint security. Employee Training and conducting periodic security awareness programs in order to prevent human errors. Monitoring and enforcing the use of automated security tools (SIEM, AI-based detection) and performing regular audits.

Some recommendations to include in the security policy would be helpful. Here are some: Implement Zero Trust principles (never trust, always verify). Enforce least privileged access to minimize security risks. Automate security operations for real-time threat detection. Regularly update policies to stay ahead of evolving threats.