Priscilla Gomes-DaCosta

Southern New Hampshire University

8-2 Journal: Consider the Motive for the Attack

12/11/2022

**Adopting secure coding**

Adopting secure coding practices in the software development lifecycle is important it optimizes security from the start, helping reduce long-term costs related to software vulnerabilities that can be exploited in sensitive data leakage. Adopting Defense in Depth standards allows integration of people, technology, and operations capabilities that serves as layers of barriers to protect the organization.

**Mitigating risk**

There are many internal and external areas that can be secured, deciding how and what to protect is determined by risk assessment, keeping in mind, that threats of today will differ from threats of tomorrow. Integrating secure coding techniques, performing tests early and often in the software development lifecycle, maintaining code amended through static code analysis carries a small cost when compared to the cost of dealing with mitigating a breach due to a threat.

**Zero trust**

Zero trust is a framework that secures infrastructure and data, it requires all users to be authenticated, authorized, and validated for security configurations before gaining access to data and the network system. Access is denied by default, user’s identity can be confirmed user credentials, credentials privileges can be set so users only have access to the portion of the system crucial for them to perform their job, geo location, and firmware versions.

**Security Policies**

Security policies serves as a guideline to maintain data safe, by creating, maintaining, reviewing security policies often, coding standards and best practices needs to be implemented in every project to allow for consistent safety.