CS-405-10861-M01 Secure Coding 2024 C-3

2-1 Journal: Defense in Depth (DiD)

Computer Science Department

Southern New Hampshire University

Eric Farkas

5/19/2024

**How deep is too deep, and what’s the tradeoff?**

Defense in Depth (DiD) is an approach to information security that leverages multiple layers of security to protect devices and data from security breaches. This multiple-layer defense strategy can be visualized by several pieces of mesh staggered so that the holes become blocked. Like each piece of mesh, each defense method has holes, but when overlapped, the secondary defense method blocks attacks left through by the first method. These defense methods often include firewalls, passwords, encryption, secure code, network security, and other specialized security methods. Defense in depth is challenging to establish and usually requires coordination between departments. This multi-layer security approach is a better defense than single-layer methods, but it can be penetrated over time. The attacker focuses on one layer at a time until all layers are compromised. It is crucial to remember that systems are designed to support authorized users. Too many layers or policies that are too strict will discourage users or impact their productivity. This is where defense in depth goes too far. A good mix defends users and data but does not limit their functionality, productivity, or accessibility. Applications, data sources, network storage, peripherals, and external storage should always be considered when implementing a defense in depth strategy.

**What are some time, money, reputation, and operational considerations?**

Time can often be more costly to organizations than actual financial loss. Security breaches affect time in several ways. One of the most expensive is lost productivity. This typically happens when business applications such as email or databases that support business activities become compromised. The productivity lost may be due to the time it takes to repair a system, redundant work required to replace lost or corrupt data, or the inability to access a system while additional security measures are put into place.

Money is most often defined as a direct financial loss due to a compromised system. This is often related to lost productivity but can extend to missed opportunities to receive or fulfill orders during the system outage. Security breaches for organizations that perform financial transactions pose a larger risk should those systems be compromised. Large amounts of money can quickly be routed to unexpected accounts in this type of breach. Organizations that rely on systems for sales are also in a higher risk category. Attacks that cause extended outages of the systems responsible for transactions are measured in financial loss per unit of time. The number of transactions will determine whether this is measured per day, per hour, or per minute.

Reputation is important for organizations that rely heavily on relationships. These organizations gain customers by being trustworthy and ethical. Security breaches within these organizations often result in the loss of personal information or account numbers. These organizations are often governed by a regulatory organization that forces disclosure based on the type and amount of data lost. These disclosures disrupt customer confidence, and a significant breach could result in a significant loss of customers. As transactions become more integrated, many of these organizations provide data through application programming interfaces (APIs). With electronic ties to many systems, a data breach can affect multiple organizations. These pathways offer greater opportunities for defense in depth as all communication is server-to-server or free from users. However, some security methods are unavailable as most traffic leverages the Internet.

The operational impact can be widespread. It can range from lost orders to the inability to ship or resupply, warehouse issues, communication problems, and more. The affected areas will experience downtime while any damage from the breach is repaired, and delays will occur if the area services customers. The financial impact is often highest when operational users and systems are affected. These users and systems most frequently impact revenue and profitability in most organizations.

**What are some additional aspects of DiD that make it unique for each situation?**

After reviewing the above considerations, it is easy to see that organizations will prioritize defense in depth differently. Organizations dealing with highly sensitive or personal data will review critical hardware or other material resources. High-risk organizations often practice security and pay consultants to test their defenses. Firewalls are often a first step in this defense strategy. Firewalls deny unwanted network traffic by inspecting inbound requests to determine if they are valid or not. Firewalls are programmed with rules and policies to protect an organization. They utilize techniques like whitelisting IP addresses, MAC locations, and ports. There are also application-specific firewalls for things like web applications and secure email that focus on specific actions and traffic. The principle of least privilege requires a documented strategy and specialized policy that focuses on clients, frameworks, and users to allow access to assets (organizations, frameworks, and documents) that are required for performing daily tasks. Strong passwords and regular password changes are required for applications and active directory authentication. These passwords are of minimum length and require a specific number of mixed and special characters. Strong passwords prohibit the re-use of previous passwords as well. Patch management keeps applications, operating systems, web browsers, and other business applications free from known vulnerabilities. Patches should be applied regularly. High-risk organizations should not lose sight of peripherals like printers, access points, and network switches, as the operating systems and management ports on these peripherals can become vulnerable occasionally. Multi-factor authentication is an additional step to ensure the identity of users logging into the network.