**Journal: Defense in Depth (DiD)**

Justin Starr

Department of STEM

CS 405 – Secure Coding

Professor Mike Alesso

July 14, 2024

**Journal: Defense in Depth (DiD)**

Defense in Depth (DiD) is a security strategy that makes use of a variety of security tools, instruments, and policies, which are deployed in multiple layers, and when used together assume that if any one of these security tools fails, another one will be in place (Fruhlinger, 2022). The following is a short analysis of Defense in Depth and how deep is too deep, its time, money, reputation, and operational considerations, as well as some additional aspects of DiD that make it unique for each situation.

To understand how deep is too deep when implementing DiD, it is essential to know that there are multiple elements that come together to protect a network, system, or application, which can be classified into three main groups: administrative controls, physical controls, and technical controls. Administrative controls are organizational strategies for creating a secure environment and include policies for how specific tools are selected and implemented, procedures for how to handle data safely, and frameworks that help mitigate the risks of connecting with outside systems (Fruhlinger, 2022). Physical controls include security measures such as implementing physical keycards and lockable and defensible doors to a company’s office and data center and even hiring security guards to help monitor and maintain the security of such facilities (Fruhlinger, 2022). Technical controls are the layers of security that are deployed for the hardware, software, and network (Fruhlinger, 2022). While it is a good idea to implement as many of these elements as possible, because the more layers of protection you have the better, it is important to understand that there is a balance that must be achieved between these three groups and that there are considerations concerning time, money, reputation, and operation.

One consideration when deploying a DiD strategy is that it can require a significant amount of time to implement and maintain depending on the size of the organization and how many layers are being implemented. It might require utilizing outside companies or hiring additional professionals who are qualified to manage the strategy, which can lead to higher expenditures. Also, as it concerns money, the more layers of security that are implemented, the more expensive it can be to incorporate the appropriate hardware, software, etc. When considering time and money, it is also important to consider the organization’s reputation. Having too weak of a DiD strategy could have a negative impact on the organization’s reputation if the organization were exploited due to a vulnerability somewhere within the defense strategy. While some components may be expensive to incorporate, it is essential to realize that not having some could expose the organization to vulnerabilities that could lead to an event such as a data breach, causing reputational harm, and the possibility of additional expenditures to remediate the event. Also, not having a sufficient DiD strategy could cause operational downtime if and when attacks occur, such as a Denial of Service (DoS) attack, or from having to shut down various systems and components while handling security vulnerabilities. Again, finding the appropriate balance, based on an organization's needs is crucial for safeguarding an organization and its network infrastructure, which includes its systems, components, and applications.

Another consideration is that a significant layer of defense exists within developers by following industry standards and best practices, such as secure coding. While not all code can be without bugs and flaws, practicing secure coding helps reduce the likelihood of introducing vulnerabilities to a company’s infrastructure, which can have a significant impact on the company’s operation including reducing operational downtime, reducing the cost associated with remediating identified vulnerabilities, as well as its associated reputational effects on the company. Practicing secure coding is a significant security layer that should be applied no matter the size of an organization, as it is a foundation for implementing and maintaining a secure infrastructure.

Additional aspects of DiD that make it unique for different situations is that for each type of control, there are various elements that can be implemented based on the needs of the organization. Large corporations, enterprises, and even government agencies may find that they need higher amounts of security at each control level and deem it necessary to have higher expenditures for these controls. In contrast, smaller businesses may not require the same level of physical, administrative, or technical controls depending on the type of organization and the services they provide. However, no matter the size of an organization, increasing the depth of defense helps to reduce the risk of an attacker gaining access to the organization’s infrastructure, and helps to protect the organization’s data.

**References**

Fruhlinger, J. (2022, July 28). *Defense in depth explained: Layering tools and processes for*

*better security*. CSO. <https://www.csoonline.com/article/573221/defense-in-depth-explained-layering-tools-and-processes-for-better-security.html>