Joseph Silva Jr.

SNHU

CS 405: 2-1 Journal: Defense in Depth

11/07/2021

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

First, the Defense in Depth (DiD) is an approach to computer information security with a multi-layer security system to protect the devices and data from security breaches. The multi-layer defense system could be described like a castle siege defense. Defenses such as firewalls, passwords, encryptions, hardened code, network security, etc., can be compared to a castle siege defense like a bridge and moat, castle walls, soldiers, anti-siege equipment, etc. The multi-layer defense causes the attackers to get through multiple areas in order to reach the system instead of only protecting the system with one layer defense. However, no matter how good one’s defense can be, there is never a perfect defense against an attacker especially over time. Most attackers will be able to adapt and overcome a defense system even a multi-layer defense system if they are given time. I believe a good system allows a user to be defended and it allows the user to have the freedom to explore as well. Since there will never be an impenetrable defense when it comes to computer security, I believe the defense is an issue when the defense prevents the user from using the system or any apps correctly. For example, I had an issue with ByteFence Anti-Malware because it prevented me from opening any Word documents due to a security issue. Overtime, I would have to shut down ByteFence in order to open up a Word document and this caused my system to be exposed with its only protection being Windows Security. Due to this reason, I went to Avast instead of staying with ByteFence. The tradeoff for DiD is user’s defense vs user’s computer exploration freedom.

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

1. **Time:**

Security breaches cause an issue with users and/or companies’ time whether it be the time lost from the use or creation of an app, which has been compromised due to a successful attack, or the time spent in repairing the damage from a successful attack that breached security.

1. **Money:**

A failed information security system can cause a loss of money for the users and/or companies being protected and also the company or individual who created the security system. A successful attack can also cause loss to the customers of a company using this security system. For example, I had a case where a customer lost their down payment on purchasing a new house because the real estate company network was breached, and the attackers were able to communicate with the customers by pretending to be employees of the real estate company. This is just one example of the loss of money due to a poor security system.

1. **Reputation:**

Users and/or companies can develop a bad reputation from their customers due to poor computer security systems from situations like the example I described above. Once these users and/or companies lose customers or clients, the company that developed the security system will also develop a bad reputation for putting out product that is easily bypassed and will mostly likely lose a lot of customers because of this reputation.

1. **Operational:**

Successful breaches can cause a company to halt its daily operations in order to redirect all of the company’s attention on fixing the damaged caused from the breach. This type of halt and redirection of resources can prevent the company’s ability to upgrade and/or update in product.

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

1. Firewall
2. Passwords
3. 2-Step Authentication
4. Hardened Code
5. Network Security

**CITATIONS:**

1. YouTube. (2016). *YouTube*. “Software Security – Design Category Defense in Depth, Monitoring Traceability”. Retrieved November 6, 2021, from https://www.youtube.com/watch?v=vaEXHX2IFHg.
2. *What is defense in depth?* Forcepoint. (2021, May 6). Retrieved November 6, 2021, from https://www.forcepoint.com/cyber-edu/defense-depth.