**CYB 220 Project Three**

Douglas Few

Southern New Hampshire University

February 20, 2022

**Fundamental Security Design Principle**

When it comes to network security, it is my opinion that layering is one of the most effective ways to protect your systems and data. Layering is the process of implementing multiple forms of protection so that there are checks and balances that must be made before access to a system is granted to a user (Tjaden, 2015). For example, if a network was protected by an intrusion detection system and an intrusion prevention system, both of those systems would act as separate layers to an overall security system. Layering could also be the process of incorporating multiple security design principles. Upholding the principle of least privilege and isolation simultaneously could be considered layering. I believe that the most secure systems are ones that incorporate many layers into their security plan, so that there is an answer to every potential vulnerability.

**Network Protection Approach**

As mentioned in the previous section, layering can often be achieved simply by combining multiple security design principles. One of the easiest and cost effective principles is that of least privilege (Tjaden, 2015). In this particular scenario, there have been incidents of employees from the acquisitions department trying to access data held within the human resources network. A quick solution to this would be user access control. By removing the ability to access the human resources network to begin with, the data held on that network would be more secure and the slowdown being experienced on that network would be relieved.

Alongside the user access controls, a network intrusion detection system (NIDS) should be installed on every subnet in the organization. This will help to automatically detect when an unauthorized attempt to access a network is being made (GeeksforGeeks, 2022). If a signature-based intrusion detection system is used, it can be configured to recognize the signatures of host computers on other subnets and signal the IT department if an unauthorized attempt is made.

Another important configuration that needs to be made is that of the network firewall. The recommendations up to this point have been made under the assumption that unauthorized access attempts were being made internally. However, external breaches to the network is also a concern. Firewalls work to monitor and filter all traffic passing through a network based on a set of rules configured by the network administrator (cisa.gov, 2019). With hardware based network firewalls, the entire organization can better defend all 150 employee computers on the network. In addition to a network firewall, it is recommended to configure the software firewall on each individual computer as well. Layering these defenses on top of one another will support the IT department in creating the most secure network possible.

**Recommend Resources**

With the number of employees currently in the IT department, the configurations and installations outlined in the preceding recommendations can be performed with relative ease. The three experienced IT employees have the knowledge to perform the enhancements while simultaneously watching over and training the two inexperienced employees. This will enable them to perform similar updates and upgrades in the future, lowering training costs for the company. Due to the fact that system maintenance is only performed weekly on Sunday nights, however, it is recommended that we staff the IT department during offshifts so that maintenance can be performed daily rather than weekly. Staffing during offshifts will also allow the upgrades to system security to be performed more quickly, which is in line with the policy that states that changes need to be implemented in the shortest amount of time.

Resources

cisa.gov. (2019, November 14). *Understanding Firewalls for Home and Small Office Use*. CISA. Retrieved February 20, 2022, from https://www.cisa.gov/uscert/ncas/tips/ST04-004

GeeksforGeeks. (2022, January 17). *Intrusion detection system (IDS)*. GeeksforGeeks. Retrieved February 20, 2022, from https://www.geeksforgeeks.org/intrusion-detection-system-ids/

Tjaden, B. C. (2015). Appendix 1: Cybersecurity first principles. Retrieved from https://users.cs.jmu.edu/tjadenbc/Bootcamp/0-GenCyber-First-Principles.pdf