CYB 420 Project One

Douglas Few

June 1, 2023

Threat Assessment: People

The first vulnerability in the people domain that I identified relates to physical security and locked doors. There are no locks on either of the IT closets and the front door on the first floor is left with open access. This creates a situation where anyone, regardless of authorization level, can enter the building and compromise the CIA triad (confidentiality, integrity, and availability) (Fortinet.com, 2023). Information may no longer be confidential and there may be no more integrity assuming data was accessed without proper authorization.

The other vulnerability that was identified is that of the two remote employees. The ability to access sensitive information for an outside network opens up the possibility for a data leak. If the remote employees aren’t handling sensitive data correctly, such as using encryption when sharing files or ensuring they use a secure connection, data leaks are much more likely to occur (TitanFile.com, 2023). Remote employees are also more susceptible to risks like device theft or other social engineering techniques if they carry their laptops with them in public.

Threat Assessment: Process

The first process vulnerability that I identified is the decision to leave all of the servers in open and unsecured areas. The web server, authentication server, and public records server are all vulnerable to being compromised because anyone is free to walk up and access them. A similar vulnerability that I identified pertains to the network switches. The decision to leave them in the open creates an environment where it is easy for the switches to be stolen or tampered with. If this were to happen, it would be possible for an attacker to gain unauthorized access to the network by connecting their own device to the switch. This would allow them to intercept network traffic or implement a network based attack.

Threat Assessment: Technology

The decision to use network hubs creates a vulnerability in which network traffic is no longer confidential. Because hubs forward packets to every device on the network, any device connected can intercept and read network traffic. Having multiple hubs also opens up the possibility that network traffic will become congested (Tull, 2023). If the second hub was added in order to increase network capacity, the extra traffic may slow down the network’s performance. Bad actors could take advantage of this by flooding the network and implementing a denial-of-service attack.

Another technology vulnerability that I identified is the decision to connect the HR Switch, Finance Switch, and Records Switch together in a bus topology. With this setup, if any of the switches goes out or malfunctions in some way, the remaining switches down the line will also lose connection to the network (GeeksforGeeks, 2023). This lack of redundancy creates a network that is more vulnerable to failures. It also allows each department to access the information of the other departments, thereby impacting the CIA triad.

Adversarial Mindset: People

Employing an adversarial mindset when assessing vulnerabilities in the three risk domains can prove to be very valuable. For any risk domain, using an adversarial mindset involves thinking about how an attacker would see a security system and how they might attempt to overcome it. In the risk domain of people, an adversarial mindset would likely show that employees can be susceptible to social engineering techniques. This could include an attacker convincing employees that they are another legitimate employee, even though they are not. Specific to the ACME Company, this could also include gaining access to the unlocked doors by pretending to be someone with legitimate access.

Adversarial Mindset: Process

When analyzing the risk domain of processes, an adversarial mindset can allow you to better identify weak points in a process. A weak or faulted process can make it possible for a potential bad actor to gain access to information such as client/patient records, billing information, or employee data. In the example of the ACME Company, an adversary would likely notice upon entering the building (which is open to the public) that many network devices are left in visible locations. It would not be difficult for an attacker to enter the lobby and gain access to a network switch or server. While these devices remain easily accessible, a large amount of the company’s confidential information is at risk, and none of the three tenets of the CIA triad are able to be maintained.

Adversarial Mindset: Technology

In the final risk domain, technology, an adversarial mindset can allow you to identify any shortcomings or vulnerabilities with the actual hardware and software used in the network. This can include any outdated devices or programs, or it can simply be the physical topology of the network. In ACME Company’s office building, an adversary would likely notice the use of network hubs and would understand that they could easily gain access to any of the information being transmitted through them. An attacker might also notice the bus topology connecting the switches on the first floor, which means they only need to take out the HR switch to bring the rest of the topology offline.

Organizational Assets: People

The control that was implemented for the first vulnerability in the people domain is simply to add locks to the unlocked IT closets. The decision came down to either RFID locks or biometric locks. RFID locks were chosen due to the ability to quickly and easily replace an RFID card if needed and the lack of difficulty required to administer a new card for a new employee when compared to biometric data (Noori et. al, 2020). While RFID comes with the risk that a card can be lost or stolen, the ability to activate or deactivate the card from a centralized location makes them relatively secure assuming the employees report lost cards in a timely manner.

For the vulnerability relating to the two remote employees, one solution would be to require multi-factor authentication any time access to the server is requested (CISA, 2022). Alongside this, I would recommend that no data be allowed to leave the server or the internal network. In other words, the remote employees should not be allowed to download any data onto their laptops. This will reduce the likelihood that data is leaked from the servers if the laptops are compromised. It would also be beneficial to have the remote employees connect to the server via a virtual private network (VPN) to ensure that all data that is transmitted is encrypted to avoid it being compromised during transit (Kaspersky, 2023).

Organizational Assets: Process

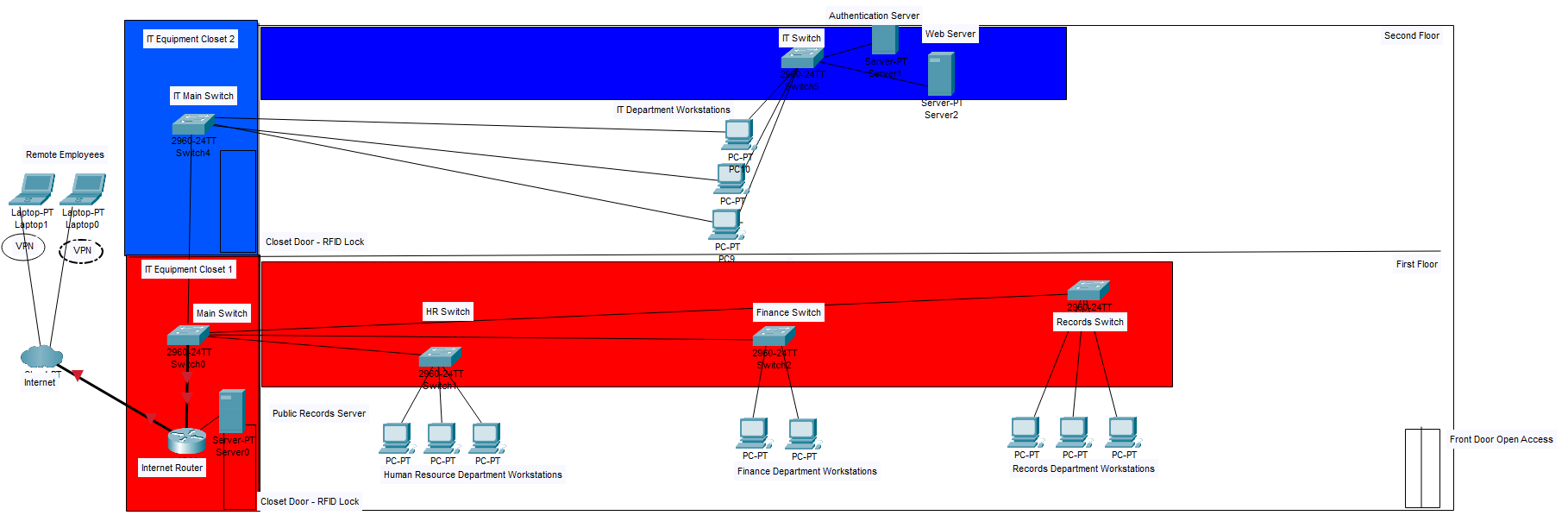
In the risk domain of process, the identified vulnerabilities pertain to the fact that network equipment (namely the switches and servers) are left in the open for anyone to access. In order to fix this issue, I recommend moving all of the equipment into the IT closet which should now be secured via RFID locks. Once the equipment is secured in the closets, only authorized personnel will have access to the equipment, minimizing the ability of bad actors to gain access to the equipment.

Aside from the physical security, another recommendation is to implement network access controls (NAC) so that any device that is not already authorized will be rejected from connecting (Netgear, 2016). This can happen in a number of ways. For example, by enabling the port security feature on the network switches, we can limit the amount of MAC addresses that can connect to the switch. This will make it so only the workstations we have in our building will be able to connect. We can also enable 802.1x authentication on the switches, which requires users to authenticate themselves before a connection can be made (SecureW2, 2022).

Organizational Assets: Technology

The issue with the hubs on the upstairs subnet can be remedied by simply replacing them with switches. Switches tend to be more efficient when it comes to moving network traffic because they are able to send traffic directly to the intended recipient rather than the entire network. Switches are also more secure in that they are able to recognize the destination MAC address of transmitted data and direct it towards the recipient. This is contrary to hubs, which simply broadcast the data to every connected device. This means that if a device were to connect to a hub without authorization, it would have access to all information being transmitted through the hub.

The final issue in the technology risk domain is fixed by changing the topology of the downstairs subnet. Currently, the HR, Finance, and Records switches are connected to the main switch in a bus topology. This is inefficient because it means data has to travel through the entire line before it reaches the last switch on the topology, but it also poses security risks. One node going down in a bus topology can mean that the entire network goes down. To fix this, we will replace it with a star topology. In this orientation, each node will have its own connection to the main switch, allowing for faster and more secure data transmission.



\*for the sake of clarity, the red and blue boxes are extensions of the IT closets.

References

CISA. (2022, January). *Multi-factor Authentication Fact Sheet - CISA*. cisa.gov. https://www.cisa.gov/sites/default/files/publications/MFA-Fact-Sheet-Jan22-508.pdf

Fortinet.com. (2023). *What is the CIA triad and why is it important?*. Fortinet. https://www.fortinet.com/resources/cyberglossary/cia-triad#:~:text=The%20three%20letters%20in%20"CIA,the%20development%20of%20security%20systems.

GeeksforGeeks. (2023, May 11). *Types of network topology*. GeeksforGeeks. https://www.geeksforgeeks.org/types-of-network-topology

Kaspersky. (2023, May 11). *What is VPN? how it works, types of VPN*. www.kaspersky.com. https://www.kaspersky.com/resource-center/definitions/what-is-a-vpn

Netgear. (2016, November 28). *What is Port Security and how does it work with my managed switch?*. NETGEAR KB. https://kb.netgear.com/21786/What-is-port-security-and-how-does-it-work-with-my-managed-switch

Noori, D., Shakeri, H. & Niazi Torshiz, M. Scalable, efficient, and secure RFID with elliptic curve cryptosystem for Internet of Things in healthcare environment. *EURASIP J. on Info. Security* 2020, 13 (2020). https://doi.org/10.1186/s13635-020-00114-x

SecureW2. (2022, October 3). *What is 802.1x? how does it work?*. SecureW2. https://www.securew2.com/solutions/802-1x

TitanFile.com. (2023, May 5). *What is Data Encryption and why is it important?*. TitanFile. https://www.titanfile.com/blog/what-is-data-encryption-and-why-is-it-important/

Tull, R. (2023). *Which is the best network device – hub or switch or router?*. Versitron. https://www.versitron.com/blog/which-is-the-best-network-device-hub-or-switch-or-router