NTW275 Final

Levi Overstreet

University of Advancing Technology: NTW275

NTW275 Final

Here's the scenario. You've been working as a Risk Assessment Analyst in the network security field. One day, you receive a work order for evaluating the network of an insurance office because it has been 10 years since the last one was done. You need do an evaluation of the network as it is provided. Your Senior Risk Analyst has asked for you to create a network configuration to help mitigate the risks the you have identified from your thorough and detailed assessment for the insurance company. What do you do?

Customer Network Specs

Before anyone can begin to evaluate anything, we need to know what kind of network this insurance company has and what it contains. We have been given the following information for what is in the insurance company's network. This network contains sensitive PCI and PII customer data. The network consists of 5 servers with 4 of them having Windows Server 2016 OS installed on them and the other one having Windows 2013 OS, spanning 2 branch offices. As for the devices connected to this network, there are 50 endpoint devices with 45 of them running Windows 10 OS and the remaining 5 running Windows 7 OS, 50 VoIP connections, and 5 printers. And there is a total of 35 employees that utilize this network. This is all the information we have been given and it seems that we're unable to physically inspect the network. We will need to make our evaluation based upon all the information that has been given to us.

The Evaluation

This is where the fun begins. Now, because we're unable to physically inspect the network and gather all details so that we may give an accurate evaluation, we will be making some educated assumptions with the information we have. Firstly, it has been 10 years since this insurance company's last risk assessment. From that we can assume that the equipment and

software in use within this network is at least that old if not older. We should also assume that the equipment is stored and ran on the premises at one of the branch offices. From that assumption we should also assume that which ever office is housing the network equipment is not staffed 24/7 with any employees and that the other branch office is not connected in a secure and encrypted means to the location housing the network. We will also need to assume that at least a few of the 35 employees are able to remotely access the company network given how most businesses operate now a days as well as assume that the insurance company does not employ any inhouse sysadmins due to the age of some of the operating systems still being used within the company. And we need to assume that the PCI and PII customer data that is stored in one of the servers is not encrypted and not backed up. After making those assumptions we can move on to the hard information we have as well. We have 5 servers with one of them running an outdated operating system. All of them are close to the End of Life date provided by Microsoft, for the 2013 OS being in 2023, if they have a support extension applied, and for the 2016 OS's being in 2022 (Windows Server Lifecycle, n.d.). For the 50 endpoint devices, there are 7 that are currently running an unsupported OS (What happens when Windows 7 support ends, 2020). And the network has 50 VoIP phones and 5 printers that we will need to secure. Even with the minimal information that we were provided we can make a halfway decent evaluation. And with that we can plan fixes to this network that will cover all our assumptions but at the same time can be modular in the sense that any one suggestion can be implemented or not without causing issue for any of the other suggestions.

The Plan

It should first be said that any and all suggested fixes are based upon my own firsthand knowledge and experience. We have also not been given any kind of budget to stay within with

this request so we will be coming at this from the point of making this a network that meets current industry standards. With that out of the way we can move on to fixing the issues with this network, starting with the physical equipment, the location it's housed at and that environment's viability for network equipment longevity. If we're assuming that the 5 servers were placed into production 10+ years ago and that they are housed at one of the branch offices, then we can begin to make proper recommendations. For instance, we wouldn't want to have the equipment stored on site at one of the offices. In most cases you find server and network equipment stored in a small closet with little to no cooling or ventilation and no power redundancy. These are very important environmental components to take into consideration with a network to help lower the risk of potential outages either due to loss of power or overheating. The ideal location would be housing the equipment at a data center with guaranteed redundant power and cooling at that facility. Along that same note you would also want to have a secondary offsite setup to mirror the first one so that if anything were to happen to cause disconnection from the primary site then your network would failover to the secondary site with minimal downtime. We will also want to make sure that each server is built to have redundant power as well as built with multiple hard drives in a redundant RAID configuration as well as updating to the most recent server OS, Server 2019 to take advantage of the extended life time support as well as the improved security features included with Server 2019. We should increase the number of servers to at least have one as a dedicated File Share or Data Base server with high level encryption to address the protection of the PCI and PII data. We would also want to implement some NGFW hardware/software into the network topology as we relocate and rebuild the current network infrastructure to help protect it from unauthorized outside access. With these changes addressed we can then move on to the issues we found within the two branch offices. First thing we need to

do is update the 7 endpoint devices to Windows 10 to bring them into a supported state. We will want to check and make sure that the 5 printers are updated with their latest firmware as well as being hard wired into the office network and disabling any WIFI connectivity to them. We will also want to confirm that one of the servers is a dedicated VoIP server that is up to date or again increase the server count to include a dedicated VoIP/printer server. Some of these suggestions can seem very big but with some planning these can be implemented with minimal down time to the company and having the added benefit of addressing any other small or unforeseen issues not initially caught with this assessment. This is achieved by taking current backups of the company's data, building out the new network infrastructure and then doing a cutover to the new network with the backups now acting at the main data point. Then it is a minimal logical migration of data for anything remaining to the new infrastructure. Now one of the biggest issues to address is making sure that the company network is manned by trained sysadmins on a 24/7 basis. These sysadmins can either be employed inhouse with the insurance company or they can be provided by a professional support company that deals with managed services. This will make sure that the company network is fully covered incase anything happens. All these changes are to mitigate any disruption to the business and loss of data.

The suggestions made within this evaluation and risk assessment are meant to help inform of potential risks and how to best mitigate those perceived risks. These suggestions are also modular so that they can be implemented all at once or piece by piece. The goal is to fully cover and protect the network, to minimize any down time or loss of data, and to safeguard all customer PCI and PII data from theft. There is no such thing as 100% security but with these measures in place the risk impact is greatly reduced to a more manageable tolerance.

References

What happens when Windows 7 support ends?. (2020). Retrieved from https://support.microsoft.com/en-us/help/4467761/windows-what-happens-when-windows-7-support-ends#:~:text=After%2010%20years%2C%20support%20for,including%20security%20updates%2C%20from%20Microsoft.

Windows Server Lifecycle (EOL). (n.d.). Retrieved from https://endoflife.software/operating-systems/windows/windows-server