Risk Assessment for [REDACTED]

Jose Ramirez

University of Advancing Technology

**Risk Assessment for [REDACTED]**

The company [REDACTED] has contacted us about a risk assessment needed for their environment. We are looking at their whole environment and determining what can be fixed and what can be replaced. Some of the areas we are looking to assess are their data protection, this includes any PPI and PCI information. The servers and clients they are using, alongside any other device in the network. Finally, we are also looking at some forms of risk coming from the company’s employees.

# PCI and PII Data Handling and Storage

PCI and PII data should never be seen or handled by unauthorized individuals. This data needs to be encrypted while at rest and while it is being transmitted. The company [REDACTED], was able to successfully demonstrate the transmission of encrypted information. Although their data transmission is encrypted, we were able to find readable information on the servers. We recommend encrypting the information while it is at rest, depending on the OS, this can be done either through built in features or through 3rd party software. Most of the clients and servers used at [REDACTED] are running Windows, which means a good temporary solution would be turning on BitLocker. Eventually, we recommend using a 3rd party program such as VeraCrypt for data encryption, especially since BitLocker will not work on devices that do not have a TPM installed.

Another problem we saw at [REDACTED] is the amount of information sharing that is done without regulation. We believe there needs to be an access control policy to limit the amount of information being accessed and shared. Since [REDACTED] is a [REDACTED] company, we can assume each user has access to their own clients’ files. If the file contains PII or PCI information, anyone requesting access to the information needs to contact the current employee handling the information and management. If approved, the information should not be shared by the user requesting the information. This should help keep track of who has access to what in the environment. If a user does not need access, they should not have it.

# Branch Assessment

[REDACTED] is a [REDACTED] company that is split into two branches. One of the branches is the main office used by most of the employees, this is where management and the claim assistants work. The second branch is a smaller office used by the IT team and the security team. Both buildings are right next to each other, so the connection between the buildings is physical. The IT branch houses some of the company servers, two of the 2016 servers to be exact. The main branch houses the other three servers, two of the 2016 servers and the 2013 server. As stated before, all information being transmitted is encrypted, but the information at rest on the servers and devices needs to be encrypted. The routers and switches being used at the branches are Cisco devices. I recommend creating some VLAN’s to segment the network, separating the claims offices from the management offices. These VLAN’s can then be used to filter traffic through a firewall, each office can have access to the resources they need.

Sadly, we could not find any firewalls in their environment, this is a huge risk they are creating. We immediately recommend them to acquire some firewall devices alongside an IPS system. We recommend Palo Alto devices, but they are expensive, so a smaller Cisco firewall appliance could work as well. If an IPS is implemented, a relatively free and open source piece of software that can be used is Snort. When configured correctly, Snort can be a very powerful and useful implementation. The firewalls would filter out any unwanted traffic and anything else that needs to be filtered can be done by Snort. Snort is also able to detect malicious activity, so using it for redundancy is also an option. If need be, a VPN connection can be made between both branches, this can be used to access company resources on the main branch or server access into the IT branch. A VPN can also be used to isolate certain devices such as VoIP devices and printers.

We would also like to see some physical security implemented to the company, we think the building is too open and exposed to outside threats. A keycard system can be implemented to block and allow access to certain areas of the office. Security cameras can also be implemented throughout the building, inside and outside. The camera footage can be reviews weekly and disposed of if not needed. We also recommend hiring a couple of security guards to keep the building entrances secured.

# Servers Assessment

The servers found at [REDACTED] are four 2016 servers and a single 2013 server. Although the servers are patched, they are old, and they need to be replaced. Especially the 2013 server, this is a 7-year-old server that is holding unencrypted information. The 2016 servers can be replaced as time goes on, but for the meantime the data found on them needs to be encrypted. All the servers are internal, except for the mail server, which should be protected by a firewall or an IPS. The rest of the servers require basic domain authentication to get to, we recommend adding multi-factor authentication to access the company’s resources. As said before, the environment needs firewalls and an IPS to protect the servers and the other devices in the network.

It’s good to see the servers are up to date, but we recommend testing any big updates or any changes that may need to be performed to the servers. This can be done on an external environment on the cloud. A problem we did find was the servers were not in a special room designed to cool servers and were easily accessible to anyone inside the buildings. If a threat was able to gain access to the building, they could upload malicious files onto the server or steal information. Creating a secure server room, fitted with proper air conditioning and key card access, could be costly but would improve the server’s security and lifespan. If this is not possible, the previously talked about key card system can also be implemented to the pseudo server room. The access control talked about earlier can be introduced to server access, only specific users can perform certain action on the servers.

# Client and Other Device Assessment

Let’s start of with the clients, as said before, none of the hard drives in the environment were encrypted. The information kept and used on these clients contains PII, therefore it should be encrypted and secured properly. Since the company did not have any firewalls, at least an anti-virus would have been good to see on the clients. Alas, the clients had no anti-virus installed and the USB ports were set to autorun, this means if a threat was able to get into the building he could get to a client and run malicious code with a USB storage device. The first step to solving this is turning off autorun, the second step is installing an anti-virus onto the clients. We recommend going with Bit Defender Enterprise edition or Malwarebytes, Sophos also offers a cloud based anti-virus.

The Windows 7 clients have got to go. Unless there is a critical reason on why these clients should stay, we recommend replacing them with Windows 10. These clients are outdated, and they are no longer supported by Microsoft, which means they are a liability they will be harder to maintain than their Windows 10 counterparts. They are also non-complaint to PCI and PII standards. Not only are they harder to maintain and non-complaint, but they are vulnerable to any new or current attacks that target Windows 7. Upgrade them as soon as possible. If they can’t be upgraded, we recommend isolating them from the network as a temporary solution. As part of the access control implementation, as previously stated, we recommend segmenting the branches and offices. The clients that are part of the claims department should be in a VLAN, the clients on the management side of things should be in a VLAN, and the IT branch should be in their own VLAN as well. The firewall can then be used to control traffic between VLAN’s.

The printers in the environment are not secured with a password, this means anyone with network access could use them. Although this is bad, unnecessary printing is the least of our concern, the information sent to the printer can be intercepted and stolen. We recommend creating a password policy for the environment, everything in the environment should comply with the policy. An 8-character password that needs to contain 1 special character, 1 uppercase letter, one number, and 1 lowercase letter. We also recommend implementing multi-factor authentication to the company resources. These printers need to be isolated in a VLAN as well, if they are compromised, the culprit will not have immediate access to anything else on the network.

The VoIP devices found on the network raised a lot of concerns. Basic authentication was enabled on the devices, but we recommend multi-factor authentication. The authentication should comply with the password policy as well. The devices, alongside everything else on the network, are not protected by a firewall. The devices should be in their own VLAN, the traffic should be managed differently from the client and server traffic. All data transmitted and stored on the devices should be encrypted, this means the traffic heading out of the network should be using the Secure Real-Time Transfer Protocol. The traffic should be monitored, and any anomaly detected should be looked at immediately.

# Employee Assessment

Finally, we can assess employee risk, we have a few things to say about the employees at [REDACTED]. As talked about before, everyone is sharing information with each other, there is no control over what should and should not be shared between employees. Training needs to be set in place, we believe this can be done with the help of a third-party program. There are plenty of companies that specialize in employee training, we would also like to see some security awareness training alongside any other employee training needed. Employees should be trained on recognizing anomalies and phishing emails, one of the biggest attack vectors used by threats is malicious emails. If an employee were to open a malicious document, it could infect the machine with malware, which could give an attacker full control over the machine. Employees should be trained to report anything suspicious and should be praised for doing so.

It’s good to some health insurance being offered by the company. Something we noticed was the outdated evacuation plan they have posted on their exits. We recommend going over this plan and updating it with any new procedures that need to be implemented. Emergencies are unexpected, and if the evacuation plan is not up to date, a terrible outcome can be expected. We don’t specialize in BCDR, but we recommend having a good plan in place. Natural disasters can cause large amounts of unexpected damage to the company’s assets, it’s good to have a plan for coming back from such disasters.

References

Brown, J. (2019, November 21). Employee training and development (From A to Z). Retrieved from https://helpjuice.com/blog/employee-training-development

Cisco. (2018, February 15). Catalyst 4500 series switch Cisco IOS software configuration guide, 12.2(25)EW. Retrieved from https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4500/12-2/25ew/configuration/guide/conf/vlans.html

Cisco. (2020, March 20). How to protect your voice: Tips on IP phone security. Retrieved from https://www.cisco.com/c/en/us/solutions/small-business/resource-center/security/tips-ip-phone-security.html

Coloff, C. (2016, December 5). PII, PCI & PHI compliance and your business - NJ | IT radix. Retrieved from https://www.it-radix.com/2016/12/05/10936/

Windows 7 support ended on January 14, 2020. (2020, January 14). Retrieved from https://support.microsoft.com/en-us/help/4057281/windows-7-support-ended-on-january-14-2020