An Enterprise-Wide Solution for Rebound Security

M. Fitzhugh

redeyesyami@yahoo.com

Columbia Basin College

CSIA 450 – 8372 Cyber Security Capstone

Spring 2020

An Enterprise-Wide Solution for Rebound Security

Introduction

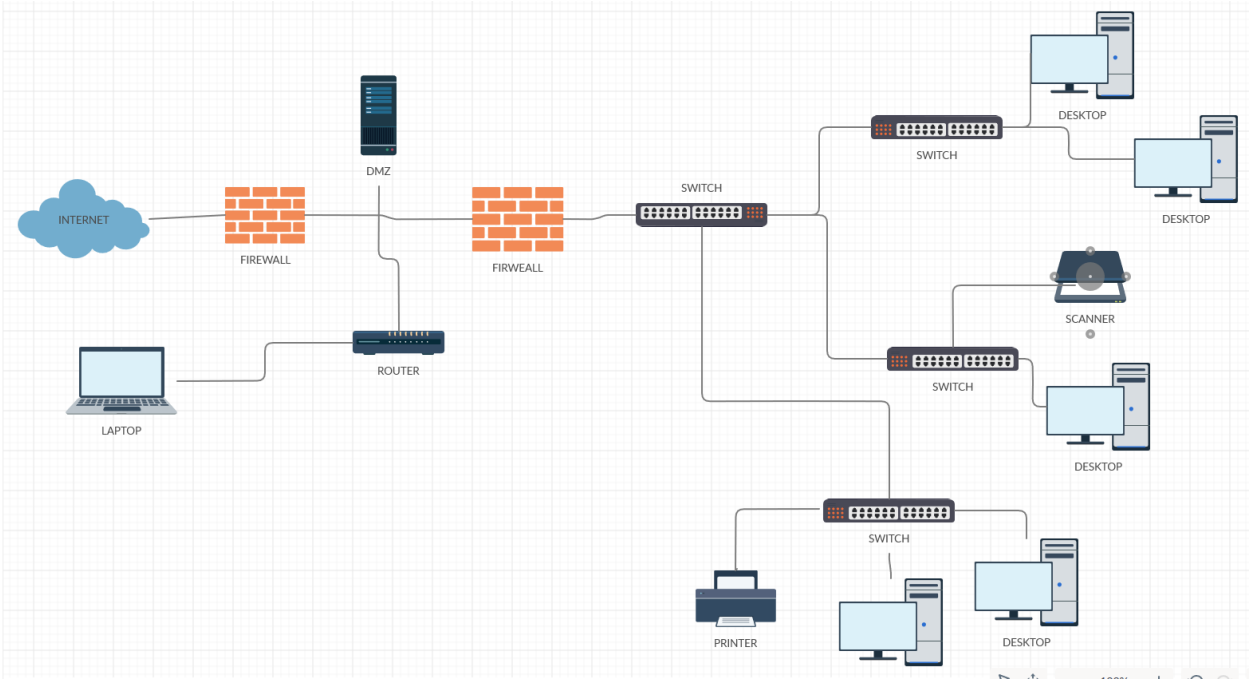
The purpose of this project is to write an enterprise-wide solution proposal for Rebound Security. Rebound Security is a small security firm of 200 employees that expects to grow to 350 employees in a year's time. With the expected growth of employees, the firm plans to have their offices span a total of three floors. All Rebound Security's employees have Windows 10 computers that are not currently connected to the corporate Local Area Network. There is a third of employees that have laptops and travel often. The proposal will include: a design of basic network topology; a developed IP infrastructure; recommended security controls; and an analysis on web port accounts,

Network Topology

According to SolarWinds Worldwide, "the configuration, or topology, of a network is key to determining its performance." The network topology that will fit Rebound Security and its expected growth is a Star Topology. Star topology is perfect for growth, allowing up to 1024 nodes (computers, printers, and other devices) to connect (Caputo, 2010). With Rebound Security planning to span three floors, the Star Topology can be adapted into a spanning tree topology, having nodes segregated into groups, one for each floor. On each floor, each node will connect to a switch, and each switch will, connect the central switch. This will allow for each device to be able to communicate with other devices, including printers and scanners, located on their floor as well as the other floors. Switches allow multiple device connections, and will accommodate Rebound Security's current number of employees and future growth, as more switches and devices can be added to the network as needed,

Rebound Security's LAN should also include a router, firewalls, and a DMZ (demilitarized zone) for the web application. Below is a basic diagram of how I recommend Rebound Security set up their network. The inside of the network will consist of all Windows computers, printers, scanners, and any

other devices, as well as the switches used to connect them. As explained above, this star topology will allow for each device to be able to communicate to each other. Each switch will connect to a central switch. The outer perimeter of the internal network will be a firewall. This firewall will protect the internal network and monitor any internal threats. There should also be an external firewall that will prevent unauthorized access from the internet and devices outside the network. Between these two firewalls we be where the router and DMZ are located. Having the DMZ and router located between the firewalls will allow for devices to connect to the web application without having to access the LAN. Having a router will allow for devices to connect remotely.



Rebound Security having Windows 10 computers will allow for easy use of file sharing options in Windows Network Sharing Settings (Rusen, 2019). Windows also has a feature called Windows Remote Desktop Connection (RDC) will allows a user to connect remotely to a computer located in Rebound Security's local area network (LAN, LearnTomato, 2015).

IP Infrastructure

My recommendation for Rebound Security's network's IP infrastructure is to use Dynamic Host Configuration Protocol (DHCP). DHCP is "a client/server protocol that automatically provides an Internet Protocol (IP) host with its IP address and other related configuration information such as the subnet mask and default gateway (Microsoft Docs). DHCP is an automated process that is managed locally; the DHCP server has a pool of IP addresses that it leases out to clients who connect to the network (Microsoft Docs). DHCP is an easy and convenient way to assign IP addresses to all client devices that Rebound Security's employees use. DHCP efficiently handles IP address changes for portal client devices that move to different locations (Microsoft Docs); which is great for the employees that travel.

Recommended Security Controls

Below, is a list of recommended security controls for Rebound Security for specific control areas.

<u>Social Engineering/internal Threats</u>

To combat social engineering, Rebound Security should have User Awareness Training. This training should include how to spot and avoid falling victim to phishing emails and keeping passwords safe and secure by not sharing them or allowing others to use one's credentials. Even with proper training, mistakes can still happen. Rebound Security should ensure all client devices are using firewalls, and that all software is up to date (Ford, 2018).

To combat internal threats, Rebound Security should have an account management policy, a user monitoring policy, and a password management policy (Netwrix Corporation, *Best Practices to Minimize the Risk of Insider Threats*). An account management policy helps prevent internal threats by disabling accounts upon employee termination so that the former employee cannot access company information. It will also ensure user accounts have proper privileges, including the principle of least

privilege—that way users can only access the company information they need to do their job. A user monitoring policy can detect changes such as permission escalations, and non-normal logon times, which could indicate the account is being used to gain access to sensitive information. A password management policy is important because it contains rules such as password expirations. This is important because should a user obtain the password to a higher privilege account, they will not have continued access as eventually that password will expire.

IDS

An Intrusion Detection System (IDS) is important for a network to have. An IDS "can notify you of any configuration errors, infections, viruses and unauthorized access" (Alarm.com). Having these notifications will alert the network administrator to any problems and allow them to quickly respond to mitigate the issues.

DLP

Data Loss Prevention (DLP) can be defined as "technology or processes that: identifies confidential data; tracks data usage; and prevents unauthorized access to data" (Brook, 2019). It is important for Rebound Security to have a DLP Policy in place to protect confidential information, as the company has over 200 employees, and a third of these employees have laptops with remote access. A basic DLP policy covers: what data needs to be protected; where the data is stored; who has access to which data; steps taken when suspicious activity is detected; how to archive data and when; and possible threats and which to mitigate (Melnick, 2020).

Authentication Mechanism(s)

Based on the data found in Portal_UserList.csv, it is clear Rebound Security already uses the Password authentication mechanism. This is great as passwords help to keep user accounts, and the

data they can access, secure. Rebound Security should make sure they have clearly defined password policies to ensure it is not easy to guess a user's password. Password policies that should be in place are: minimum password length; enforce password history; minimum password age; maximum password age; enable password complexity (Netwrix Corporation, *Best Practices to Manage and Setup Password Policy*).

Vulnerability Assessment

Imperva defines a vulnerability assessment as "a systematic review of security weaknesses in an information system." It is important for Rebound Security to create and implement Vulnerability Assessments to find and mitigate risks to their network. A basic Vulnerability Assessment covers:

- Testing – testing applications, servers, and other systems for vulnerabilities;
- Analysis – identifying the cause of the vulnerabilities;
- Risk Assessment – prioritizing vulnerabilities by what system is affected, what data is at risk, the likelihood of an attack, and the possible damage from an attack;
- Remediation – mitigating or remediating higher rank vulnerabilities (Imperva).

Web Portal Account Analysis

Rebound Security has several issues it needs to address for its web portal accounts. The highest risk is lack of a password aging protocol. According to Portal_UserList.csv, there are several accounts who have not changed their password since December 2014, and most of those accounts are active. Below is a screenshot of the accounts with the oldest passwords.

UserName	PasswordChangedDate	Status
naveen.mohan123@emids.com	12/11/2014	PendingPassword
abc123@gmail.com	12/12/2014	PendingPassword
xyz123@gmail.com	12/12/2014	PendingPassword
arunkumar.bangalore@medsolutions.com	12/13/2014	Active
anand.mahadevappa@medsolutions.com	12/15/2014	Active
carecore730@yahoo.com	12/16/2014	Active
sanju.nagaraj@medsolutions.com	12/16/2014	Active
ankit.mahakul@medsolutions.com	12/17/2014	Active
gwen.montgomery@medsolutions.com	12/17/2014	Active
abhishek.pulast@medsolutions.com	12/18/2014	Active
june.stansberry@premierradiology.net	12/18/2014	Active
Marisa.Anderson@Premierradiology.net	12/18/2014	Active
susan.moore@premierradiology.com	12/18/2014	PasswordExpired
susan.moore@premierradiology.net	12/18/2014	AccountSuspension
jerry.guel@vanderbilt.edu	12/19/2014	PendingPassword
kenny.thurman@vanderbilt.edu	12/19/2014	AccountSuspension
susan.fitzgerald@Vanderbilt.edu	12/19/2014	Active
charlotte_test.young@medsolutions.com	12/30/2014	PendingPassword

There are many more active accounts who have not changed their password in over five years. Changing passwords is important because it helps to prevent constant access from a hacker if they obtained a user's password, as well as helping prevent a user from using another user's stored password if they've changed computers, and it prevents access gained from a keystroke logger (Information Technology Services, 2017).

Another issue of Rebound Security's web portal is user account names. From the data found in Portal_UserList.csv, it stems to reason there is no naming standard for accounts. The picture below shows there are several accounts with variations of "areed" as well as "areeves."

48765	areed@cpspain.com	8/25/2017	Active
48766	areed@tampabaysurgicalgroup.com	2/14/2018	Active
48767	areed001	11/26/2019	Active
48768	areed0712	7/21/2017	Active
48769	Areed1491	7/16/2016	Active
48770	AREED18	12/26/2019	Active
48771	areed1986	1/17/2019	Active
48772	AReed2014	7/16/2016	Locked
48773	AReed2018	10/3/2019	Active
48774	areed2019	6/5/2019	Active
48775	areed395	4/12/2018	Active
48776	AREED444	12/11/2019	Active
48777	areed922	6/5/2019	PendingPassword
48778	AReed99503	10/16/2018	PendingPassword
48779	AReeder	12/31/2019	Active
48780	areeder19	2/17/2020	Active
48781	areedhoope	1/14/2020	Active
48782	areednkpt	12/31/2019	Active
48783	areedy	2/14/2020	Active
48784	areeger1	12/19/2019	Active
48785	areel01	12/3/2019	Active
48786	areen713	2/20/2020	Active
48787	Arees2000	8/2/2018	Active
48788	areese@challiance.org	11/15/2019	Active
48789	areese10	7/16/2016	Active
48790	areese1002@yahoo.com	2/27/2016	Active
48791	aReese12	7/16/2016	Active
48792	areeves@centralcarolinaortho.com	1/23/2018	Active
48793	areeves10	7/16/2016	Active
48794	areeves16	4/14/2017	PendingPassword
48795	areeves200	2/13/2020	Active
48796	areeves2018	5/29/2019	Active
48797	areeves28	7/16/2016	Active
48798	areeves39	7/16/2016	Active
48799	areeves69	2/25/2020	Active

Rebound Security is a small business of 200 employees, and this user list file has hundreds of thousands of usernames listed. It is possible that some of the employees have created multiple user accounts for a reason such as they forgot their login and created a new one. It is also possible that some of these accounts belong to former employees. The problem with these examples is that most of these accounts

are listed as Active. This provides a huge risk to Rebound Security because a hacker could obtain those user account credentials and logon to the web portal. A way to mitigate this risk is to have a standard naming protocol. Having a standard naming protocol makes the administrators job easier, as well makes it easier for users to remember their logins (Active Directory Pro, 2020). Rebound Security should also impose an inactive account policy, where accounts will be disabled after a set amount of inactive days. Doing so will prevent that account from logging into the web portal, should a hacker obtain the inactive accounts credentials.

Conclusion

In this project I gave recommendations for how Rebound Security should set up their LAN. These recommendations included what devices to use to connect employee devices and how the topology should look. Included with these recommendations were policies on IP address assigning, as well as security controls to employ to ensure Rebound Security's data stays secured. The project ended with recommendations for further securing user accounts from the web portal. These recommendations were done with security in mind and accounted for future company growth.

References

Active Directory Pro. (2020, February 25). Active Directory user naming conventions. Retrieved June 02, 2020, from https://activedirectorypro.com/active-directory-user-naming-convention/

Alarm.com. (n.d.). Prevention and Detection: Does Your Business Need IPS, IDS or Both? Retrieved June 02, 2020, from https://www.vectorsecurity.com/blog/prevention-and-detection-does-your-business-need-ips-ids-or-both

Brook, C. (2019, December 05). Establishing a Data Loss Prevention Policy Within Your Organization. Retrieved June 03, 2020, from https://digitalguardian.com/blog/establishing-data-loss-prevention-policy-within-your-organization

Caputo, A. C. (2010). Understanding Networks and Networked Video. Retrieved June 02, 2020, from https://www.sciencedirect.com/topics/computer-science/star-topology

Ford, N. (2018, August 31). GRC eLearning Blog. Retrieved June 02, 2020, from https://www.grcelearning.com/blog/5-ways-to-mitigate-social-engineering-attacks

Imperva. (n.d.). What is Vulnerability Assessment: VA Tools and Best Practices: Imperva. Retrieved June 03, 2020, from https://www.imperva.com/learn/application-security/vulnerability-assessment/

LearnTomato. (2015, April 16). Setup a Remote Desktop Connection for LAN / WAN Access. Retrieved June 03, 2020, from https://learntomato.flashrouters.com/setup-remote-desktop-connection-lan-wan-access/

Melnick, J. (2020, March 27). 10 Best Practices Essential for Your Data Loss Prevention (DLP) Policy. Retrieved June 03, 2020, from https://blog.netwrix.com/2019/07/16/10-best-practices-essential-for-your-data-loss-prevention-dlp-policy/

Microsoft Docs. (n.d.). Dynamic Host Configuration Protocol (DHCP). Retrieved June 03, 2020, from https://docs.microsoft.com/en-us/windows-server/networking/technologies/dhcp/dhcp-top

Netwrix Corporation. (n.d.). Best Practices to Manage and Setup Password Policy. Retrieved June 03, 2020, from https://www.netwrix.com/password_best_practice.html

Netwrix Corporation. (n.d.). Best Practices to Minimize the Risk of Insider Threats. Retrieved June 02, 2020, from https://www.netwrix.com/Insider_Threat_Prevention_Best_Practices.html

Rusen, C. (2019, May 01). Customizing Your Network Sharing Settings. Retrieved June 03, 2020, from https://www.howtogeek.com/school/windows-network-sharing/lesson3/

SolarWinds Worldwide, LLC. (2020, May 13). What is Network Topology? Best Guide to Types & Diagrams. Retrieved June 02, 2020, from https://www.dnsstuff.com/what-is-network-topology

M. Fitzhugh

CSIA 450 – 8372 Cyber Security Capstone

Spring 2020

Project Deliverable 2: Retrospective

A. What worked well for you?

What worked well for me was having a period of three weeks to work on this paper. This length of time provided me enough time to research and write my paper, as well as submit it for review, with time to edit before the due date.

B. What did NOT work well for you?

The premise of the paper did not work well for me. Network designing is not my strong point and is not something I would like to do for a career.

C. What actions could you take to improve your work for the next project?

An action I could take to improve my work for the next project would be to reach out to my peers. Talking with my peers, who are in the same boat as me, may help to provide additional insight into the project as well as possibly giving me ideas on what to write about.

D. What did you learn most about yourself from this project?

What I learned about myself was I needed to change how I approached difficult project topics. Thinking about the project as a whole and how I was going to write it was stressful. Breaking it down into sections and researching and writing about those sections made it easier to deal with.