**Secured Network Design for Home Depot**

Mecahel Demissie

Department of Computer Technology, Bowie State University

CTEC 345: Foundation of Computer and Network Security

Prof. Latson

May 17, 2020

Table of Contents

Abstract---------------------------------------------------------------------------------------------------------3

Introduction to Company-------------------------------------------------------------------------------------4

NIST Phase 1: Identify---------------------------------------------------------------------------------------5

NIST Phase 2: Protect----------------------------------------------------------------------------------------6

NIST Phase 3: Detect-----------------------------------------------------------------------------------------7

NIST Phase 4: Respond--------------------------------------------------------------------------------------8

NIST Phase 5: Recover---------------------------------------------------------------------------------------9

Security in Network Design Explained-------------------------------------------------------------------10

Scenarios for Attacks----------------------------------------------------------------------------------------11

Appendix A: Network Design Explained ----------------------------------------------------------------12

Appendix B: Subnetting------------------------------------------------------------------------------------13

Appendix C: Acceptable Use Policy----------------------------------------------------------------------14

Appendix D: NIST Framework----------------------------------------------------------------------------15

Appendix E: Network Design Pictures-------------------------------------------------------------------16

References----------------------------------------------------------------------------------------------------19

Abstract

In 2014, Home Depot found out that there was a malware program in their cash registers that stole credit card information from customers. Since then, the company has paid a lot of money for compensation for the attack and was at a major setback point. None of this would have happened if the network had programs and protocols that could find malware programs within the scope and protect themselves with authentication and authorization. This paper will describe the design created for this network and how malicious programs or intruders may not enter the network due to enforced security of the company’s network. This paper will also enlighten the reasoning of what nodes and protocols were added, used and how they help the network.

Introduction to Company

The company based on the security network design is Home Depot. Home Depot is known for selling building materials for construction and products for improving your home, they also have installation services for your house, other services like rentals for tools and equipment, and decorations for lawns and gardens. The company has an estimate of around 400,000 employees in North America with Atlanta, Georgia being the headquarters. After a security breach in 2014 the company lost millions of dollars for compensation for the attacks. In the design, the company is following the policies in the National Institute of Standards and Technology (NIST) Framework. This framework will help with all aspects of security from employees, to hackers, and natural disasters.

NIST Phase 1: Identify

In Phase 1 of NIST you have to identify. Identify who is in your network, what they are conducting in the network, who they are sending messages to, and what they have access to. Identifying users is helpful because you can pinpoint whoever sent that message to other devices and what is in it. To identify every user, we would need authentication, which is that every user needs credentials to log into the network. This can help the database understand that the person logging in is an employee and has access to the network. When the database finds the credentials for the employee they can see what files they have access to and what they can’t access due to the hierarchical ranks of employees. This network would also run background checks for employees to see what programs they have opened up and look at their search history when users log in.

NIST Phase 2: Protect

The next phase of the framework is to protect. Employees need to protect sensitive data that cannot be access by an untrusted device. Sensitive data can include accounting for employees and user credentials to log into the network. Employees of higher level can enforce access control, where they can approve other employees to use resources they want them to. The model of access control that seems good for this company and used is Role-Based Access Control (RBAC). This model helps with finding out what roles do employees have in the network by first setting permissions for roles then assigning users to those roles. For example, a system administrator permits an employee to access the network and that is all they can do. When the user tries to access a file like “useraccounting” for example, they do not have access to it and the system administrator protects that file from untrusted users. Employees will also be trained on who can give permissions to what and who are privileged to access secure resources.

Firewalls can be used to protect the network also from malicious programs including malware and viruses. The network design has firewalls on connections before entering each building and between DMZ zones.

NIST Phase 3: Detect

The third phrase of the framework is to detect. NIST describes the Detect phase as “the development and implementation of activities “to identify the occurrence of a cybersecurity event,” with a focus on supporting the timely discovery of such events.”[[1]](#footnote-0) When you are a system administrator of a network you need to detect what goes in and out of the network. This includes programs installed by a user, the messages being sent, and what tasks are running. Employees must be aware when every single task is being asked to run and what time they run. System admins should be able to see the properties of the program in the user’s account to see when the program was last used.

NIST Phase 4: Respond

The fourth phase of NIST is to Respond. This is after an incident and how the company responds to the public on the event that happened, using a real event that happened with Home Depot they had a security breach in 2014 within the Point-Of-Sale network where there was a malicious program in it and took credit card credentials which cost them $179 million, this was also known as “the largest point-of-sale heist of all time, as well as the biggest credit-card compromise ever seen”.[[2]](#footnote-1) Home Depot responded to this attack by giving out $134.5 million in compensation to credit card companies and banks, then removing the malware. Home Depot then offered identity protection to customers that paid with a card from April 2014 to the end of 2014, while training the employees to never have this incident happen again by learning their lesson. Home Depot did everything they could to give back to the customers and that’s what should be done in a case like this, they have trained their employees for the next incident and will develop a plan for whenever something like that happens again.

NIST Phase 5: Recover

The fifth and final phase of NIST is to Recover. Recovering in computer terms is to have a copy of an earlier state of the node. This is needed in the framework in case if things go wrong and the network shuts down, all configurations for devices will be lost and connections would have to be reestablished. Databases of users, mail, and accounting will be lost too which will leave the company in shambles. If there was no backup, employees wouldn’t know which customers rented equipment from the stores and they would lose profit. This phase of the network would help the company in making sure the network will stay safe in case there was a shutdown or maintenance. It is recommended to have scheduled backups in case the network crashes out of nowhere and you can just bring it back with a recovered backup.

Security in Network Designed Explained

In the network, there are devices that will help maintain security throughout the nodes. Security has been layered by adding antivirus programs on every PC, and firewalls before each building when connecting the edge routers to the core routers. The network also has a demilitarized zone (DMZ) where it is separated from the network so when untrusted devices access the DMZ, they only have access to the DMZ but not the network. In the Packet Tracer design, the DMZ zone shows to have two firewalls, one from the internet to the DMZ routers, and the DMZ routers going to the core router. The DMZ routers also have servers which are accessible to the public like the mail server, FTP server, and HTTP server, this is because the network would want to give access like this to the public, for example, they have the mail server in the DMZ zone in case users want to email employees about customer service in stores or update on rental equipment. Each building has a RADIUS server within them which admits permission to new devices after providing authentication by username and password, this helps employees see who wants to join the network. All switches have been configured with port security so only the amount requested, which in the design is eight, can be approved by the switch and if more MAC addresses are connected then they will be ignored since they are untrusted. The routers are configured with Access Control List (ACL) by filtering what kind of data is permitted into the network, although this is very strict for employees, it enforces security and has slightly less chance of malware from sneaking into the network.

Scenarios for Attacks

A hacker breaches into the company’s database where they can see the rentals of equipment and information of the customer renting the equipment. The hacker downloads the data of customer information to sell online.

This can be stopped by the many firewalls within the network and protocols used by switches and routers. The hacker would not get access to the LAN information from each building but only servers in the DMZ zone including mail, HTTP, and FTP servers.

Another scenario is where a script kiddie can use a script on a trusted customer and get into their account to talk to an employee. The employee would try to talk to the hacked customer and the script kiddie could try to send a script giving the employee a malware program.

If the employee falls into the trap, the PC the employee is using has an antivirus program that can detect the malware and alert the user, the user can then delete the malware and backup the computer to its original state.

Appendix A: Network Design Explained

The United States map will be used for the design of my WAN topology. Because Home Depot has a lot of locations and at least one location in every state, The WAN topology was considered to be a star topology. A star topology is good for companies with lots of locations and network traffic so every site can be connected to the central hub, looking at the United States map you can see the headquarters is in the South-East part of the map, data sent from there to California would take longer than normally so a central hub located in the middle of them all would help replies from building to building be quicker, although it is more expensive than other topologies, this will be very efficient for locations to update each other on information like sales, stocks, deals, etc. When pinging the website of Home Depot, the address pinged was a Class A network with the numbers “23.61.252.251”. This will help the subnetting part of the project so each node can be configured with an IP address.

Appendix B: Subnetting

IP address pinged: 23.61.252.251

Subnet Mask: 255.0.0.0

Class: A

Usable Host Range: 23.56.0.1 – 23.63.255.254

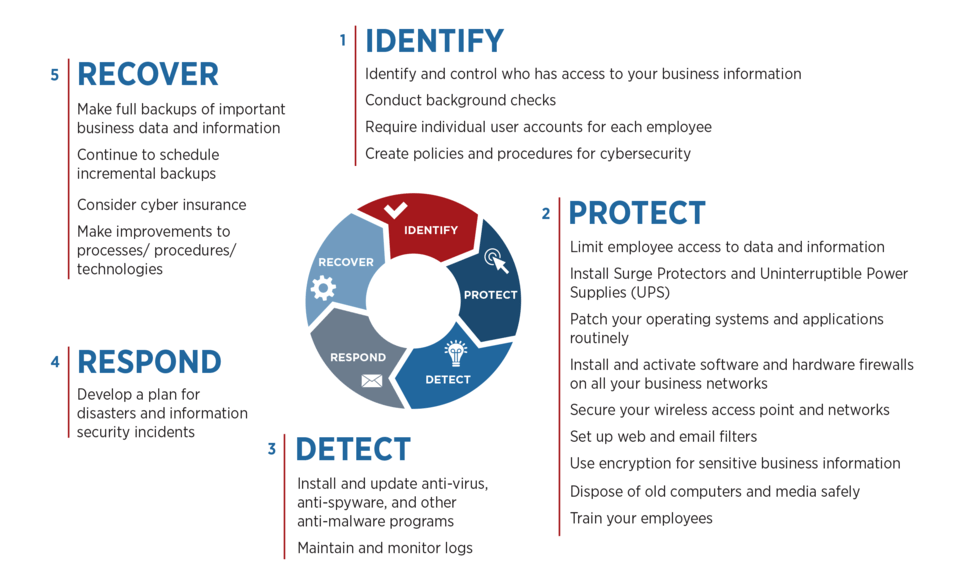
Devices: Computers, Edge Routers, Core Routers, Switches, Phones, Hub, Firewalls, RADIUS Server, VoIP, DNS Server, HTTP Server, FTP Server, Mail Server, DMZ Routers, Firewalls, DHCP Server, Cloud

Appendix C: Acceptable Use Policy

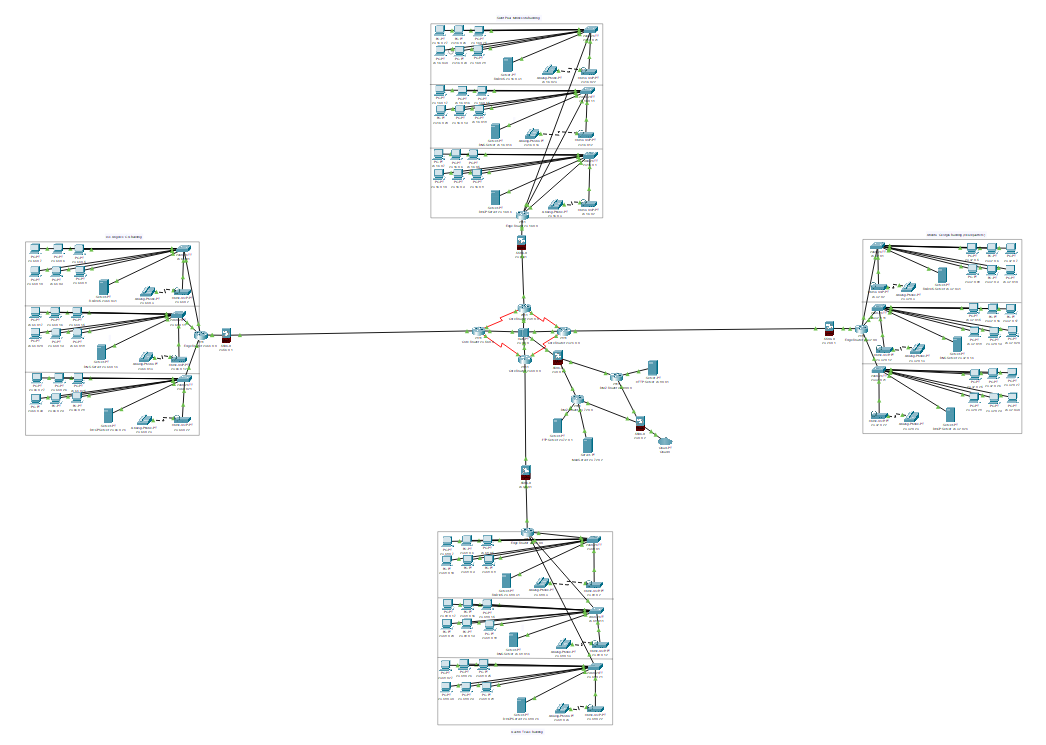
Home Depot is committed to protecting your privacy. We may use information users registered from our website to get a better understanding of our customers when it comes to our tools purchased. We would also collect this information to “process and complete the commercial transactions you request, and to provide you with a more personalized experience on our site.”[[3]](#footnote-2) This policy statement was created for us to demonstrate the commitment to protecting the privacy of customers and visitors.

We collect information so tickets or products are handled appropriately when customers purchase them. Information we collect includes the customer’s first name, last name, phone number, email address, and age. If a customer has signed up for sweepstakes or promotions we may ask for a shipping address so packages can be delivered to the customer’s house. The website may also collect IP addresses and click stream data, we collect IP addresses so our computers can identify the customer’s device. It's like a name for the computer. Click stream data helps show us which page is popular the most by how many have clicked the link and the time spent in that page. All this information we collect is to help us with marketing and promoting our tools for better profit and service to our customers. If we share your information we would only share it to “to service providers or other companies who work on our behalf”[[4]](#footnote-3).

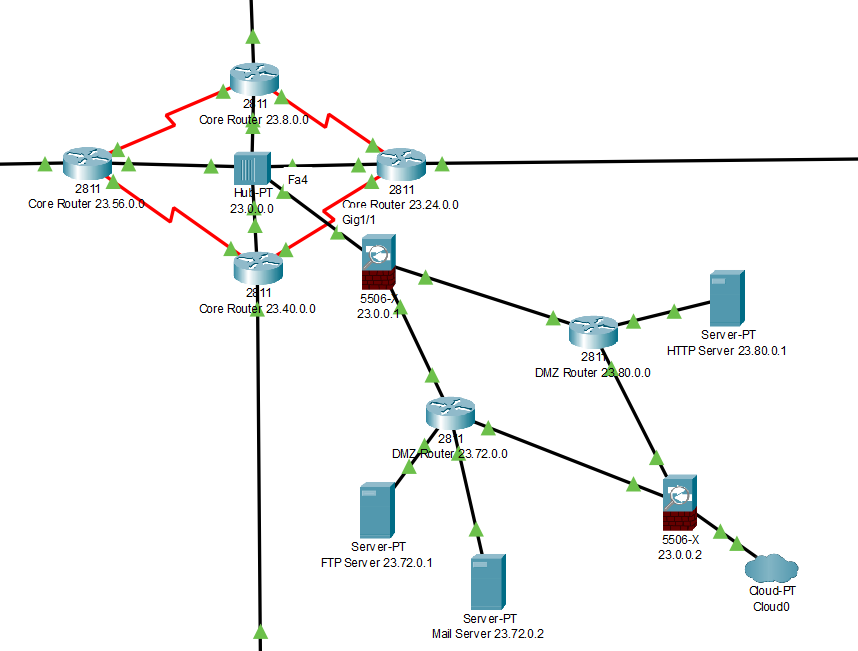
Appendix D: NIST Framework



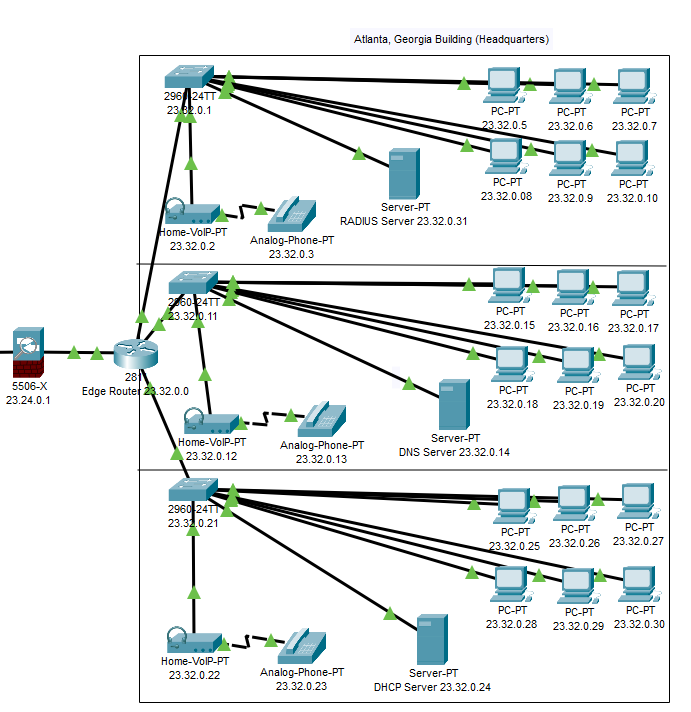
Appendix E: Network Design Pictures



Appendix E: Network Design Pictures



Appendix E: Network Design Pictures



(How every building is designed)

References

1. Micro, T. (2018) NIST Cybersecurity Framework Series Part 3: Detect. *TrendMicro* https://blog.trendmicro.com/nist-cybersecurity-framework-series-part-3-detect/

2. Seals, T. (2017) Home Depot to Pay $27.25m in Latest Data Breach Settlement. *InfoSecurity Magazine*

3. *Home Depot Center* retrieved from http://www.homedepotcenter.com/footer/privacy-policy.html

1. **Micro, T. (2018) NIST Cybersecurity Framework Series Part 3: Detect. *TrendMicro* https://blog.trendmicro.com/nist-cybersecurity-framework-series-part-3-detect/** [↑](#footnote-ref-0)
2. **Seals, T. (2017) Home Depot to Pay $27.25m in Latest Data Breach Settlement. *InfoSecurity Magazine* https://www.infosecurity-magazine.com/news/home-depot-to-pay-2725m/** [↑](#footnote-ref-1)
3. ***Home Depot Center* retrieved from http://www.homedepotcenter.com/footer/privacy-policy.html** [↑](#footnote-ref-2)
4. ***Home Depot Center* retrieved from http://www.homedepotcenter.com/footer/privacy-policy.html** [↑](#footnote-ref-3)