ISEC-615 - Fundamentals of Cybersecurity

Assignment No. 2 - Cybersecurity Environments

Due: 6/16/2019

Eric Webb

[ew774@mynsu.nova.edu](mailto:ew774@mynsu.nova.edu)

Dr. Yair Levy

Hardware Components of Office Network………………………………………………………………….………..3

Office Network Security……………………………………………………….…4

Hardware Components of Cloud-based Hosting Services…………………………………………………………………................5

Cloud-based Hosting Services Security………….………………………………………………………………....6

Conclusion………………………………………………………………………….7

Work Cited……………………………………………………………………….....8

Certificate of Authorship……………………………………………………………9

The typical office is made up of a plethora of network equipment.

These hardware components all play an integral part in making up the network.

To begin, the modem is what connects your network to your internet service provider.

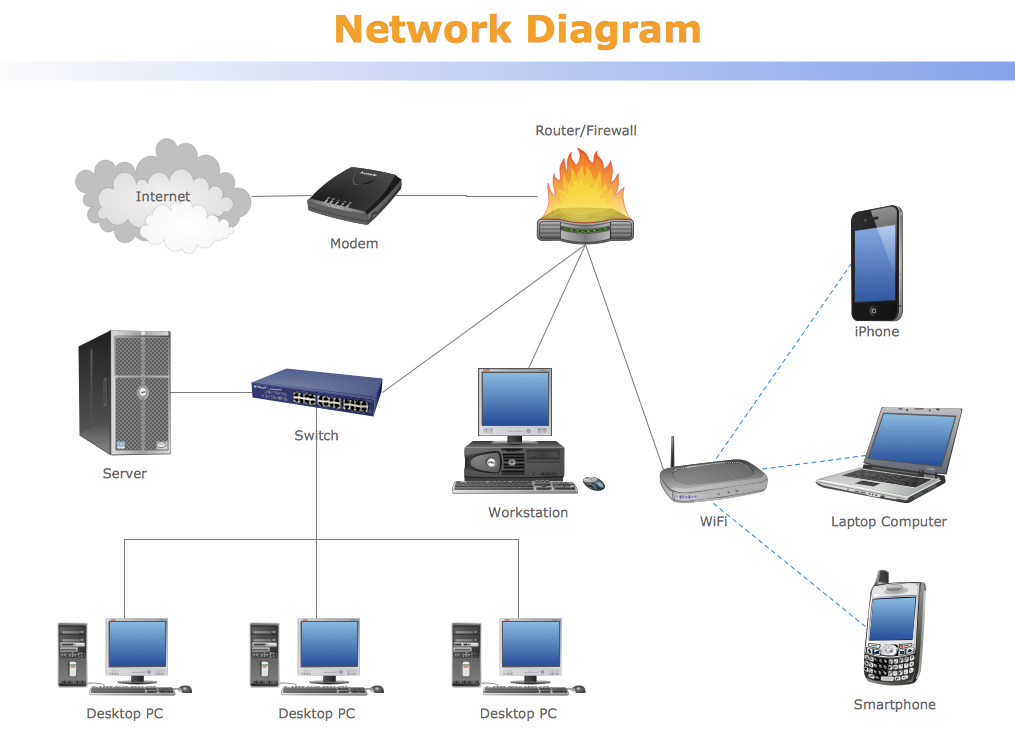
It is the interface between the outside world and you. From here you can connect your local machines to the internet. (10 Types of Technology Office Equipment That All Small Businesses Should Have in 2019, 2019).

Next we have a firewall. The firewall protects the network by filtering packets, User settings, and real time alerts. A firewall has the ability to block ports and perform inbound and outbound NAT’s. Every protected network should have a firewall for defense. (Bauer, n.d.)

After that we have the Router. The Router can assign IP addresses to network equipment along with setting up virtual LAN’s to segregate different parts of the network and setting up VPN capabilities. The Router is crucial for routing packets in your network.

Finally a piece that holds the network together will be the network Switch.

The device connects these devices together on multitude of ports. The switch will provide a connection for the PC’s, phones, and other equipment back to a central location. (10 Types of Technology Office Equipment That All Small Businesses Should Have in 2019, 2019).



(Computer Network Diagrams. n.d.).

Networks will use both physical and cyber controls to maintain a system usability vs. cyber security prospective.

To begin physical controls are things you can physically see and touch for instance ID badges, Cameras, and biometric readers. When maintaining a network one must keep in mind the physical controls to maintain a secure network.

Cyber Controls on your network would be specific controls within your network that cannot be physically seen or felt without the proper interface. One example would be Linux Permissions or using an Access Control list to add the control of a need to know basis. These are functionalities embedded digitally in your network that need to be implemented to help maintain security. (What is an Access Control List n.d)

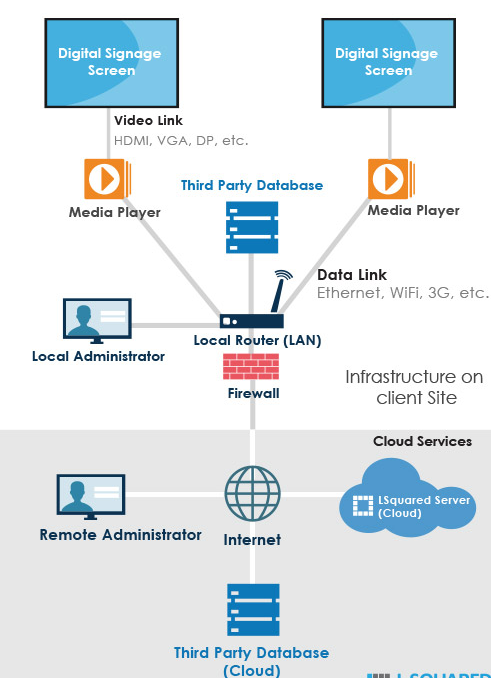
When maintaining these physical and cybersecurity defenses it is important to take into account security versus usability. Take away the usability of you network then tasks become cumbersome for the everyday user. This brings the ergonomics and efficiency of your network into question. Adding usability in turn typically means giving up a portion of security. Typically the more secure the harder to use, and the easier to use the less secure.

So keeping in mind usability without giving up your cybersecurity is an important topic to be discussed when implementing your network.

Recently, cloud-based hosting has been a big topic in the deployment of network infrastructure. Some benefits of cloud-based hosting are the ideas of scalability, backups, and reliability. To better understand these topics will go into detail on their hardware components and the functions.

To being all cloud services available our hosted by some type of physical device. Now-a-days cloud providers are using the concept of virtualization to run multiple independent virtualized services on one machine. Virtualization makes use of a hypervisor so that you can dedicate hardware to run independent virtualized environments. Essentially many computers in one. So having hardware that is optimized for virtualization is a good idea. This allows the cloud to run multiple services at once. (Pal, K.2015)

They beauty of the cloud is that you can access your services remotely as long as you have an internet connection. A good internet connection is ideal for cloud-based hosting solutions. From these cloud servers it is a good idea to run automated data backups along with hosting applications from a cloud provider then compared to onsite. This eliminates cost and resources along with improving uptime and scalabitly as well.



(Cloud vs Local Hosting n.d.).

When implementing security controls in your cloud-based hosting services it is good to keep in mind the cybersecurity versus system usability balance.

Physical controls might be access to badge readers and cameras to access network closets where the virtual cloud servers are running. You may not want someone accessing your server room but in case of emergency you want to make sure access is available. Another Physical control would be taking local backups to physical on site equipment. Although the point of the cloud is to be more data redundant with automated backups and guaranteed uptime. You still will not want to put all your eggs in one basket so the question of backing up locally as a failsafe to the cloud environment comes into question. (SelectHub. n.d.).

When access your cloud services remotely, you want to make sure you are accessing them in a safe manor. One Cyber controls that come into place is the establishment of a VPN to access your cloud. Another important role is not just encrypting your traffic to and from your cloud but also encrypting the data on your cloud itself. That was in case of a breach an attacker must also decrypt the information in order for the attack to be successful. Multi-factor authentication is another cyber control that would safe guard your system. That way obtaining a password is not enough but having something you physically have or physically are will add another level of security. (Using The Cloud Securely 2016).

Of course all this should be taken into account when making you system secure while still maintain a strong security position.

From this we have gather information about the network equipment and security of your typical office to the components that make up a cloud-based hosting service with the security aspects as well.

In a typical office we will have networking equipment like a switch, router, firewall, and modem. (10 Types of Technology Office Equipment That All Small Businesses Should Have in 2019, 2019). While implementing physical controls like mantraps and security cameras we can also implement cyber controls likes SSL encryption or VLAN’s to separate networks.

In a cloud-based hosting service we can set physical controls such as ID badges for entry and a Faraday cage to block the magnetics of the cloud servers. Cyber controls would be encrypting the data in the cloud and also encrypting traffic to and from the cloud servers. (Using The Cloud Securely 2016).

Networks have a lot of moving parts whether local or hosted in the cloud and it is important to keep in mind the physical and cyber controls, while keeping in mind how they affect the security vs system usability aspect of your environment.

10 Types of Technology Office Equipment That All Small Businesses Should Have in 2019. (2019, February 09). Retrieved from <https://fortistelecom.net/it-support/office-equipment-list-small-businesses>

Bauer, J. (n.d.). What Does a Firewall Do. Retrieved June 5, 2019, from <https://firewalling.com/what-does-a-firewall-do>

Computer Network Diagrams. (n.d.). Retrieved June 9, 2019, from <https://www.conceptdraw.com/samples/network-diagram>

Cloud vs Local Hosting. (n.d.). Retrieved June 8, 2019, from <https://www.lsquared.com/article-cloud-localhost>

Pal, K. (2015, April 29). 10 Ways Virtualization Can Improve Security. Retrieved June 9, 2019, from <https://www.techopedia.com/2/31007/trends/virtualization/10-ways-virtualization-can-improve-security>

SelectHub. (n.d.). Cloud Hosting Requirements - Top 5 When Implementing Cloud Hosting. Retrieved June 8, 2019, from <https://selecthub.com/cloud-technology/top-cloud-hosting-requirements/>

Using The Cloud Securely. (2016, November). Retrieved from <https://www.sans.org/security-awareness-training/ouch-newsletter/2016/using-cloud-securely>

What is an Access Control List (ACL)? - Definition from Techopedia. (n.d.). Retrieved June 9, 2019, from <https://www.techopedia.com/definition/24766/access-control-list-acl>

Certification of Authorship of Assignment



Submitted to: Professor Yair Levy.

Student’s Name: Eric Webb

Date of Assignment: 06/16/2019

Title of Assignment: Assignment No. 2 - Cybersecurity Environments

Certification of Authorship: I hereby certify that I am the author of this document and that any assistance I received in its preparation is fully acknowledged and disclosed in the document. I have also cited all sources from which I obtained data, ideas, or words that are copied directly or paraphrased in the document. Sources are properly credited according to accepted standards for professional publications. I also certify that this paper was prepared by me for this course.

Student's Signature: ERIC WEBB