20LLP127
Coursework Report

ID Number: B620035

Programme: Cyber Security and Big Data

Module Title: Information Systems Security

Project Title: EasyTarget Ltd. Network Security Proposal

Contents

1 Introduction

1.1 Background

Looking at the current trends when it comes to a company's reliance on the internet to allow staff carry out their daily job tasks and how digitalisation continues to impact our lives constructively and in some cases destructively, the need for information security has never been more important. According to a survey by the Institute of Directors, of approximately 1000 firms it is seen that around 74% plan on maintaining the increase in home working caused by the ongoing pandemic [1]. The director of policy at the institute was also quoted as saying "Remote working has been one of the most tangible impacts of coronavirus on the economy. For many, it could be here to stay" [1].

As there has been a rise in the number of high-profile cyber-attacks during COVID-19 [2] (showing the relationship between internet use /remote working and web related criminal activity), efforts need to be made by organisations to ramp up information security.

1.2 Project description and aim.

A medium sized manufacturing company known as EasyTarget Ltd. is looking to overhaul its information security system. It is stated that:

- The company has a dedicated web server which hosts its website (accessible to the public and internal employees).
- All employees can access the internet through the company's internal network
- There exists a file server for sharing information internally

The aim of this project is to propose a solution that enhances the security of Easy Target's computer network by looking at possible measures to detect, defend and prevent the company's system from threats and attacks. Finally, the proposal should be feasible with available technologies, devices and applications currently on the market, including both commercial and open source applications.

1.3 Project objectives.

The following objectives were set in order to meet the project aim:

- Gain an understanding of network security concepts; common threats, attacks and vulnerabilities on networks or network security systems.
- Analyse EasyTarget Ltd's current network architecture and security to see if they meet business requirements, search for possible loopholes and areas of improvement.
- Examine state-of-art solutions which will ensure issues found are mitigated as best as possible and network security standards are met.
- Provide/propose off-shelf solutions based on findings, market availability and give an explanation of how they shall be implemented.

- Give further suggestions on keeping company's computer network secure such as ethics, best practices etc.

2 Investigations/Methodology

Threats, vulnerabilities (such as Viruses, Spyware, Backdooors, Worms, Logic Bombs, Ransomware etc.) and attacks(such as Replay attacks, Eavesdropping, Denial of Service, DNS/ARP poisoning, social engineering attacks etc.) pose a huge risk to all businesses as they can cause major damage to any company. This is simply because most businesses are fuelled by data and leakages, loss or theft of key data such as client/employee data can cost the company in terms of having to pay ransoms and being at the mercy of attackers. In some cases cyber-attacks also affect the future/growth of a company and can end up destroying its potential.

It is important to note that poor implementation of certain network security solutions can sometimes be worse than not implementing any measure and so in order to propose network security solutions for EasyTarget Ltd. which can mitigate some of the risks posed the aforementioned attacks, the company's network architecture was examined.

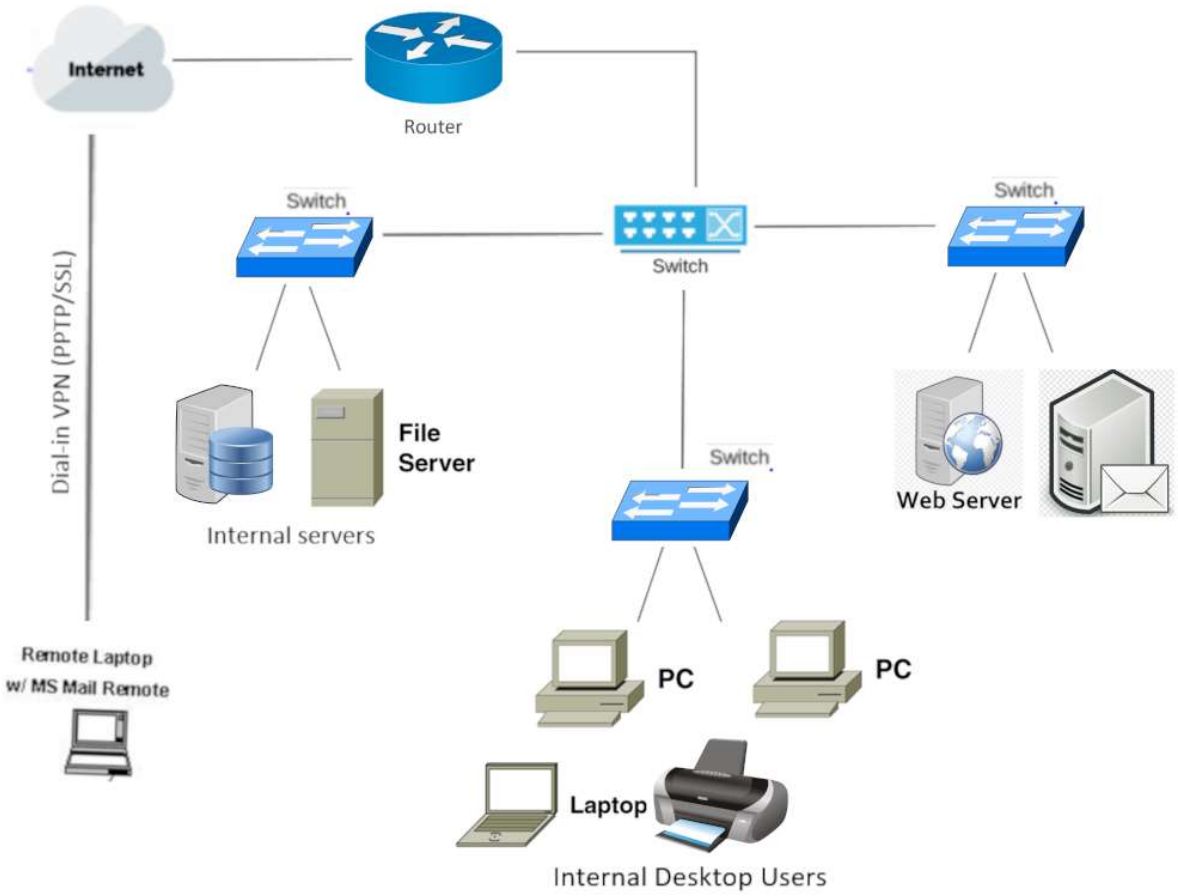

Figure 1: EasyTarget Ltd's current network architecture

After an analysis of the company's computer network as shown in figure 1, it is clear that this set up is very insecure and as such the technologies earmarked to carry out the network security overhaul process are presented in section(s) 2.1-2.5.

2.1 Firewalls

Firewalls are a sort of barrier/fence which separate an internal/trusted network from external (untrusted) networks [3]. They tend to be the first line of defence in network security designs [4]. They function by assessing the headers of data packets for information such as (origin, destination etc) and then filtering them based on a set of rules/protocols [5]. They are not usually able to protect a network from internal attacks like a DDoS and are usually used in conjunction with an IDS [5]. A brief examination of the different types of firewalls is presented in table 1 [6].

Type of firewall	Advantages	Disadvantages
Packet filtering firewall	• Filtering can be done using just one device • Traffic analysis is fast and efficient • cheap • Has little impact on network performance.	• traffic filtering is based entirely on IP address or port information hence it lacks broader context that informs other types of firewalls • Doesn't check the payload and can be easily spoofed • Not the best for every network • difficult to set up and manage access control lists
Circuit-level gateway	• Only processes requested transactions; all other traffic is rejected • Easy to set up and manage • cheap • has little impact on end-user experience	• needs to be used together with other security technology to protect against data leakage from devices within the firewall • No application layer monitoring • Requires constant updates to keep rules current
Proxy firewall (suggested)	• communications between outside sources and devices behind the firewall are tracked by examining address, port, TCP header information, and the data itself before any	• Can affect network performance • Relatively expensive • Requires a high degree of effort to derive the maximum benefit from the gateway

	traffic passes through the proxy • additional security controls which can, for example, allow access to a certain pages on a website. • user anonymity security	• Doesn't work with all network protocols
Stateful inspection firewall	• Monitors the entire session for the state of the connection, while also checking IP addresses and payloads for more thorough security • Provides good level of control over what content is let in or out of the network • Provides profound logging capabilities	• Impacts Network performance negatively • Relatively expensive • Cannot detect spoofing of traffic sources.
Next-generation firewall	• Combines deep packet inspection with malware filtering. • Tracks all traffic from Layer 2 to the application layer for more accurate insights than other methods • Can be automatically updated to provide current context	• Better deployed with other security systems, which is more cumbersome. • Most expensive

Table 1: comparing the pros and cons of different firewalls [6]

2.2 Virtual Private Network (VPN)

A VPN is simply a secure internet connection between a network and a device or two remote networks [7]. VPNs function by encapsulating, encrypting incoming/outgoing data and authenticating a remote connection [8]. A common application of a VPN is in providing remote access to an organizations internal network and from figure 1 it is clear that a VPN is needed for remote connections to the file server. The different types of VPN technologies available are described in table 2 [8].

VPN technology	Functionality
Trusted VPN	Uses leased circuits from a service provider and conducts packet switching over these leased circuits
Secure VPN	Uses security protocols, such as IPSec, to encrypt traffic transmitted across unsecured public networks like the Internet
Hybrid VPN	Combines the two, providing encrypted transmissions (as in secure VPN) over some or all of a trusted VPN network

Table 2: Different types VPN technologies [8]

"Secure VPNs provide security but no assurance of paths. Trusted VPNs provide assurance of properties of paths such as QoS, but no security from snooping or alternation. Because of these strengths and weaknesses, hybrid VPNs have started to appear, although the list of scenarios where they are desired is still evolving" [9].

For this project network security is the main focus and as such a secure VPN is suggested for use.

2.3 Antivirus Software

Antivirus softwares are programmes that can detect, remove and in some cases prevent malware such as worms, spyware, trojans etc [10]. They are one of the most common security solutions used on computers. They are included in this proposal to protect the company's network from threats brought about when a work PC or device is used outside the office (i.e. connected to another network) [11]. Antivirus softwares can either be standalone software, cloud-based software or security software suites (preferred) [10].

2.4 Network Access Control (NAC)

With clients or partners having to make visits these days to organisations to carry out certain aspects of a project, there has been an issue of ensuring their work devices are not carrying malware when they connect to other networks [12]. NAC helps remediate this issue by administering of policies/protocols for controlling access to their network [13]. A survey in 2019 conducted by eSecurity Planet shows that NAC was a huge consideration in IT security just based of the amount of money and confidence put into it [13]. NAC can be split into pre-admission NAC (for ensuring initial connections to a network are safe) and post-admission NAC (for controlling access to different parts of a network) [14].

2.5 Intrusion Detection & Prevention Systems [IDPS]

IDPSs are network security solutions which monitor a network and perform functions such as identifying threats, log information about them, report them to administrators and in some cases stop them from disrupting the normal functioning of the network [15].

IDPS Technology	Malicious Activity Detected	Strengths	Weaknesses	Medium
NBA	Network, transport, and application TCP/IP layer activity that causes anomalous network flows [15].	more effective than the others at identifying reconnaissance scanning and DoS attacks, and at reconstructing major malware infections [15].	small-scale attacks which are conducted slowly and don't violate policies set by administrators are less accurately detected [15], delay in detecting attacks [15].	Multiple network subnets and groups of hosts [15].
Wireless	Wireless protocol activity; unauthorized wireless local area networks (WLAN) in use [15].	Only IDPS capable of monitoring wireless protocol activity [15].	Inability in detecting some wireless network attack [15], IDPS sensors also susceptible to attacks [15].	Multiple WLANs and groups of wireless clients [15].
Network-based	Network, transport, and application TCP/IP layer activity [15].	only IDPS that can thoroughly analyse a wide range of application protocols.	Requires tuning & customization to reduce inaccuracies [15], cannot detect attacks in encrypted network traffic [15], unable to perform full analysis under high loads [15], IDPS sensors are victims of external attacks [15].	Multiple network subnets and groups of hosts [15].
Host-based	Host application and operating system (OS) activity; network, transport, and	Only IDPS with functionality to analyse activity transferred in end-to-end	Often cause false positives/negatives [15], host resource usage [15], conflicts with existing	Individual host [15].

	application TCP/IP layer activity [15].	encrypted communications [15].	security controls [15], alert generation delays [15].	

Table 3: Comparing different IDPS technology types [15]

Reliable IDPS solutions tend to be realised by combining different types of IDPS technologies [15] and as such a combination of network-based (for network segments/devices) and host-based (for hosts)IDPS solutions are recommended to EasyTarget Ltd based on the company's network infrastructure.

3 Discussion/ Proposed Solution(s)

Figure 2 shows the proposed network design for EasyTarget Ltd. improved with security technologies and/or measures to help improve the security network.

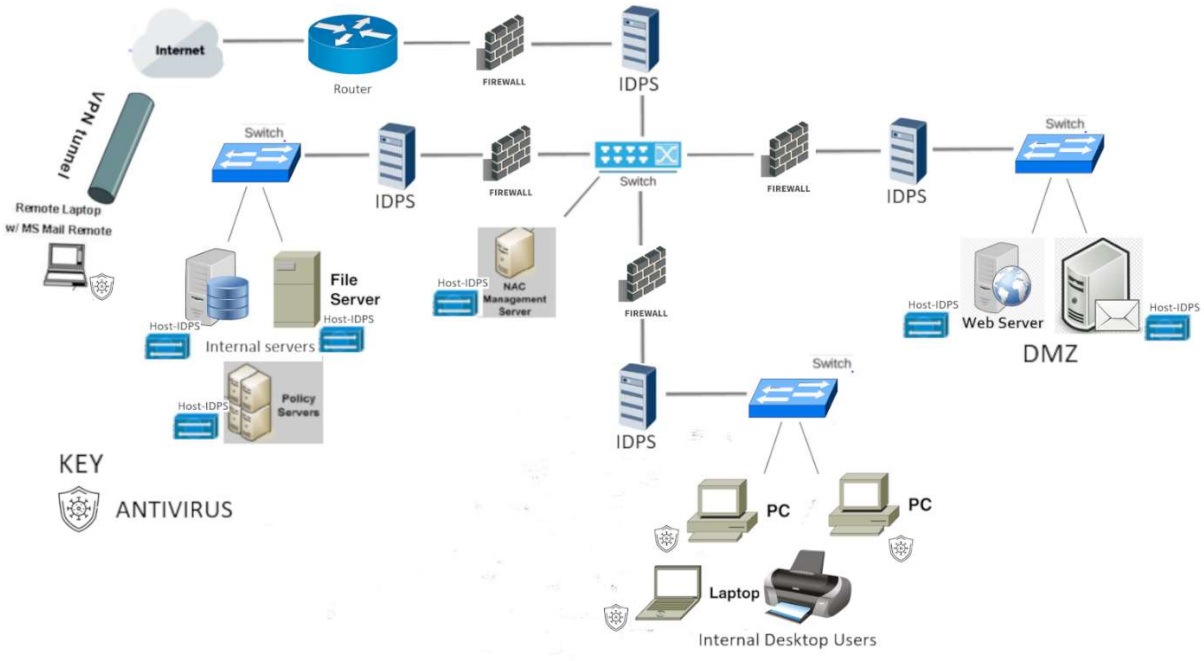

Figure 2: Proposed Network Design for EasyTarget Ltd

From figure 2 it can be seen that the main entry point to the network (i.e. internet) is protected with a proxy firewall and a network-based IDPS to mitigate threats targeted at the core/master switch. Entry points to the other areas (DMZ, Internal servers, Internal desktop users) of the network are also safeguarded by proxy firewalls and network-based IDPS.

A] **Demilitarized Zone (DMZ):**

The demilitarized zone is the region of a network which contains assets which are public/open to the outside world such as the web server and email server. Due to the threats these assets are faced with they are equipped with host-based IDPS. They are also protected internally using a proxy firewall and a network-based IDPS.

B] **Internal company network:**

The internal network is comprised of the internal servers (file server, database, policy servers) and internal office (PCs, printers etc.). In addition to the firewalls and IDPS which safeguard the entry points to both network segments and the core switch; all servers are also protected with host-based IDPS while the PCs or workstations are protected with antivirus software. These measures ensure that the company's personal information/data is protected as much as possible.

C] **Remote users:**

A secure VPN with IPSec traffic encryption is used to ensure a secure connection via the internet for remote users who access the company's internal resources. All remote workers must also have antivirus software running on their work devices.

D] **NAC:**

NAC is implemented with the use of a NAC management server which facilitates the process of carrying out checks on devices connecting to the network and then carrying out a verification process whereby results of scans are verified with policies configured in the policy servers [16].

4 Conclusion

In this report an examination of EasyTarget Ltd.'s computer network was done in order to carry out improvements that will help achieve information security goals of confidentiality, authentication and availability. Common network attacks were discussed and based on these security technologies/solutions were proposed. Finally, a more secure network design which made use of the proposed security solutions was created (figure 2).

From figure 1, it is fair to say that EasyTarget had little or no security measures in place leaving the network quite open for attackers. Ironically, it can be said that the network setup in the eyes of attackers mirrored the name of the company with it being an easy target. With the proposed network design shown in figure 2 however, the company's network can be said to have a good level of security which is not bad given the fact that idea of 100% security is a mere fantasy.

Information security is more than the mere implementation of technological solutions and so in addition to the network security measures proposed, it is also important to focus works on aspects of security such as ethics, access control/physical security, risk management, staff training, recruitment of InfoSec professionals etc. Only after all of these areas meet set security requirements can EasyTarget start to see a light at the end of the tunnel in regards to information security.

Finally, it is important to understand that achieving a good level of security is a continuous process given that there are technological advancements every day and therefore security measures need to be constantly reviewed and improved.

5 References

[1] BBC, "Home working here to stay, study of businesses suggests," *BBC*, 2020.

[2] A. Auld and J. Smart, "Why has there been an increase in cyber security incidents during COVID-19?," *PwC UK Cyber Threat Intelligence Team*, 2020. https://www.pwc.co.uk/issues/crisis-and-resilience/covid-19/why-an-increase-in-cyber-incidents-during-covid-19.html (accessed Mar. 09, 2021).

[3] M. Imran, A. A. Alghamdi, and B. Ahmad, "Role of firewall Technology in Network Security," *Int. J. Innov. Adv. Comput. Sci.*, no. December 2015, pp. 3–6, 2015, Accessed: Mar. 09, 2021. [Online]. Available: https://www.researchgate.net/publication/292138198_Role_of_firewall_Technology_in_Network_Security.

[4] I. Kashefi, M. Kassiri, and A. Shahidinejad, "A Survey on Security Issues in Firewalls: A New Approach for Classifying Firewall Vulnerabilities," *Int. J. Eng. Res. Appl.*, vol. №3, no. 2, pp. 585–591, 2013, Accessed: Mar. 09, 2021. [Online]. Available: https://www.researchgate.net/publication/262116695_A_Survey_on_Security_Issues_in_Firewalls_A_New_Approach_for_Classifying_Firewall_Vulnerabilities.

[5] W. Bul'ajoul, A. James, and M. Pannu, "Improving network intrusion detection system performance through quality of service configuration and parallel technology," *J. Comput. Syst. Sci.*, vol. 81, no. 6, pp. 981–999, 2015, doi: 10.1016/j.jcss.2014.12.012.

[6] A. DeCarlo and R. Ferrell, "The 5 Different Types of Firewalls Explained," 2021. https://searchsecurity.techtarget.com/feature/The-five-different-types-of-firewalls (accessed Mar. 09, 2021).

[7] Cisco, "What Is a VPN? - Virtual Private Network - Cisco." https://www.cisco.com/c/en/us/products/security/vpn-endpoint-security-clients/what-is-vpn.html (accessed Mar. 09, 2021).

[8] X. Shi, "Topic 6-Access Control LLP127-Information Systems Security 1 LLP127-Information System Security Topic 6: Information Security Technologies (2)-Access Control Topic 6-Access Control," 20LLP127, Institute for Digital Technologies, Loughborough University, 2021.

[9] "VPN Technologies : Definitions and Requirements," 2003. http://www.hit.bme.hu/~jakab/edu/litr/VPN/vpn-technologies.pdf (accessed Mar. 09, 2021).

[10] "What is Antivirus Software? The Top 5 Types You Need to Know." https://softwarelab.org/what-is-antivirus-software/ (accessed Mar. 09, 2021).

[11] C. Lauterbach, "Intrusion Detection, Intrusion Prevention, and Antivirus: The Differences," 2019. https://www.bestructured.com/intrusion-detection-intrusion-prevention-and-antivirus-the-differences/ (accessed Mar. 09, 2021).

[12] P. Wood, "Alternatives to buying full-on network access control (NAC) systems," 2010. https://www.computerweekly.com/answer/Alternatives-to-buying-full-on-network-access-control-NAC-systems (accessed Mar. 09, 2021).

[13] D. Robb, "Top 9 Network Access Control (NAC) Solutions for 2021," 2020. https://www.esecurityplanet.com/products/network-access-control-solutions/

(accessed Mar. 09, 2021).

[14] "What is Network Access Control? | VMware Glossary." https://www.vmware.com/topics/glossary/content/network-access-control (accessed Mar. 09, 2021).

[15] K. Scarfone and P. Mell, "Guide to Intrusion Detection and Prevention Systems (IDPS) Recommendations of the National Institute of Standards and Technology," *Nist Spec. Publ.*, vol. 800–94, p. 127, 2007, doi: 10.6028/NIST.SP.800-94.

[16] T. Olzak, "Strengthen Data Protection with Network Access Controls Deperimeterization," no. May, 2006, Accessed: Mar. 09, 2021. [Online]. Available: https://www.researchgate.net/publication/228635953_Strengthen_Data_Protection_with_Network_Access_Controls.