International Journal of Computing and Mathematics
Vol. 1, Issue. 2, June 2024, pp. 29~35

Analysis of Computer Network Security System

Emmanuel O.C. Mkpojiogu[1], Ahmed Al-Athwar[2]
[1]Department of Computer and Information Technology, Veritas University, Abuja, Nigeria.
[2]School of Computing, Universiti Utara Malaysia, Sintok, Kedah, Malaysia.

Article Info

Article history:

Received Apr 5, 2024
Revised May 18, 2024
Accepted Jun 12, 2024

Keywords:

Network security
Intrusion Prevention Systems (IPS)
Cryptography
Authentication

ABSTRACT

For PC users, alliances, and the military, network security has become more imperative. Security has become a major concern with the appearance of the web and the historical context of security allows for a superior understanding of the growth of security innovation. The internet infrastructure itself considered that there were multiple safety hazards. When updated, the architecture of the site will reduce the possible assaults that can be sent around the companye. The required protection to be improved is taken into account by understanding the attack techniques.

Numerous organizations use firewall techniques and encryption software to protect themselves from the internet. To remain connected to the internet, the companies create an "intranet" but have ensured that future risks are involved. The entire area of protection for organizations is enormous and in a stage of growth.

The scope of the analysis involves a brief history going back to the origins of the web and the recent change in network security.

Foundation information on the network, its vulnerabilities, and assault techniques through the network to understand the analysis being carried out today, and security advancement is necessary and they are inspected in this way.

Corresponding Author:

Emmanuel O.C. Mkpojiogu,
Department of Computer and Information Technology, Veritas University, Abuja, Nigeria.

1. INTRODUCTION

Numerous data applications are becoming more and more commonplace due to the rapid advancement of computer networks, especially the growth of the Internet. However, a lot of information is shared and stored in the public conversations system, which might be illegally wiretapped, intercepted, changed, or damaged by attackers for a variety of reasons, leading to a never-ending cycle of bad luck. Unauthorized access, hackers posing to be legitimate potential consumers, destruction of data, waiting in line and employing an organization to spread infection, and other similar behaviors are the main manifestations of network security issues. Since the organization's security problem is becoming more and more obvious, one of the main factors impeding the organization's success is whether or not it can be repaired. Information security and network framework security are typically included in organization security challenges. Information security is necessary in order to safeguard sensitive and private data from being stolen or illegally duplicated, whereas organizational architecture cybersecurity is to prevent the architecture from illegal assault availability, and disintegration [1].

The computer network security issue is identified with numerous fields, for example, PC innovation, correspondence innovation, science, cryptography, data hypothesis, the executives, and low. Different fields have different solutions for network security problems, and these solutions should be used to understand the problem [2]. With the advent of internet connectivity and fresh developments in systems administration, the globe is becoming increasingly interconnected.

Globally, there is a wealth of information on administration of systems foundations from individuals, corporations, the military, and governments. Organizational security is becoming incredibly

important because to licensed innovation that is easily accessible online. There are as of now two in a general sense various organizations, information organizations and simultaneous organization contained switches. The web is viewed as an information organization. Since PC-based switches make up the current information network, unusual initiatives, like "Diversions," installed in the switches, can obtain data. Since the switch-based simultaneous organization does not support information, attackers cannot compromise it. For this reason, information organizations, such as the web and other networks that link to it, place a high priority on security. The vast topic of organization security is broken down by looking into the related:

1. The background of network security
2. The Internet's inadequate security features and web engineering
3. Types of online attacks and security measures
4. Network security for web-access networks
5. Current developments in programming and equipment for network security

Given this analysis, organization security's ultimate destiny is uncertain. Additionally, emerging patterns will be taken into account in order to understand the direction of security arrangements.

Network Security

Network privacy, data safety, information infrastructure privacy, information network privacy, connection data frameworks privacy, PC frame security, and so forth are the typical items associated with PC security. These factors ultimately imply the two implications that follow: to ensure that the data framework's security activity in the organizational environment is guaranteed, as well as that the information stored, prepared, and transmitted within the data framework is securely guaranteed. In summary, the term "security of the network" in this paper refers to the reliability of the network framework, as well as the confidentiality, integrity, and availability of data within the framework, all of which are characteristics of network security [3].

Network Security Design

In summary, the term "security of the network" in this paper refers to the reliability of the network framework, as well as the confidentiality, integrity, and availability of data within the framework, all of which are characteristics of network security [3].

The organization's structure and development are externally reflected in the Network Security Architecture Diagram, as are all the activities undertaken to ensure the organization's security that can be carried out with the aid of programming tools and equipment, such as firewalls, antivirus software, network monitoring devices, tools for identifying attempts at unauthorized access or disruption, intermediary workers, and validation workers [4].

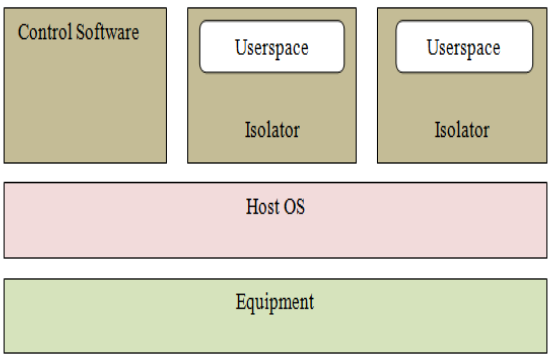

Figure 1. Network Security Architecture

2. NETWORK SECURITY SOLUTIONS AND TECHNOLOGIES

The process of proactively safeguarding the fundamental network components against unwanted access, abuse, malfunction, alteration, destruction, or breach of confidentiality is known as network protection. By following these procedures, users, programs, and computers can carry out their authorized actions in a secure setting with important features. A sophisticated set of hardware components, including firewalls, routers, and anti-malware software, is needed to secure a network. Government organizations and businesses employ highly skilled information security professionals to implement security measures and monitor their efficacy on a regular basis [5].

For any enterprise operating in the 21st century, Network Security is essential and aids identify and assure business performance. Unfortunately, many businesses find it difficult to determine which network security techniques are suitable for protecting their extensive network and data in such a broad field of technology. If they grow up in size, organizations will eventually neglect systems and users in their network. These unnoticed schemes, or disregarded clients frequently " leap" on and off of the network at will, represent broken links in the security chain. Inadequate password policy implementation exposes companies to rising the use of force logon theft and "silent failure," in which the attacker obtains authorization to remain (silent) undetected. in your network. Everyone can precisely carry out their network security estimation with the following information.

Next-Generation Firewalls

At the point when the limits reach out to cover numerous destinations, on-premise server farms, and private, half breed, and multi-cloud conditions, ventures investigate broad firewall arrangements that help guard against the foes focusing on clients, substance, and applications.

Since ventures are continually confronting advanced digital assaults that compromise business congruity, Next-Generation Firewalls (NGFWs) are set up. Cutting edge Firewall assurance assists with making sure about the server farm, branch, network border, and brutal mechanical conditions [6].

NGFW Vendors to consider

Cutting edge firewalling is important for third era firewall innovation. An NGFW combines the capabilities of a firewall, sandboxing, VPN, application control, interruption avoidance system (IPS), URL filtering, and more. The leading NGFW vendors provide firewalls that detect and thwart online attacks instantly, with fully automated phases that, in certain cases, can help to simplify security.

Palo Alto Networks NGFW

The following invention protection of Palo Alto Networks are entirely based on a predictable Single-Pass Architecture. For Enterprise Network Firewalls, Gartner perceived Palo Alto system as a pioneer for the seventh time, positioned most highly capable of implementing and ultimately in achieving the vision for large business network firewalls.

Forti-Gate Next-Generation Firewall (NGFW)

Without a doubt, allowing the FortiGate Firewall is worthwhile. It provides mechanized permeability to prevent attacks and high-risk security execution. The plan based division permits network administrators to make security areas or fragments situated as per business goal. Expectation based division is the capacity to send danger assurance any place it is required, both on-premises and in all cloud occasions, to diminish hazard, accomplish consistence, and ensure business-basic applications [7].

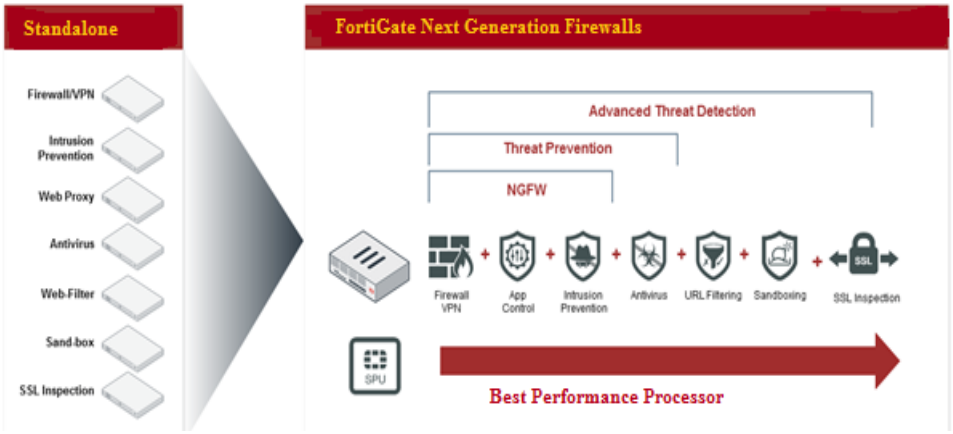

Figure 2. Forti-Gate Next-Generation Firewall

Secure Access

Network Access Control (NAC)

Organization Access Control is an attempt to streamline the chaos of associations from both the inside and the outside. Contact of some kind is necessary with faculty, clients, specialists, temporary employees, and tourists. Sometimes it comes from within the grounds, and other times it comes from a

distance. Bringing your own device (BYOD) policies, the prevalence of related smart devices, and the rise of the Internet of Things (IoT) are just a few examples of how NAC has become more complex over time.

Network Access Control configurations are used to restrict and appropriately verify this access to your company and data. A new level of security is added to the company and its data by determining which customers and devices have authorized consents [8].

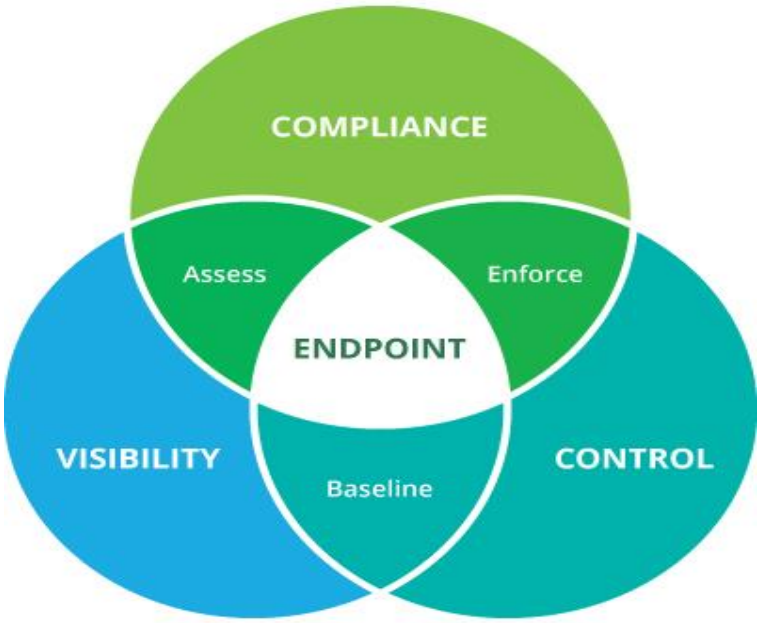

Figure 3. Network Access Control

Remote Security

Being significantly more defenseless to capture attempt contrasted with wired innovation, numerous associations experience difficulties while making sure about data communicated remotely between a gadget and passage. Snoops can accumulate logins, passwords, exclusive data, intranet worker addresses, and substantial organization and station addresses. 'Remote interlopers' send spam, take Internet transmission capacity, or use undertaking organizations to assault others. In huge endeavors, WLAN interruption identification might be essential, which offers a kind of appropriated observation with focal assortment and examinations.

Here are some pointers for setting up a secure Wi-Fi setup.:

Characterize access prerequisites all through the strategy necessity system. (Who needs access to what resource, and how?)

Have security measures been put in place that define guidelines for visitors to the "walled garden"? (For instance, logged visitor meetings through passageways with restricted objections, conventions, term, and data transmission could be allowed, while you may disallow shared systems administration.

Recognize resources and list dangers and evaluate dangers to guarantee costs weigh facing dangers and safety efforts taken.

Control Network Access Outcomes

Full NAC capacities are available at the ForeScout stage and the sky is the limit from there, in light of constant permeability of gadgets the moment they access the organization—paying little heed to where that organization exists inside your all-encompassing endeavor. It ceaselessly filters organizations and screens the movement of referred to, the organization claimed gadgets just as obscure gadgets, for example, actually possessed and maverick endpoints.

Forescout use cases for NAC

Control access to confidential data based on client profiles and device

Keep tainted or rebellious gadgets from spreading malware

Naturally, implement activities for distinguished circumstances without human association

1.1 DLP- Controlling the destruction of data

Information is becoming the mainstay of associations' operations, as discussed in our master blog on Data Loss Prevention. We continually create, send, consume, and store information. Information has become a fundamental resource for security and upkeep because of this.

Lamentably, information spills happen continually at a wide range of associations. There have been cases where a large number of clients' Visa information was leaked, or where disgruntled professionals copy sensitive information from the organization they plan to leave and sell or distribute it, severely harming clients and organizations' reputations [9].

Suggested Vendors for Data Loss Prevention

Neither the amount of information that can be disclosed nor the amount of harm that ought to be conceivable are restricted.

Eliminating loss of information in Forcepoint

Forcepoint's Data Loss Prevention features allow you to monitor your data across devices and organizations, both in use and in storage. Make and authorize arrangements that arrangement the entrance and development of information to forestall information breaks and aid in guarantee consistency with Forcepoint Data Loss Prevention (DLP).

McAfee Prevents Data Loss

Across endpoints, enterprises, and the cloud, McAfee Integrated Safety for Data Protection offers universal information insurance. It is easier to enable device-to-cloud DLP thanks to the open stage and McAfee EPO programming. Current undertaking DLP techniques can be extended to the cloud by McAfee DLP clients, who can also impact basic arrangements to ensure consistent information misfortune recognition. A solitary sheet of glass the executives reassure deals with all DLP infringement and occurrence work processes, notwithstanding if the DLP infringement are originating from business gadgets or cloud functions.

Vendors of Cloud Access Security Brokers (CASB)

This merchant causes you to ensure the information on another person's framework. As per Gartner investigator Steve Riley, they are becoming just as essential to cloud computing as firewalls were to server farms.

Either on-site or in a public cloud, CASB programming is transmitted [10]. It facilitates communication between cloud-specialized companies and cloud-administration buyers, maintains security and management agreements for cloud services, and enables initiatives to extend their on-premises methods to the cloud. Because employees frequently choose convenience above security, CASBs provide this demand by only allowing agents and associates to use approved cloud services and making sure they stay away from the riskier ones. Furthermore, CASB ensures information that lives in cloud specialist organizations' workers.McAfee MVISION Cloud and Forcepoint CASB are the two main CASB vendors.

Figure 4. CASB

Email Security

Email is the most obvious attack vector because it is one of the most well-known correspondence routes for associations nowadays. Email is being gotten to utilizing numerous gadgets, from various areas

(home, office, progressing) forming a 'merged gadget scene' for Email use. When getting to Emails representatives for the most part coincidentally click on the connections to malware facilitating sites or surprisingly more dreadful, they unknowingly insert harmful substances into the device, which are subsequently transmitted to other individuals.

Leading providers of email security

If you want to understand the fundamentals of email security, recall the key points of each secure email item, and figure out how to incorporate them into your existing setup, check out our comprehensive column on the digital death chain and sorting out email security.

Proofpoint Email Protection

For many years, Proofpoint served as a true pioneer in the field of email security. In addition to fake email danger security and inner mail guard, Proofpoint's Email Protection provides advanced email sifting, control, and permeability. You can protect your family, knowledge about and brand from current threats and frequent disruptions, such as [11], spam, malware, impostor emails, and mass mail, with Proofpoint's state-of-the-art email protection.

Email Security with FortiMail

Fortinet demonstrated their commitment to designing and developing effective email security solutions for the company by obtaining the highest possible score in the Internet Security Services bunch test. Associations frequently choose FortiMail to protect their customers and eventually information from online threats, such as the constantly growing amounts of unwanted spam, socially designed phishing and business email scams, the increasing ransomware and other malware variants, the increasingly focused attacks from adversaries, and more.

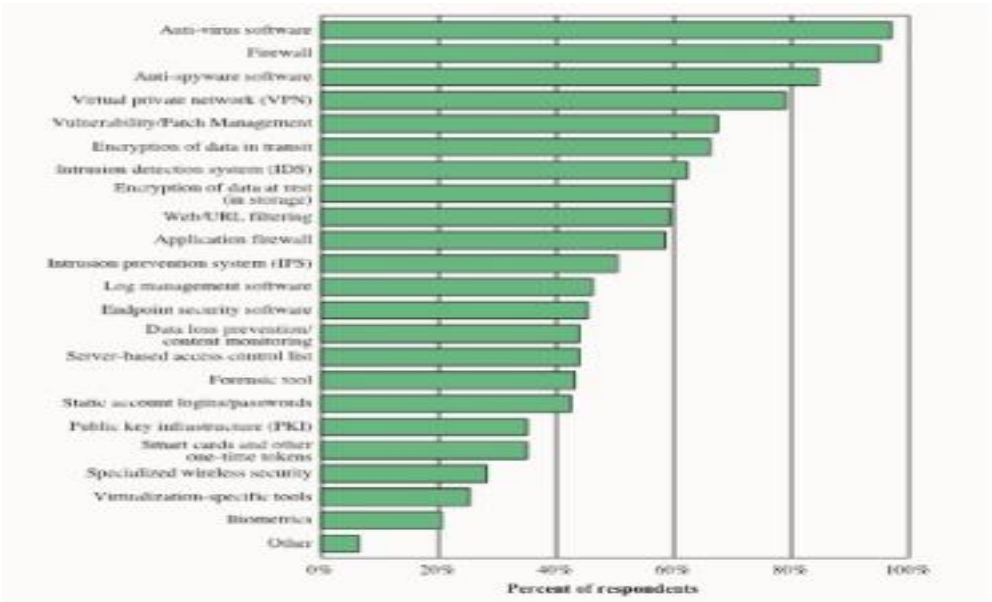

Figure 3. Network Security Technologies

3. CONCLUSION

Since security is a long term concern, a security plan needs to be established by service providers. A good place to begin is to teach workers about best practices. It is necessary to start by implementing a safety plan when implementing a security plan. First, the most apparent protections and by deploying equipment capable of the most advanced protection, deploying equipment capable of offering privileged EXEC authentication, such as AAA Services, and a higher degree of scalability than line-level. Even if this can mean shutting off features on servers. Finally, the growth of physical infrastructure and its increasing presence in an enterprise has created the need to protect the structures themselves physically, not just from cyber attacks, but also from physical attacks that can be carried out against them. The introduction of policy-based security also provides many benefits to the security arsenal, as it automates the introduction of the security theory. The computer network security solutions and technologies are discussed in this paper.

REFERENCES

[1] C Bing, W Lisong. Research on Architecture of Network Security [J]. Computer Engineering and Applications, 2002, 38(7):138-140. DOI:10.3321/j.issn:1002-8331.2002.07.047.
[2] Marin G A. Network Security Basics [J]. Security & Privacy, IEEE, 2005, 3(6):68-72.
[3] Y Bingyu. An Elementary Introduction to Computer Network Security [J]. Computer Knowledge and Technology, 2009.
[4] https://www.conceptdraw.com/How-To-Guide/network-security-architecture-diagram
[5] https://www.herzing.edu/blog/what-network-security-and-why-it-important
[6] Infradara, "Top 5 Network Security Solutions and Technologies".
[7] Fortinet in Network Firewalls, "FortiGate: Next Generation Firewall (NGFW) Reviews, https://www.gartner.com/reviews/market/network-firewalls/vendor/fortinet/product/fortigate-next-generation-firewall-ngfw
[8] Genians, "What is Network Access Control?", 2018, https://www.genians.com/learn-more/insights/what-is-network-access-control/
[9] CISCO, "What is Data Loss Prevention (DLP)?", https://www.cisco.com/c/en/us/products/security/email-security-appliance/data-loss-prevention-dlp.html
[10] Forecepoint, https://www.forcepoint.com/cyber-edu/casb-cloud-access-security-broker
[11] Proofpoint, "Email Security and Protection", https://www.proofpoint.com/au/products/email-protection/email-security-and-protection