Assessing tools to analyze the techniques and mechanism for network risk minimization

Dr.Kamalakannan Machap
School of Technology
Asia Pacific University of Technology and innovation (APU)
Kuala Lumpur, Malaysia
dr.kamalakannan@staffemail.apu.edu.my

Taha Khamis
School of Technology
Asia Pacific University of Technology and innovation (APU)
Kuala Lumpur, Malaysia
tp064246@email.apu.edu.my

***Abstract*— In the presence of the increasing of dependency on the technologies nowadays, it's getting more and more essential to make sure that all the aspects of online information and data are secured. The internet is growing every day and the computer networks access increasing gradually. Therefore, the data integrity becomes one of the most important aspects that the organizations are looking at in the current moment. Network security has always been very important aspect that you need to consider while working over the internet. It's a fact that there is no network which can be immune to attacks but, to secure client data, a solid and effective network security solution is required. Data theft and sabotage can be reduced with a solid security system. Every organization requires the appropriate tools to deal with potential network risks and uncertainties. The security tools and techniques are meant to cope with a wide range of threats by performing various functions to make the network environment more secure and reliable.**

Keywords—Network security, email security, cryptography, packet filtering, Anti malware, firewall.

I. INTRODUCTION

The internet is growing increasingly popular. Cellphones, tablets, desktop computers, laptops, and pretty much any other form of smart device are used to access the internet by people all over the world. As the number of people using the internet grows, so do the number of treats and problems. Hackers are continuously seeking for network vulnerabilities or loopholes to exploit to gain access to your system and steal your data, therefore cybercrimes are becoming more common these days. As a result, we can see why network security is so important in keeping all our data safe and secure. Our gadgets are protected by network security from cyber threats from all around the world. Network security refers to the preventive steps taken by an organization to prevent cyber dangers such as cyber-attacks, unauthorized access to personal information, or any damage to the network's private data, users, or devices. The goal of a network security system is to keep the network reliable and secure for all its legitimate users [1].

According to latest research [2], a cyber-attack is defined as any attempt to gain unauthorized access to a computing system, computer, or computer network with the goal of causing damage to any of them. Individuals or groups could launch cyber strikes from any location. Cyber-attacks are aimed to create damage with a variety of goals in mind, including financial gain, distribution and retribution, or cyberwarfare. In this paper, discusses the three most important trends in computer security right now. Disruption, Distortion, and Deterioration are the main risks [3].

II. LITERATURE REVIEW AND RESEARCH

A. Network Security

According to latest research [2] a cyber-attack is defined as any attempt to gain unauthorized access to a computing system, computer, or computer network with the goal of causing damage to any of them. Individuals or groups could launch cyber strikes from any location.

Cyber-attacks are aimed to create damage with a variety of goals in mind, including financial gain, distribution and retribution, or cyberwarfare. In this article, we'll go through the three most important trends in computer security right now. Disruption, Distortion, and Deterioration are the main risks [3].

B. Issues and Challenges of network security

According to [4] there are five major network security concerns around the world, all of which are linked to one condition in network security: IT infrastructure complexity. This is the most serious problem in network security today, and we can't escape it. The current COVID-19 situation is causing an increase in the number of remote workers. Currently over 16 million remote workers are accessing the network, which means we must manage more devices and connectivity. Need to speed up the process of recognizing and responding to network security challenges.

C. Security misconfiguration

One of the most important network dangers is still misconfiguration. The majority of firewall vulnerabilities are caused by misconfiguration rather than firewall faults, because of the complexity of networks, which is growing all the time, fire barriers are difficult to manage. Hundreds of fire walls are used by many organizations, making it nearly hard to manage them manually. To manage the fire barriers, an automated approach is required. Humans, on the other hand, cannot be completely replaced in this process. The idea is to reduce human errors by providing networks with adaptive control and visibility.

D. Lax Previliged access control

A Special access for users, such as applications and machine identities, is referred to as privilege access. Over the last decade, misuse of privilege access has been linked to a number of security issues. Many prominent organizations, like as Yahoo! and Uber, have been victims of such attacks that illegally leveraged privilege access [5].

E. Tools Interoperability

The true issue isn't having too many tools; it's having too many tools that don't communicate data as well as they should. A network isn't truly made up of just one location. The exponential complexity is caused by a mix of "software-defined networks," "micro-segmentation," "network rules," and "network assets." To have a better knowledge of what's going on in a network, the security team must move from one panel to the next, attempting to make sense of what one metric means in connection to the others [4]. As a result, the environment invites user error and exposes vulnerabilities that attackers can exploit.

F. Network Visibility

For several years, the term "network visibility" has been well-known, and it has a devoted following. If you read the industry headlines from 2020, you'll think network visibility is a panacea for all your cybersecurity problems [6]. Safeguard Cyber performed a poll of 100 security leaders about their digital risk management system and digital communication protection, according to [7]. According to the findings of this poll, the majority of executives understand how to succeed in digital security, but they are having difficulty protecting their communications, which includes using third-party cloud services. The leaders were asked to rate their abilities to mitigate risk. Over 75% of them admitted to having limitations and vulnerabilities that prevent them from protecting all communication channels and digital assets. The lack of visibility on third-party cloud apps, which was at the heart of the recent Electronic Arts Slack hacking, is currently their biggest issue.

III. SECURITY TOOLS AND TECHNIQUES

Many companies have spent a significant amount of money on security tools and products to safeguard their networks from various dangers such as viruses, worms, DDoS assaults, and so on. (Veracode, undated). There are network security tools that can help your firm protect not only sensitive data but also the overall performance and integrity of its network. Its ability to stay in business is crucial as well. Two of the most crucial advantages of strong network security are the ability to continue operating and the ability to keep one's reputation. Because your network is subject to a variety of attacks, it must be prepared to defend against, identify, and respond to a variety of threats [8].

A. Cryptography

Encryption is used in encrypted email and other communications to ensure that only the intended recipient can read them. The symmetric key system, which is a "secret key" structure, is a simplified system. The information is encrypted with a private key before being delivered to the receiver for decryption. If the transmission is found, it may be intercepted and decoded by a third party. As a result, asymmetric cryptography, sometimes known as "public key" cryptography, was developed. Each user is given two keys: one for public use and the other for private use. Senders encrypt and transmit the message after requesting the recipient's public key because the message can only be deciphered with the recipient's private key, stealing the information is impossible [9].

B. Packet filtering

The method of maintaining network security by selectively permitting or denying packets based on the IP addresses, protocols, and channels of the sender and receiver. Packet filtering rule sets are used to configure network-layer firewalls, which provide very efficient security solutions. Packet filtering is also known as static filtering. “Unfiltered packets are sent throughout the network, adhering to the norms and regulations set forth. A packet that has been accepted or rejected is matched. Packets are filtered based on their IP addresses. If both IP addresses match, the packet is safe and valid. Packet filtering also looks at source and destination protocols like UDP and TCP because the sender may use many apps and programmes (TCP). Port addresses are also checked by packet filters. Some packet filters are inefficient and forget about used packets. Other packet filters, on the other hand, may keep track of previously utilised packet elements like IP addresses. Packet filtering protects a local area network against outside attacks (LAN). Because most routing devices include built-in filtering, packet filtering is a widespread and cost-effective security technique [10].

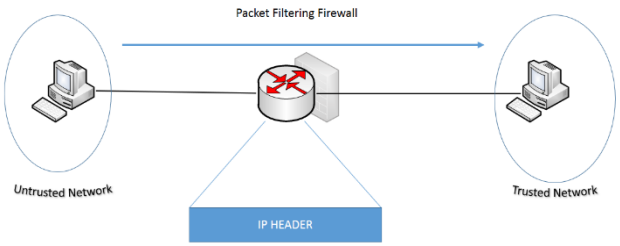

Fig1. Packet filtering

C. Email Security

Email messages are susceptible to misinterpretation, raising worries about email security. This became a worry with the introduction of email. An attacker can quickly read the contents of an email if it is intercepted. Corporations have enhanced email security practices over time to protect sensitive or secret information. Enterprises should employ a secure email gateway to implement best practices. Email gateways check for security flaws by authenticating and scrutinizing incoming and outgoing messages. Because of sophisticated cyberattacks, traditional safety precautions, such as preventing the attachment of known harmful files, have become useless. A secure email gateway with multiple layers is a preferable alternative [11].

D. Network Segmentation

A computer network's physical or logical segmentation. Direct interaction between two devices on the same network segment is possible. For communication between devices on different segments, a separate demarcation point is necessary typically a router or firewall. This will aid traffic and security management, resulting in enhanced overall security. Because of the various security precautions that hackers must take, separating the network into several pieces makes it more difficult for them to attack. End devices in a segmented network are workstations and servers with exactly the right network connectivity for legitimate business reasons.

Ransomware cannot spread and an attacker cannot swap out a system that has been isolated [12].

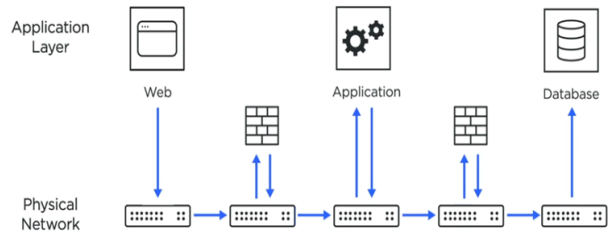

Fig 2. Network segmentation

E. *Anti Malware Software*

Anti-malware software checks compromised devices and networks for malware, finds it, and eliminates it. Antimalware software defends a computer or a corporate network against malicious infections such as viruses, worms, ransomware, rootkits, spyware, keyloggers, and other malware. Antimalware software can be set up on a single computer, a gateway server, or a network appliance. Effective antimalware programmes contain anti-spyware and anti-phishing features [13].

F. *Firewall*

A firewall acts as a guardian. Intruders can't get into your system since there's a barrier between them and it. Firewalls act as a filter, preventing access to your computer from the outside world. A firewall is a programme that prevents intruders from entering your network. By handling network traffic, it aids in the protection of your network and data. This project includes tasks such as blocking undesired network traffic and scanning for hackers and malware. Many operating systems and antivirus programmes include a firewall as a standard feature. Check to see if those options are enabled. Also, make sure your security settings are automatically updated [14].

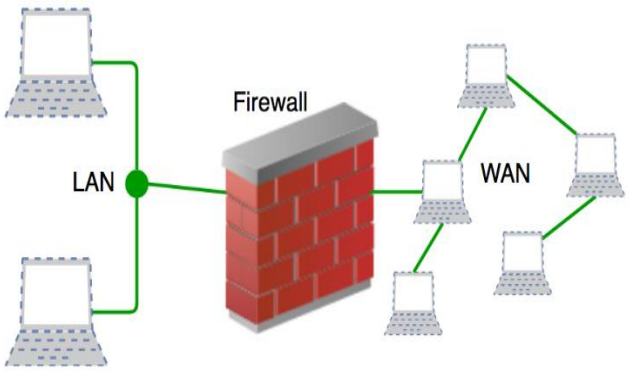

Fig 3. Firewall

IV. SECURITY TOOLS AND TECHNIQUES

A. *Simulation tools for email security*

Email Security is a programme that can help you keep your emails safe from various attacks. Protects against email-borne threats such as malware, unsafe links, phishing attacks, and spoofing, in addition to spam and viruses. AI-driven scanning was used to scan inbound and outbound traffic using threat intelligence.

B. *Simulation tools for firewall*

To provide complete next-generation firewall protection, the firewall employs deep learning and Synchronized Security. With Security Heartbeat, this firewall exposes hidden user, application, and threat hazards on the network and provides unique insights.

Fig 4. Home Page

C. *Simulation tools for anti malware*

Anti-Malware, a light-weight antivirus programme, can protect your PC from unwanted software such as viruses, ransomware, spyware, trojans, and adware. Surf Protection, Real-time File Guard, and Behavior Blocker are the three security levels of this anti-malware application. Surf Protection and Real-time File Guard scan for malware, preventing access to dangerous websites and fake connections. It detects threats that try to flee or that are downloaded from the internet quickly.

Fig 5. Home page

V. CONCLUSION

Every day, new risks and vulnerabilities emerge as a result of technological advancements. The vast expansion in the number of devices and networks is posing new challenges in terms of managing and controlling their security. As a result, with these new network risks, we need the assistance of tools and strategies that can help secure our digital lives. There are several solutions that can assist us reduce the possibilities of our data being stolen or our gadgets being harmed. It is critical for any firm to employ appropriate management solutions that may assist them in safeguarding sensitive information and preventing hackers from causing

damage to the organization's assets. Network security has long been a major priority for all enterprises and internet consumers. When it comes to technologies and networks, we live in a world that is speeding up. It is critical for everyone to maintain their digital lives safe and secure from hackers and threats all over the world. Although the level of risk varies from one attack to the next, it is always critical to keep our equipment and connections secure. A simple attack or a brief server crash can have a large impact and inflict significant damage to some companies and individuals. As a result, having the most up-to-date tools and procedures to protect our connections is critical. There are numerous tools and approaches for securing our connections and networks, yet the tools alone are insufficient. If we are faced with a situation where we must take action to preserve our network security, we must be informed and trained. Tools and software cannot replace users, but they can assist humans in limiting risks and monitoring network security.

REFERENCES

[1] Smartinfosys. Why Is Network Security Important? Kloud9. December 15, 2020.

[2] Pratt, M. K. cyber attack. SearchSecurity. January 13, 2021.

[3] G.Computer. Top 10 Computer Security Threats to Business IT in July 20,2021.

[4] FireMon. Network Security Challenges & Threats | Vital IT Security Issues. May 30, 2020.

[5] CyberArk Software. What is PAM? Privileged Access Management Definition, July 22, 2021.

[6] Brode, B. *The Problem With Network Visibility*. Network Computing. January 11, 2021.

[7] SecurityMagazine. Lack of visibility is the biggest challenge for security leaders when safeguarding digital communications. 2021–07-12 | Security Magazine. July 12, 2021

[8] ElysiumPro. Network Security Tools and Techniques. December 18, 2020.

[9] Kaspersky. Cryptography Definition. January 13, 2021. Www.Kaspersky.Com.

[10] Techopedia. Packet Filtering. Techopedia.Com. January 25, 2017.

[11] ProofPoint, Email Security Proofpoint US. June 1, 2021.

[12] Grimmick, R. Network Segmentation Varonis. Inside Out Security. January 12, 2021.

[13] Comodo, C. What is Antimalware? | Benefits and How does it Works. Comodo News For Enterprise Security. August 12, 2021.

[14] Grace, A. What is a firewall? Firewalls explained and why you need one. Norton. July 17, 2021.