Use of network and cyber security tools to counter the security obstacles

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

Abulla Muaza
School of Technology
Asia Pacific University of Technology and innovation (APU)
Kuala Lumpur, Malaysia
tp060110@email.apu.edu.my

***Abstract*— In this study we have discovered the issues of challenges in networking and cyber security that everything is dependent on latest technology, and the most significant feature of technology is the network. It is critical to limit the risk of threats to create a stable and reliable network environment for users. According to certain surveys, most security vulnerabilities are caused by "insider risks." That is, the hazards that arise within in companies are greater than the threats that arise externally. There are numerous tools and strategies that can be utilized in a network environment to address security issues and challenges. Although security risks and obstacles can be mitigated with the use of these tools and strategies, it is difficult to make a network completely threat-free. The fundamental cause for this is the rapid advancement of technology and the increasing use of it. According to surveys, security concerns are increasing day by day because of rapid technological change and the growing number of devices connected around the world. Attackers are continuously coming up with new ways to get around the security protections built into devices and networks. Several security technologies and strategies could be utilized in a network to address or lessen these security difficulties and obstacles. Some are software tools, while others are physical tools.**

Keywords*— *Network security, cryptography, firewall, Wireless networks, BYOD, Cyber Security.

I. INTRODUCTION

The Networking has brought us all together under one roof, allowing us to interact and collaborate more easily. The reality remains the same whether it is our house, a school, a college, or a corporate organization. It is nearly difficult to meet our daily demands without the assistance of network technologies. While it makes our lives easier, it also puts us at risk, if necessary, security precautions are not done. That is, it is critical to secure the network on which we are connected to protect data from unauthorized access. Network security ensures that the network and its services are protected from illegal modification, destruction, or disclosure. This means that it's critical to secure the network we're on to keep our data safe from unauthorized access. Network security is defined as the protection of a network and its services against unauthorized modification, destruction, or disclosure, as well as ensuring that the network has no negative impact on users or employees [1].

According to [2] cyber-attacks have obviously increased in recent years, with the world witnessing some horrendous attacks involving large data breaches, crypto jacking, and a variety of other forms in 2018. According to Threat Horizon 2019, there will be nine key categories of threats that organizations will encounter in the next years because of technological transformation. These dangers are organized into three main themes in the paper. Disruption, Distortion, and Deterioration are their names [3].

II LITERATURE REVIEW AND RESEARCH

A. Network Security

In the commercial world, network security is a big concern, particularly when devices are connected to a network in a disjointed manner. Third-party networks and IoT devices are thought to be the most common sources of network disruption. Hackers also utilize more advanced and comprehensive technologies, as well as networked devices that are not linked to the network and users who are unaware of the potential hazards to their devices and the network they are on. The more devices connected to a network, the greater the risk of a security breach [4].

According to [4] conducted a study among security professionals based on 2019 security issues and difficulties. According to the report, the number one security risk is "Insider threats," which is cited by 44% of respondents. Threats to an organization that originate from within the company are referred to as "internal threats."

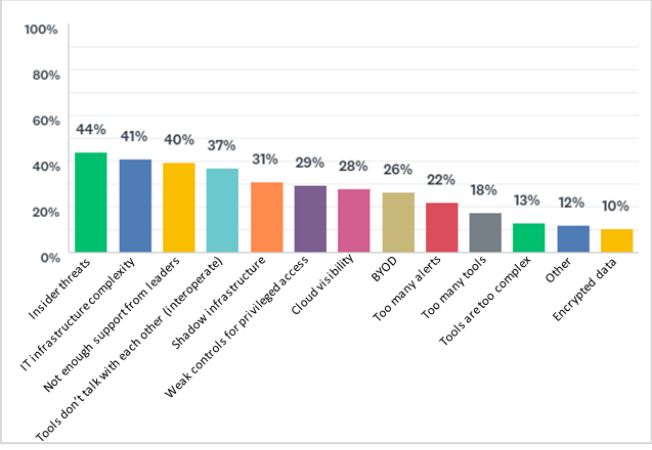

Fig 1. Top 10 security challenges

According to the graph above, the number one hazard to a network is threats that originate within the organization, most likely owing to a lack of awareness regarding security issues. The network's complexity, as well as a lack of technological support and resources, are some of the organizations' key issues. Weaker access management and Bring Your Own Device (BYOD) are also among the top ten problems and

challenges. BYOD (bring your own device) is becoming more popular in schools, universities, and businesses, yet it is well recognized that BYOD increases the risk of data theft and virus infection [5].

B. Wormhole attacks

In wireless networks, a wormhole assault is a typical occurrence. It is a risky attack in which two attackers strategically position themselves in the network to listen to the network to obtain wireless information [6]. The attackers' strong positioning in the network.

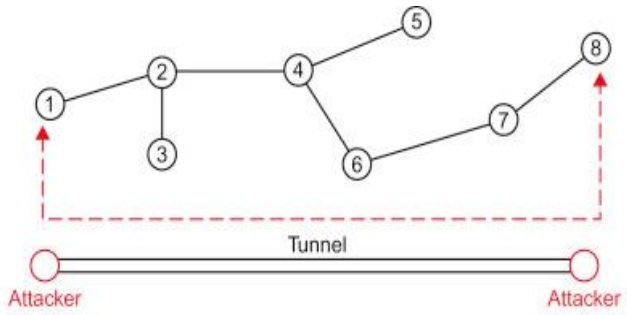

Fig 2. How attackers locate in the network.

C. Eavesdropping Attacks

This is a dangerous sort of assault that primarily targets wireless sensor networks. The attacker obtains confidential and private information from a weakened connection by installing network monitoring software that captures data as it is transmitted in this type of attack.

Aside from the active and passive security challenges described above, there are other factors that might affect a network's security, such as physical security. When everyone is focused on cyber dangers, it's crucial not to overlook the data's physical security [7].

III. SECURITY TOOLS AND TECHNIQUES

A network manager's most significant and critical responsibility is to protect the company's data. This information could include personal and confidential information about the company, its employees, and its customers. Another thing to remember is that the sort of treat differs according on the type of business, the network's design, and its security. As a result, it's critical to carefully select the best and most appropriate security tools and procedures for the Network. One of these tools or strategies cannot be relied upon solely by a firm or organization [8]. The important thing to remember is that practically every security technique can and will fail at some point, whether due to design flaws, poor implementation, or human error. As a result, you shouldn't count on a single tool to save you from calamity.

A. Cryptography

One of the most extensively used techniques for safeguarding information and services is cryptography. “Secret writing” is the term used in Greek cryptography. It is feasible to encrypt data transported from one node to another and decode the data at the receiving end using cryptography. This eliminates the possibility of data theft during transmission [9]. Cryptography technology is utilised in thousands of applications, including social media apps like WhatsApp and Viber. Currently, billions of individuals use this feature in their apps all over the world, though the majority are unaware of it [10].

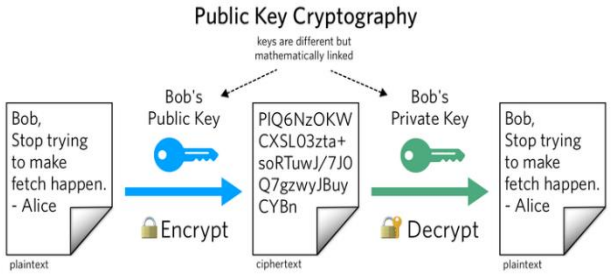

Fig 3. How Cryptography works

B. Firewall

Another security strategy that may be applied in the network to secure data using router settings is packet filtering. By default, the router permits all types of data to flow freely in and out of the organization's network. We can define what kind of access is allowed for outside the network to access the internal network by turning on the router's ACL (Access Control List). Packet filtering has the drawback of not being able to confirm that the source address is what it claims to be. As a result, multiple layers of packet filters are required to localize traffic [9].

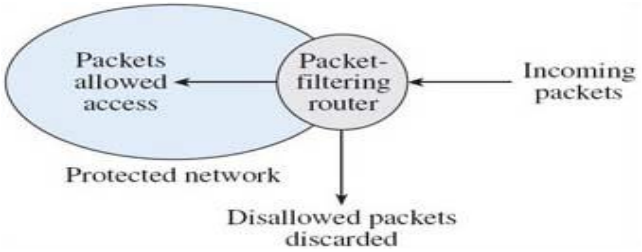

Fig 4. How packet filtering is done by the router

C. Use tools with simulated data

As most of the official and important communication are conducted through emails, it’s very important to have an email security system. Email security detects and filters questionable email, warning the user that opening it could be dangerous. Most email clients and service providers, such as Microsoft (Office365) and Google (Gmail), employ this technology to identify potentially harmful emails and block them. Phishing using emails is one of the most common ways for hackers to obtain users' personal and confidential information.

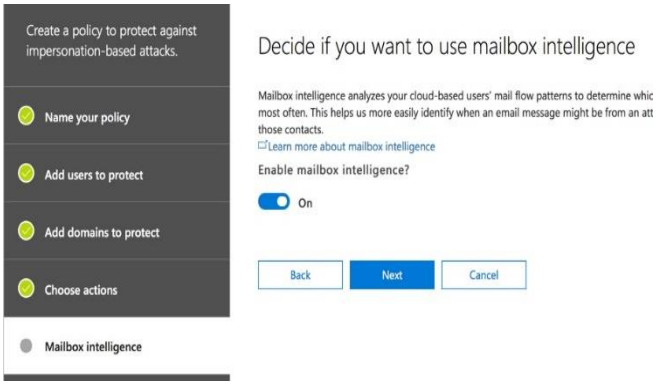

Fig 5. Office365 Mail box intelligence

D. Firewall

A firewall is one of the most effective hardware tools for protecting a network from both external and internal threats. Intrusion detection and prevention, bandwidth and access control, VPN, content filtering, anti-spam, and other features are included in the latest firewalls.

If BYOD (bring your own device) services are available, connect filtering and bandwidth management are two very important functions for schools and universities. The bandwidth will be affected when more devices join to the network, however the problem can be mitigated by using the bandwidth management option. Students can be protected against infidelity and undesired content by using content screening [11].

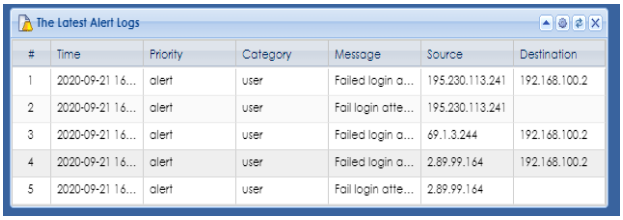

Fig 6. Alerts of a firewall with details

E. Simulation tools.

An online simulator is used to test how cryptography works. To begin, the system generates two random keys that will be used as the public and private keys. The message is subsequently encoded with the encryption key and sent to the recipient. When the receiver receives the communication as an encrypted message, the decryption code is used to decode it [11]. A screenshot of the simulation is shown below.

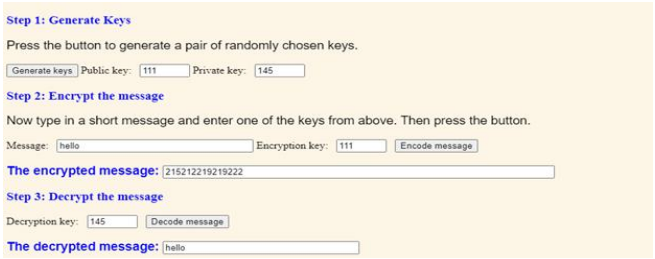

Fig 7. Public-Key encryption demonstration

The Huawei HG8247H router is utilized in this simulation. The goal of this simulation is to prevent some external addresses from being accessed. To do so, first enter the device's mac address into the router, and then create a rule to block the address. The device is added to the rule after it has been created. This will prevent the user from visiting the address.

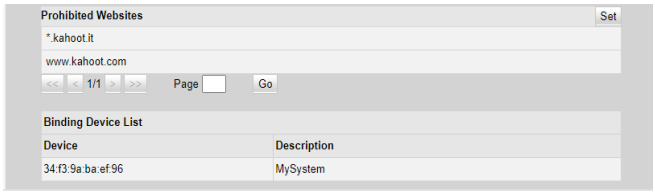

Fig 8. Prohibited address is entered

In this test, the live firewall configuration in one of the schools that allows students to bring their own devices to class. Because this firewall is primarily utilized to deliver services to two types of users (staff and students), two separate rules were designed based on the management's requirements. All social networking platforms are, in general, prohibited by the application filtering module. This means that no device connected to the school network will be able to access social media sites like Facebook, Twitter, or WhatsApp. The displays below demonstrate how various configurations are made in the firewall.

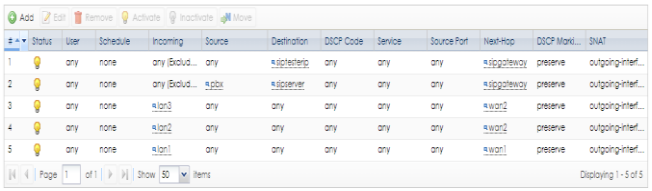

Fig 9. How networks are distributed

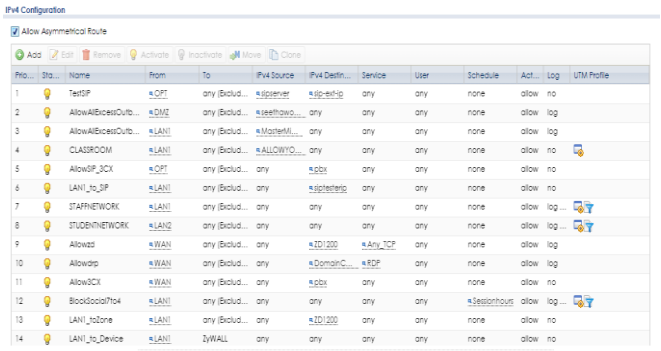

Fig 10. Policy control for staff and students

Fig 10. shows how polices are created based on the user types. As highlighted on screenshot, there are content filtering rules created for classrooms, staff network as well as student network.

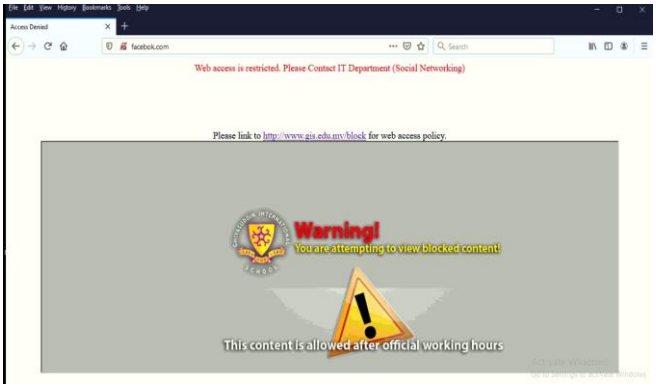

Fig 11. Access denied

Fig 11. shows the alert which users get when because access to social media is blocked through firewall.

IV. CONCLUSION

According to research and studies, technology is rapidly evolving, and the use of electronic devices in our everyday lives is expanding. As the use of these gadgets in our daily lives and work environments grows, the potential for security issues and challenges grows as well. Security threats from within and outside the company, attacks due to end user ignorance, and the way security measures are implemented in the network are some of the most typical concerns and challenges in the network. There are numerous tools and

strategies that may be employed to address the concerns and challenges we encounter in network security. Network security has become one of the most pressing concerns for businesses all around the world. The level of risk is the same whether it's a hospital, an NGO, a school, or an IT firm. In technology advances, attackers try to come up with new ways to target the network and the devices on it. It is critical to adopt defensive measures in the network to reduce the chance of data being lost or stolen by a hacker and to improve network security.

As a result, the network should employ all available tools and methodologies. We can't rely on just one security instrument or technique, as points out. When considering network security, it's equally critical to consider how the network should be designed. For example, hierarchical or the notion of network segmentation approach allows network administrators more control over monitoring and managing traffic flow in the network. Aside from the tools and procedures, it is critical for an organization to keep its employees and customers informed about the current security dangers. We will never be able to completely secure our data, but we can constantly reduce the security risks and problems by using tools and procedures.

REFERENCES

[1] S.Pandey, "Modern network security: Issues and challenges," International Journal of Engineering Science and Technology, vol. 3, no. 5, pp. 4351-4357, 2011.

[2] Belani, G, Cybersecurity Threats to Be Aware of in 2020, pp. 67-71.

[3] Infosecurityeurope, THREAT HORIZON 2019,pp.64-66.

[4] Bricata, The Top 10 Network Security Challenges in 2019. pp.45-48

[5] Hollander, G., 2019. 7 Risks Involved With Bring Your Own Device (BYOD) 2019. Pp. 112-114.

[6] M., K.Gayathri, K. & Inbavalli, M., n.d. Network Security and Types of Attacks in Network Security. Journal of Engineering (IOSRJEN) , pp. 58-63.

[7] Ahola, M., Top 5 Physical Security Risks - And How to Protect, 2019, pp. 126-129.

[8] Shadowsky, G. Information technology security hand book. In: WASHINGTON: THE WORLD BANK, 2003. pp. 30-40.

[9] PANDEY, S., MODERN NETWORK SECURITY. Volume 3,2011. pp. 1-7.

[10] Qadir, A. M. & Varol, N., A Review Paper on Cryptography. A Review Paper on Cryptography, 1(1), pp. 2-6.

[11] Kaspersky, IT SECURITY RISKS SPECIAL REPORT SERIES 2019.