International Journal of Advanced Trends in Computer Applications
www.ijatca.com

A Review on Network Security and Privacy

[1]Diksha Gupta, [2]Karnish Sharma, [3]Neeshu Sharma
[1, 2,3]Computer Science Department,
Chandigarh University, Punjab
[1]19bcs1557@gmail.com, [2]19bcs1544@gmail.com, [3]neeshusharma.cse@cumail.in

Abstract: *In today's world which is getting digitalized day by day and the data is increasing exponentially it becomes very important to check for the data security and privacy. As with the increasing data, the threat to that data is also increasing at the same rate. The data which is getting uploaded on the internet or any other network needs to be safe for the sake of the company's private data or for the people who are using that network. In this paper the authors had discussed the various types of attacks, threats on the network from which the company or an individual needs to be careful to protect the company from any malicious activity. This paper also explores the various security measures to protect the data and offer proper security and privacy to it.*

Keywords: Network security, virtual private network, network access control, firewall.

I. INTRODUCTION

Network security refers to a set of rules and regulations that protects our data from getting leaked and protects the confidentiality and accessibility of computer networks by using both hardware and software technologies.

Today's fast-growing technology has made it very important to protect our data thus creating the need for data security and privacy. Talking about privacy it refers to the usage of data by someone else i.e. the method it is being used. Thus, to protect the mishandling of data we need knowledge of both network security and privacy. One of the ways by which the data is protected includes cybersecurity products such as Virtual Private Networks (VPNs) which at the same time does not compromise with the security and privacy of data.

Network security starts with the authentication of users like it asks for the username and password thus allowing only the authentic user to enter the system. It is often regarded as one-factor authentication. One example of this one-factor authentication is 'Firewall Authentication'. There are two types of attacks on networks one is **Passive** such as wiretapping and encryption and another type of attack is **Active** attack such as virus, eavesdropping, etc. types of protections includes antivirus and anti-malware software, application security, firewall authentication, application security, firewall authentication, data loss prevention, email security, mobile device security network segmentation. Besides all this a user needs to be careful every time while he is using the online networks and an organization or business should change their online protection settings from time to time to get protected from the data leakage or data-stealing or from getting hacked and losing important information of their company.

II. LITERATURE REVIEW

The research in the field of network security and privacy is accelerating very fast as never before due to the increasing rate of data production and spams. The authors [1] have done their work in the field of security in wireless sensor networks using authentication and security of the users.

The authors [2] had extended their work in the field of medical sciences whereby using computing technologies we can inspect the patients' health using devices like WBAN and the need for data privacy and protection there. The major concerns were secure and dependable distributed data storage, and fine-grained distributed data access control.

The authors [3] had carried forward the authors [2] work and done their work in identifying the physical layer as the important layer from which the attackers might get access in the system and can steal the data. The protection of the physical layer becomes very important for wireless networks as compared to wired ones.

The basics of network security and privacy and the areas which needed the work most and the various threats in the IT sector are researched by the authors [4].

Thus, from the above works and researches we had reviewed are paper and conferred that this new emerging field of computer science and the future scopes.

III. WORKING OF NETWORK SECURITY

There are many layers of network security. As a company or organization can't make it that where the attackers might attack and steal their data [4]. Thus, the organization should get ready at every level to protect their data. The layers included for network security are:

3.1 Physical layer/physical network security

This layer is designed so that no unauthorized personnel can access the routers, cables or cupboards and so on physically. The protection at this layer can be done using biometric authentication of the authorized persons and using other such locks to prevent the stealing of the company's important data [2].

3.2 Technical layer/technical network security

This layer works in two ways- first by making sure that no unauthorized personnel can access the data which is stored on the network or which can be present around the network and second is making sure that there is no attack on the data using malicious activity by the employees.

3.3 Administrative network security

This control level makes sure that how the authentication of the employees should be done. It also consists of security policies and processes that control user behavior.

IV. ENSURING NETWORK SECURITY AND PRIVACY

Since we had talked about the layers at which data is at risk of getting stolen or getting corrupted. Now it's time to talk about the protection devices or software to achieve network security and ensure privacy of data [7].

4.1 **Various steps include**

- Securely monitoring and reporting
- Endpoint protection
- Email protection
- Internet content filtering
- Firewall monitoring and management
- Dual factor authentication

To achieve all this [1] — [5] we have got various software and techniques as listed below.

4.2 **Network access control**:

To ensure that potential attackers cannot infiltrate the network by joining their devices and control the basic infrastructure of their company Network Access Control can bet set at the basic granular level by allowing access to most of the folders but restricting the confidential folders and thus ensuring proper privacy of data.

4.3 **Antivirus and anti-malware sources:**

These are the most basic software's that are used to prevent malicious software or virus to attack the system and hack or steal the data. Some examples of antivirus software are Norton antivirus, avast antivirus.

4.4 **Firewall protection:**

Firewall act as a barrier between the distrusted external networks and allows only trusted administrators to enter and have access to the data and thus ensuring that no unauthorized personnel can enter the network and do some activity that can risk the data of company or organization [3].

4.5 **Virtual Private Networks:**

These networks create a connection to the network from another endpoint or site. A most basic example of these networks is that if an employee is working from his home and connect to the company's network using VPN's he/she can get encrypted data and can use that only after authentication and can thus communicate easily between these networks.

V. TIPS FOR PROTECTING YOUR PRIVACY AND SECURITY

Besides the network security and privacy of a company/organization it is also important that one should also take care of his/her data at an individual level to protect his/her network.

Below are the tips which we can take at our level:

- ➢ We should not share our important information on social media since some hackers who are watching you over and can risk your information.
- ➢ We should shred the important information or documents before recycling them in the trash.
- ➢ Always read the privacy policy of an app or software before signing in to them since once you share any information online it's no longer in your control.

- ➢ Always guard your social security number and avoid giving it to anyone instead uses other forms of identification.
- ➢ Always use good antivirus software on your system.

VI. TYPES OF ATTACKS

Network attacks refer to attacking a software or a hardware that is on the network either by diverting the route of the path from which the data is traveling or by initiating some command to make the network activate to get some sort of information. [7]. Based upon this network attacks can be categorized into two types: "**Passive Attacks**" are those attacks in which a network intruder catches data traveling through network and "**Active Attacks**" in which an intruder start commands to disturb the networks normal operation or to conduct a scan or something like this on the lateral movements of the system to find and gain access to the important data or information available through assets via the network.

6.1 **Passive Attacks**

- ➢ Wiretapping
- ➢ Port scanner
- ➢ Idle scan
- ➢ Encryption
- ➢ Traffic Analysis

6.2 **Active Attacks**

- ➢ Virus
- ➢ Eavesdropping
- ➢ Data Modification
- ➢ Denial-of-service attack
- ➢ DNS spoofing
- ➢ Man in the middle
- ➢ ARP poisoning
- ➢ VLAN hopping
- ➢ Smurf attack
- ➢ Buffer overflow
- ➢ Heap overflow
- ➢ Format string attack
- ➢ SQL injection
- ➢ Phishing
- ➢ Cross-site scripting
- ➢ Cyber-attack

VII. THREATS TO THE NETWORK

Network security threats are classified into different layers/types-

7.1 Physical theft:

By physical theft it means to access the hardware such as routers, cables or cupboards etc. Some of the physical theft examples include line monitoring or buffer force attacks or theft etc.

7.2 Identification:

It refers to hack some software or some hardware through some illegitimate means such as through password crack or cheat passwords.

7.3 Program attacks:

It means that some type of malicious program enters into the system by some means such as Trojan horse or worms etc.

7.4 System Vulnerability:

This type of network threat includes compromising with the system that is not using genuine software or hardware in the system such as implementation code, unsafe service etc.

7.5 Access control:

It includes allowing access to an illegitimate user to enter into the system and preventing the legitimate once in some cases such as denial of service attacks, buffer overflows, brute force attacks, social engineering, etc. [4]. The below picture indicates that the majority of the people face (almost 45%) receiving spam mails which could result in the virus into their systems followed by phishing i.e. making a trap for the people to steal their personal information (about 25%) followed by malware receiving, account sent spam and password stolen/ account hijacked.

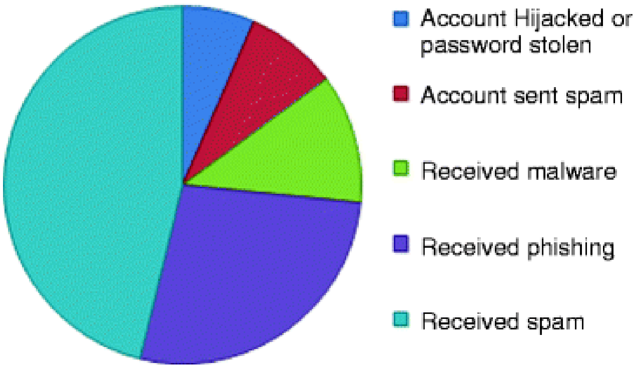

Figure 1: Problem experienced on social networks.

VIII. THE FUTURE OF NETWORK SECURITY

Today's world is getting a technology addict it is very important to think about network security. As in the coming years' technology would be in every place, all the data would be digitalized and the threat to these data would also increase with the increase in the scope of network security as a carrier option [7]. As a security engineer many people are working towards providing more secure networks for companies as well as for individuals to prevent data leakage and steal. For network and data privacy one should always use encrypted data for information transfer which is provided by many apps and in the future it is expected that all the data would be encrypted and it would only be available to the authorized users. Some advancements that can come into the market keeping in view the network security and privacy include there will be software that will have inbuilt security modules with each endpoint/server being firewalled by default and no more DMZ would be required. Also, with the increase in cloud services the firewall rule sets would be automatically, created based on the provisioning of cloud instances.

IX. CONCLUSION

In conclusion we can say that while using technology one should be careful what he/she is sharing online. Since any information once shared carelessly online or over a distrusted network can get you in danger and can leak your valuable personal information. In today's world when most of our data is getting digitalized one should know the importance of network security. For a company it becomes very important to seriously look at the network security. As any carelessness used in network security and data privacy can lead to a very high cost for the company to pay. Some protective measures which the company must take include firewall authentication, biometrics for the physical access of important hardware, so that only authorized personnel could get access to the data. The IT security department of the company should prepare a very strict model of network security so that it becomes difficult for the hackers to enter either through passive or active ways of hacking the system and can interrupt the network. At the end network security and data privacy should be taken seriously by every individual and every company. No information should be shared online without proper knowledge.

References

[1]. L.Devi, S.P.Shantharajah, “A Survey on Authentication and security maintenance in wireless sensor network”, Vol.4 Issue.5, pp 53-70, May-2015

[2]. M. Li, W. Lou, and K. Ren, "Data security and privacy in wireless body area networks," in IEEE Wireless Communications, vol. 17, no. 1, pp. 51-58, February 2010

[3]. K. Zeng, K. Govindan, and P. Mohapatra, "Non-cryptographic authentication and identification in wireless networks [Security and Privacy in Emerging Wireless Networks]," in IEEE Wireless Communications, vol. 17, no. 5, pp. 56-62, October 2010

[4]. SattarovaFeruza Y. and Prof. Tao-hoon Kim, “IT Security Review: Privacy, Protection, Access Control, Assurance and System Security,” International Journal of Multimedia and Ubiquitous Engineering Vol. 2, No. 2, pp. 17-32 April 2007

[5]. Arpna Dhingra, S Mittal, H Kaur, A Singh “A Review on Techniques of Spam Classification in Twitter,” International Journal of Advanced Trends in Computer Applications (IJATCA) Volume 1, Number 5, May 2015, pp. 57-59 ISSN: 2395-3519

[6]. Adrian Perrig, John Stankovic, David Wagner, “Security in wireless sensor networks,” Volume 47, Number 6, pp 53-57, 2004

[7]. Shailja Pandey, ” Modern Network Security: Issues And Challenges”, Vol. 3, Uttar Pradesh Technical University, 2011

Author Profile

Diksha Gupta is a student pursuing bachelor of engineering in computer science from Chandigarh University, Punjab from the year 2019-2023.