NETWORK SECURITY CHALLENGES

[1]Rajeswari.C, [2] Saravanan.P
[1]M.Phil. Research Scholar, D.B.Jain College (Autonomous), Thoraipakkam, Chennai, India.
[2]Assistant Professor, D.B.Jain College (Autonomous), Thoraipakkam, Chennai, India.

Abstract : Security is a broad topic and covers a multitude of sins. In its simplest form, it is concerned with making sure that nosy people cannot read, or worse yet, secretly modify messages intended for other recipients. It is concerned with people trying to access remote services that they are not authorized to use. Most security problems are intentionally caused by malicious people trying to gain some benefit, get attention, or to harm someone. Network security problems can be divided roughly into four closely intertwined areas: secrecy, authentication, nonrepudiation, and integrity control. Secrecy, also called confidentiality, has to do with keeping information out of the hands of unauthorized users. This is what usually comes to mind when people think about network security. Authentication deals with determining whom you are talking to before revealing sensitive information or entering into a business deal. Nonrepudiation deals with signatures.

IndexTerms - Network Security, attacks, hackers, Cloud-environment security, zero-trust model (ZTM), Trend Micro internet security.

I. INTRODUCTION

Network Security management is different for all kinds of situations and is necessary as the growing use of internet. A home or small office may only require basic security while large businesses may require high maintenance and advanced software and hardware to prevent malicious attacks from hacking and spamming [1]

The Network Security is constantly evolving, due to traffic growth, usage trends and the ever changing threat landscape [3]. When developing a secure network, the following need to be considered [2]:

1. Access – authorized users are provided the means to communicate to and from a particular network
2. Confidentiality – Information in the network remains private
3. Authentication – Ensure the users of the network are who they say they are
4. Integrity – Ensure the message has not been modified in transit
5. Nonrepudiation – Ensure the user does not refute that he used the net

Network devices—such as routers, firewalls, gateways, switches, hubs, and so forth—create the infrastructure of local area networks (on the corporate scale) and the Internet (on the global scale). Securing such devices is fundamental to protecting the environment and outgoing/incoming communications. You also have to be aware of security risks and controls available in the public switched telephone networks (PSTN) infrastructure because PSTNs are often used for computer communications. This section of the chapter introduces the security concepts applicable to physical devices, network topologies, and storage media.

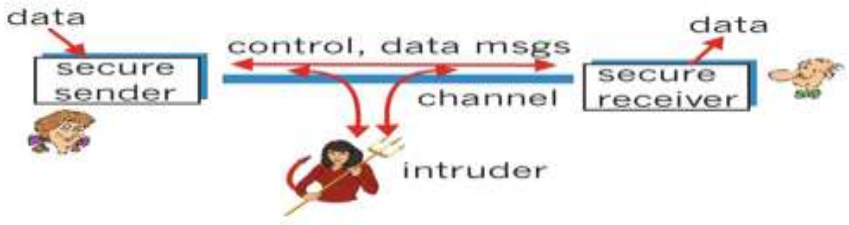

Figure1. Network Security

II. OBJECTIVE

As time goes on, more and more new technology will be developed to further improve the efficiency of business and communications. At the same time, breakthroughs in technology will provide even greater network security, therefore, greater piece of mind to operate in cutting edge business environments. Provided that enterprises stay on top of this emerging technology, as well as the latest security threats and dangers, the benefits of networks will most certainly outweigh the risks [6].

III. WHY SECURITY NEEDED

The security has become very essential due to wide spread use of internet in our daily life. Initially internet was developed for connectivity purpose. Now all the critical information related to banking, business correspondence, money transactions, online purchasing happens with the use of internet. Hence it is very important to protect subscriber personal information, confidential data, passwords, credit or savings card information (used for online purchasing) etc.

Today internet is evolving very fast and use of application specific online contents has become predominant on various networks. Security companies are working on different ways to handle security related aspects.

IV. NETWORK SECURITY: WORKING AND BENEFITS

Network security is an organization's strategy that enables guaranteeing the security of its assets including all network traffic. It includes both software and hardware technologies. Access to the network is managed by effective network security, which targets a wide range of threats and then arrests them from spreading or entering in the network.

Network security is an integration of multiple layers of defences in the network and at the network. Policies and controls are implemented by each network security layer. Access to networks is gained by authorized users, whereas, malicious actors are indeed blocked from executing threats and exploits.

Our world has presently been transformed by digitization, resulting in changes in almost all our daily activities. It is essential for all organizations to protect their networks if they aim at delivering the services demanded by employees and customers. This eventually protects the reputation of your organization. With hackers increasing and becoming smarter day by day, the need to utilize network security becomes more and more impotent.

V. TYPES OF NETWORK SECURITY

- Application Security
- Data Loss Prevention (DLP)
- Email Security Firewalls
- Mobile Device Security
- Network Segmentation Virtual Private Network (VPN)
- Web Security
- Wireless Security
- Behavioral Analytics
- Security Information and Event Management (SIEM)
- Endpoint security
- Network Access Control (NAC)
- Antivirus and Antimalware Software

5.1 ANTIVIRUS AND ANTIMALWARE SOFTWARE:

This software is used for protecting against malware, which includes spyware, Trojans, worms, and viruses. Malware can also become very dangerous as it can infect a network and then remain calm for days or even weeks. This software handles this threat by scanning for malware entry and regularly tracks files afterward in order to detect anomalies, remove malware, and fix damage. Viruses are self replication programs that use files to infect and propagate [5]

5.2 Application Security:

It is important to have an application security since no app is created perfectly. It is possible for any application to comprise of vulnerabilities, or holes, that are used by attackers to enter your network. Application security thus encompasses the software, hardware, and processes you select for closing those holes.

5.3 Behavioral Analytics:

In order to detect abnormal network behavior, you will have to know what normal behavior looks like. Behavioral analytics tools are capable of automatically discerning activities that deviate from the norm. Your security team will thus be able to efficiently detect indicators of compromise that pose a potential problem and rapidly remediate threats.

5.4 Data Loss Prevention (DLP):

Organizations should guarantee that their staff does not send sensitive information outside the network. They should thus use DLP technologies, network security measures that prevent people from uploading, forwarding, or even printing vital information in an unsafe manner.

5.5 Email Security:

Email gateways are considered to be the number one threat vector for a security breach. Attackers use social engineering tactics and personal information in order to build refined phishing campaigns to deceive recipients and then send them to sites serving up malware. An email security application is capable of blocking incoming attacks and controlling outbound messages in order to prevent the loss of sensitive data.

5.6 Firewalls:

Firewalls place a barrier between your trusted internal network and un trusted outside networks, like the Internet. A set of defined rules are employed to block or allow traffic. A firewall can be software, hardware, or both. The free firewall efficiently manages traffic on your PC, monitors in/out connections, and secures all connections when you are online.

Intrusion Prevention System (IPS): An IPS is a network security capable of scanning network traffic in order to actively block attacks. The IPS Setting interface permits the administrator to configure the rule set updates for Snort. It is possible to schedule the rule set updates allowing them to automatically run at particular intervals and these updates can be run manually on demand.

5.7 Mobile Device Security:

Mobile devices and apps are increasingly being targeted by cybercriminals. 90% of IT organizations could very soon support corporate applications on personal mobile devices. There is indeed the necessity for you to control which devices can access your network. It is also necessary to configure their connections in order to keep network traffic private.

5.8 Network Segmentation:

Software-defined segmentation places network traffic into varied classifications and makes enforcing security policies a lot easier. The classifications are ideally based on endpoint identity, not just IP addresses. Rights can be accessed based on location, role, and more so that the right people get the correct level of access and suspicious devices are thus contained and remediated.

5.9 Security Information and Event Management (SIEM):

SIEM products bring together all the information needed by your security staff in order to identify and respond to threats. These products are available in different forms, including virtual and physical appliances and server software.

5.10 Virtual Private Network (VPN):

A VPN is another type of network security capable of encrypting the connection from an endpoint to a network, mostly over the Internet. A remote-access VPN typically uses IPSec or Secure Sockets Layer in order to authenticate the communication between network and device.

5.11 Web Security:

A perfect web security solution will help in controlling your staff's web use, denying access to malicious websites, and blocking web-based threats. It enables protecting your web gateway on site or in the cloud. "Web security" also refers to the steps taken in order to protect your own website.

5.12 Wireless Security:

The mobile office movement is presently gaining momentum along with wireless networks and access points. However, wireless networks are not as secure as wired ones and this makes way for hackers to enter. It is thus essential for the wireless security to be strong. It should be noted that without stringent security measures installing a wireless LAN could be like placing Ethernet ports everywhere. Products specifically designed for protecting a wireless network will have to be used in order to prevent an exploit from taking place.

5.13 Endpoint Security:

Endpoint Security, also known Endpoint Production or Network Security, is a methodology used for protecting corporate networks when accessed through remote devices such as laptops or several other wireless devices and mobile devices

5.14 Network Access Control (NAC):

This network security process helps you to control who can access your network. It is essential to recognize each device and user in order to keep out potential attackers. This indeed will help you to enforce your security policies. Noncompliant endpoint devices can be given only limited access or just blocked.

VI. TYPES OF NETWORK SECURITY

When setting up a network, whether it is a local area network (LAN), virtual LAN (VLAN), or wide area network (WAN), it is important to initially set the fundamental security policies. Security policies are rules that are electronically programmed and stored within security equipment to control such areas as access privileges. The policies that are implemented should control who has access to which areas of the network and how unauthorized users are going to be prevented from entering restricted areas. The individual or group of people who police and maintain the network and its security must have access to every area of the network. Once your policies are set, identity methods and technologies must be employed to help positively authenticate and verify users and their access privileges. Making sure that certain areas of the network are "**password protected** "only accessible by those with particular passwords is the simplest and most common way to ensure that only those who have permission can enter a particular part of the network.

The golden rules, or policies, for passwords are:

- Change passwords regularly
- Make passwords as meaningless as possible
- Never divulge passwords to anyone until leaving the Company.

A type of attack called port scanning occurs when a whole section of a network is scanned to find potential targets with open services [4]

VII. CONCLUSION & FUTURE ENHANCEMENTS

The future will possibly be that the security is similar to an immune system. The immune system fights off attacks and builds itself to fight tougher enemies. Many security developments that are taking place are within the same set of security technology that.

Network security is an important field that is increasingly gaining attention as the internet expands. The security threats and internet protocol were analyzed to determine the necessary security technology. The security technology is mostly software based, but many

common hardware devices are used. The current development in network security is not very impressive.

Secure networks are important for proper operation of IT systems as most applications work in the networking environment. An essential part of the network design is the security architecture that describes security zones and layers.

REFERENCES

[1].Predictions and Trends for Information, Computer and Network Security [Online] available: http://www.sans.edu/research/security-laboratory/article/2140

[2].ES Dowd, P.W.; McHenry,J.T., "Network security: it's time to take it Seriously," Computer, vol.31, no.9, pp.24- 28, Sep 1

[3] Network Security [Online] available: http://en.wikipedia.org/wiki/Network_security.

[4].Kartalopoulos, S. V., "Differentiating Data Security and Network Security," Communications, 2008. ICC '08. IEEE International Conference on, pp.1469-1473, 19-23 May

[5].deyinka,O., "Internet Attack Methods and Internet Security Technology," Modeling&Simulation, 2008. AICMS 08. Second Asia International Conference on, vol., no., pp.77-82, 13-15 May 2.

[6].http://www.rroij.com/open-access/network-security-an-approach-towards-secure-computing-160-163.pdf