Network Security - Importance and Types

Veda. V[1]
Sujatha. R[2]
[1] UG Student, Department of Computer Science, KLE S.Nijalinagappa College, Bengaluru.
[2] UG Student, Department of Computer Science, KLE S.Nijalinagappa College, Bengaluru.

Abstract

Computer networks are essential part of our life by which we can share the information through different technologies like wired or wireless networks. Now a days wireless technologies [4] are adopted because of its advantages and secured information transmission. This article includes definition of network, network security and their working process on information security.

Keywords: Computer network, shared hardware, shared storage devices, NAC,VPN.

1. INTRODUCTION

Network is a group of interconnected computers and peripherals that is capable of sharing software and hardware resources between many users. Network Security [1-2] is a specialized field in computer networking that involves securing a computer network infrastructure. it is typically handled by network administrator or system administrator who implements the security policy, network software and hardware needed to protect a network and the resources accessed through the network from unauthorized access and also ensure that employees have adequate access to the network and resources to work.

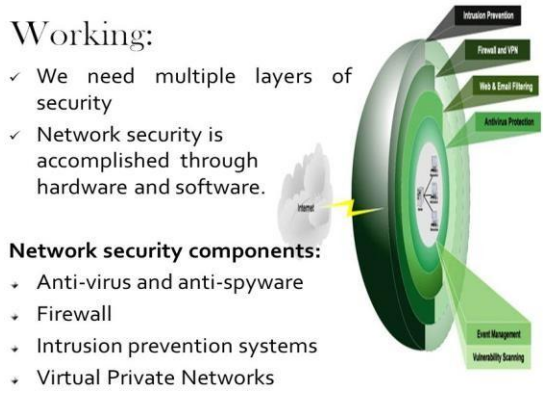
A network security system typically relies on layers of protection and consists of multiple components including networking monitoring and security software in addition to hardware and appliances. All components work together to increase the overall security of the computer network.

Network Security combines multiple layers of defenses at the edge and in the network. Each layers implement on the policies and controls. Only authorized users can access and the unauthorized users are blocked. This also helps in protecting proprietary information from attack.

Network security consists:

- Protection: We must configure the systems and networks properly to certain extent.
- Detection: Ability to identify when the configuration has changed or some network traffic indicates a problem.
- Reaction: After identification of the problem, a quick response is needed to keep the network in a safe zone.

WORKING OF NETWORK SECURITY



There are multiple layers to an effective network security system. Often first layer is authentication

means which require password to access the network resources.

Network also has intrusion detection system which alert's network administrators to breach and detect unusual activities within the network and also identify the unauthorized users.

Network firewall can enforce rules within the network to control that can or can't use certain resources.

Types

1. Access Control
2. Antivirus and Antimalware software
3. Data loss prevention
4. E mail security
5. Firewalls
6. Intrusion prevention software
7. Mobile device security
8. Network segmentation
9. Security information and event management
10. VPN
11. Web security
12. Wireless security

Brief about the Types:

1. Access control:

   In this type [3][5] all the users need not have to access to the network. In order to prevent potential hackers, we need to recognize each user and each device. Therefore security policies are enforced. This process is also called as Network Access Control (NAC)

2. Antivirus and antimalware software:

   Malicious software in short malware includes viruses, worms, Trojans, ransom ware and spyware. This can infect a network and lie dormant in it for days or even weeks. The best antimalware software's will not only scan the files but also keeps a track of it and fixes damages if any.

3. Data loss prevention:

   Organizations must make sure that their staff do not send any sensitive information outside the network. DLP technologies can stop people from uploading, forwarding or even printing critical information in an unsafe manner.

4. Email security:

   Email gateways are the number one threat vector for a security breach. Attackers use personal information and social engineering tactics to deceive recipients and send them to sites serving up malware. Email security application blocks incoming attacks and controls the outbound messages to prevent the loss of sensitive data.

5. Firewalls:

   These put up a barrier between the trusted internal and untrusted external networks such as INTERNET. They use a set of rules to allow or block traffic. A firewall can be a hardware, software or both.

6. Intrusion prevention systems:

   These scan the network traffic to actively block attacks.

7. Mobile device security:

   Cybercriminals are increasingly targeting the mobiles and applications. We need to control the devices which can access to our network and

configure their connections to keep the network traffic in private.

8. Network segmentation:

   Software defined segmentation puts the network traffic into different classifications and makes enforcing policies easier. The classifications are based on endpoint identity. We can assign rights based on role, location and more so that the access is given to right people.

9. Security information and event management:

   SIEM products put together the information that a security staff needs to identify and respond to threats. These products come in various forms like physical and virtual appliances and server software.

10. VPN(Virtual private network):

    This encrypts the connection from an endpoint to a network (often internet).A remote access VPN uses IPsec or SSL to authenticate the communication between device and network.

11. Web security:

    A web security solution will control staff's web use, block web threats and deny access to malicious websites. It will protect the web gateway on site or in the cloud.

12. Wireless security:

    These networks are not as secure as the wired networks. Installing a LAN is like putting Ethernet ports everywhere, including parking lot. To prevent this internet exploitation we need products specifically designed to protect a wireless network.

Computer networks serve a number of purposes

1. Communications such as email, instant messaging, chat rooms, etc.
2. Shared hardware such as printers and input devices.
3. Shared data and information through the use of shared storage devices.
4. Shared software, is achieved by running applications on remote computers.

Benefits of Network security

- Network security [6] facilitates protection of information that is shared between the devices on the network.
- Hacking attempts or virus attacks from the internet will not be able to harm physical computers and external attacks are prevented.
- Private networks can be provided protection from external attacks by closing them off from the internet. Network Security makes them safe from virus attacks, etc.
- Network security centrally applies and enforces consistent policies across wired, wireless and remote-access users and devices.
- Reduce operational expenses by simplifying network segmentation and defining security groups based on business roles and not IP address.
- Limit the impact of data breach through more effective segmentation and by quickly isolating the threats using the network.
- Reduce the scope of regulatory compliance by protecting sensitive information from inappropriate access.

2. ADVANTAGES OF NETWORK SECURITY

- Protect data: Network security keep a track on the unauthorized user. This help in protecting the personal data so the network security is used.
- Prevents the cyber-attack: Most of the attack on the network comes from the internet. There are expert hackers who can hack the personal information so the network security is used to protect the network.
- Levels of access: There are different levels to access the network. The network security helps to identify the authorized and unauthorized user.

3. DISADVANTAGES OF NETWORK SECURITY

- Costly set up: The set up of network security system is bit expensive. Here we are not talking about the single computer but the single computer store the massive data.
- Time consuming: The software installed in some network is difficult to work with. The authentication using two passwords that ensure the double security. If we need to edit a document we need to enter the password so, that consume lot of time.
- Requires skilled staff: to manage large network is not an easy task. It requires highly skilled technicians who can handle any security issue that arises.

4. CONCLUSION

Network security is an important field that is getting more and more attention as the internet expands. This field concentrates on protecting the data from the unauthorized users. The security technology consists of mostly software and even certain hardware devices too. Network security plays an important role in authorizing the users so that they can secure their data from the hacker or unauthorized users. An effective network security plan can be developed to manage the understanding of security issues, potential attackers, needed levels of security and the factor that makes the network to attack. In addition to protect the network systems from the other external threats or failures, the network security is used. It can be stated that, using Network Security data transmission can be the safer mode of transmission with very less possible interruption to the any particular system.

5. REFERENCES

[1] Network Security [Online] available: http://en.wikipedia.org/wiki/Network_security.
[2] ―Network Security: History, Importance, and Future‖ , University of Florida Department of Electrical and Computer Engineering, Bhavya Daya.
[3] Ateeq Ahmad, ―Type of Security Threats and its Prevention", Ateeq Ahmad, Int.J.Computer Technology & Applications, Vol 3 (2), 750-752.
[4] Dr. G. Padmavathi, Mrs. D. Shanmugapriya, ―A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks‖ , (IJCSIS) International Journal of Computer Science and Information Security,Vol. 4, No. 1 & 2, 2009.
[5] Network Security Types of attacks [Online] available: http://computernetworkingnotes.com/network-security-access-listsstandards-and-extended/types-of-attack.html.
[6] Adeyinka, 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 2008.