JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

SECURITY PRECAUTIONS FOR THE NETWORK TO PREVENT DATA AND INFORMATION

[1]Roopa P, [2]Aishwarya P, [3]Febina KS, [4]Shamimunnisabi
[1]Assistant professor, [2]Assistant professor, [3]Co-ordinator, [4]Assistant professor
[1]Computer science department,
[1]VET First Grade College, Bangalore, India

Abstract

Network security it consists of some processes and rules to manage, protect and detect unauthorized access to the system which will prevent the misuse of information, modification and denial of computer network and network resources, network security is giving an authorization control to the user to make use of computer and networking peripherals and other resources to make data communication easy and this access is normally given by network administrator, network security will be provided by giving proper authentication which is commonly by username and password this is known as one-factor authentication where his/her password will be taken into consideration, and in two-factor authentication user may also use his/her mobile number, ATM card as security token, and three-factor authentication user may use finger print, retinal scan along with username and password, once after giving proper authentication, a firewall enforces access polices to check whether what services are allowed to be accessed by the network users. A Firewall is a network security device that monitors and filters incoming and outgoing network traffic based on an organization's previously established security policies

Keywords: Data security, Firewall, VPN, Intrusion prevention, levels of security

Introduction

Anything we do to ensure the usability and integrity of a network and data is considered network security, it targets a variety of threats and prevents them from entering or spreading on our network. Effective network security manages access to the network. It includes both hardware and software technologies.

In the computer network, data can be shared and distributed quickly, which makes people's lives much easier. However, the network has a problem, it is very open, so a lot of information with viruses is also scattered around at random, posing a significant hidden threat to computer network security

At this point, threats to computer network security include more than just traditional issues like network viruses, hacker attacks, and system vulnerabilities. Big data and cloud computing are also constantly bringing about a new set of threats. As a result, computer network security technology continues to gain importance. The research topic will conduct in-depth research on the security of the computer network and propose specific security mitigation and countermeasures in order to guarantee the network's continued stability and safety.

Objective

Security is needed to protect the network from hackers and attackers. There are two fundamental guarantees in Network Security. The first is protecting data from unauthorized access and loss, also known as data security. The second is computer security, which entails safeguarding data and preventing hackers. In this context, "network security" refers to protection for any network or network of networks, not just one.

There are now two requirements for network security. There are two requirements: computer security and information security.

Levels of Network Security

There are typically three different controls for network security: administrative, technical, and physical. A brief explanation of the various kinds of network security and how each security levels works is provided here.

Physical Network Security: The purpose of physical security controls is to prevent unauthorized user from physically accessing network components like routers and cabling cabinets. Any organization needs devices that control access, such as locks, biometric authentication, and others.

Technical Network Security: Data that is either stored on the network or in transit across, into, or out of the network is protected by technical security controls. Two aspects of safety exist: Data and systems must be shielded from unauthorized access, and employees' malicious behavior must also be prevented.

Administrative Network Security: Administrative security controls are security policies and procedures that control how users behave. These controls include how users are authenticated, how much access they have, and how IT staff members put infrastructure changes into action.

Types of Network Security

The following are a few examples of network securities:

1. **Network Access Control (NAC):** Access to the network and its data should not be available to everyone at all times. Taking a look at the details of each employee is one way to investigate this. Network Access Control is used to accomplish this, requiring only a small number of authorized personnel to be able to utilize the available resources.
2. **Antivirus and Anti-malware Software:** This kind of network security makes sure that no malicious software gets into the network and could compromise data security. The management of malicious software, such as viruses, Trojan horses, and worms, is the same. This ensures that the system is well-prepared to combat the malware once it has entered the system as well as preventing its entry.
3. **Cloud Security:** Numerous businesses are collaborating with cloud technology to store a significant amount of important data online. This is extremely susceptible to the wrongdoings that a small number of unauthorized dealers might commit. This data must be safeguarded, and it should be made certain that this safeguard is unaffected by anything. When it comes to giving some of their employees access to cloud-based data, many businesses use SaaS applications. This kind of security makes sure that data can't always be seen.
4. **Firewall Protection:** As their name suggests, firewalls create a barrier between your secure internal network and unreliable external networks. Most of the time, administrators set up a set of rules that decide whether or not to let traffic onto the network. For instance, Force point's Next Generation Firewall (NGFW) provides centralized control of network traffic, regardless of whether it is in the cloud, virtual, or physical form.
5. **Virtual Private Networks:** From another endpoint or location, a virtual private network (VPN) establishes a connection to the network. Users who work from home, for instance, typically use a virtual private network (VPN) to connect to the company's network. The user would need to authenticate in order to allow communication between their device and the network because the data between the two points is encrypted. With Force point's Secure Enterprise SD-WAN, businesses can quickly set up VPNs by using drag-and-drop, and our Next Generation Firewall solution protects all locations.

Principles of Network Security and Cryptography

In today's world, any organization must put the system's security first. Any business's primary objective is to safeguard its data from outside threats. There are two kinds of attacks in cryptography: passive attacks and active attacks.

Active attacks are those that retrieve system information and alter system resources and their operations, whereas passive attacks retrieve information from the system without affecting its resources.

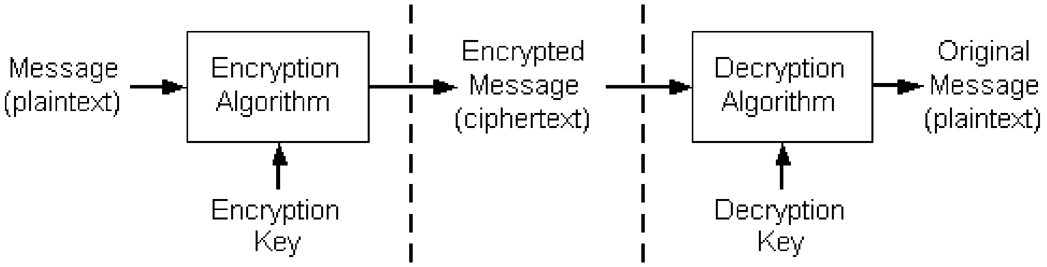

Figure 1: Encryption and Decryption of data

The following categories can be applied to the Security Principles:

Authentication: The way to identify the user, the system, or the entity is through authentication. It validates the identity of the individual attempting to access the data. Most of the time, username and password are used to secure the authentication. The authorized individual whose identity has been preregistered is able to verify their identity and access the sensitive data.

Confidentiality: The information's secrecy is determined by the level of confidentiality. The principle stipulates that the information exchanged between sender and receiver can only be accessed by the sender and receiver. If a non-authorized person is able to access a message, confidentiality is compromised.
Consider the scenario in which sender A wishes to share confidential information with receiver B but the information is intercepted by the attacker C. As a result, the confidential information is now in the possession of the attacker C.

Non-Repudiation: A technique known as non-repudiation prevents a network from rejecting the message content. Sometimes the sender sends a message and then denies it. However, the non-repudiation prevents the sender from rejecting the recipient.

Integrity: The assurance that the received information is precise and accurate is provided by integrity. It is considered to have lost its integrity if the message's content is altered after the sender has sent it but before it reaches the intended recipient.

Availability: The principle of availability states that the resources will be available to authorize party at all times. Information will not be useful if it is not available to be accessed. Systems should have sufficient availability of information to satisfy the user request.

Access control: Role and rule management determine the fundamentals of access control. Rule management limits that can access the data, while role management determines who should have access. The user who accesses the information determines how it is presented.

Issues of ethics and law: The security system uses the following categories to classify ethical quandaries.
Privacy refers to an individual's right to access personal information.
Property: It is concerned about the owner of the information.
The ability of an organization to gather data is at the heart of accessibility.

Accuracy: It is about the need to ensure the authenticity, fidelity, and accuracy of information.

There is a difference between network security and information security.

Information Security: The measures taken to prevent unauthorized use and access to information are referred to as information security. It offers availability, integrity, and confidentiality. Cyber security and

network security are included in this superset. Any company or organization that works on a large scale needs it.
The following are examples and inclusions of information security: Controls for the procedure, access, technical, and compliance

Network Security:

Any business or organization that uses both hardware and software systems to protect its computer network and data is practicing network security. The confidentiality of the data and network as well as their accessibility is the goals of this. There are a variety of cyber-threat mitigation options available to every business or organization that handles a significant amount of data.

The following are examples and inclusions of network security:

- Firewall
- Network Segmentation
- Remote Access VPN
- Email Security
- Intrusion Prevention Systems (IPS)
- Sandboxing
- Hyper scale Network Security.
- Data Loss Prevention (DLP)

Firewall: A firewall is a software- or hardware-based network security device that accepts, rejects, or drops particular incoming and outgoing traffic based on predetermined security rules. To accept: permit the traffic deny: block the traffic while responding with an "unreachable error" Drop: block traffic without responding A firewall creates a barrier between secured internal networks and untrusted external networks like the Internet.

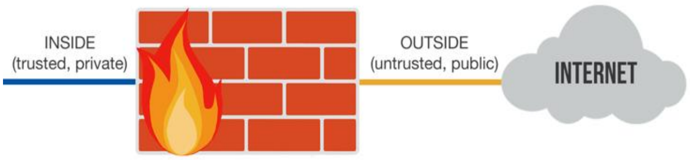

Figure 2: Firewall to protect data

Network Segmentation: When various components of a computer network, or network zones, are separated by devices like bridges, switches, and routers, this process is known as network segmentation. The discipline and framework of network segmentation can be utilized both in the data center and on-premises at your facilities.
The following are some significant advantages of network segmentation:

- Restricting access privileges to those who absolutely require them
- Preventing widespread cyber-attacks on the network
- Improving network performance by reducing the number of users in particular zones.

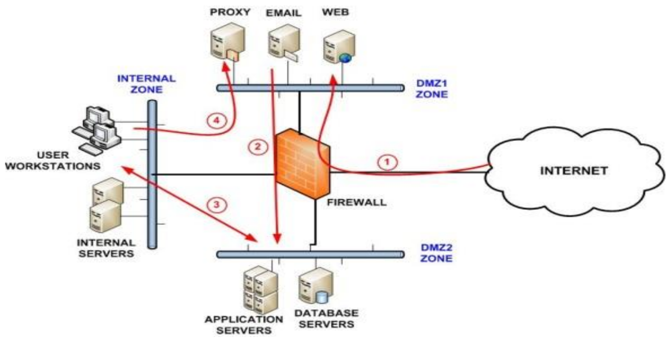

Figure 3: Network Segmentation

Remote Access VPN: Users who are working remotely can use a remote access virtual private network (VPN) to securely access and use applications and data in the corporate data center and headquarters, encrypting all traffic. The term "virtual private network" refers to a secure network that connects your enterprise edge to a remote office, mobile user, or home user via a public network. The tunnels are created by VPNs by transporting traffic over an established IP infrastructure. To move data from one end to the other, VPN technologies make use of the Internet, ATM/Frame Relay WANs, and point-to-point connected IP infrastructures.

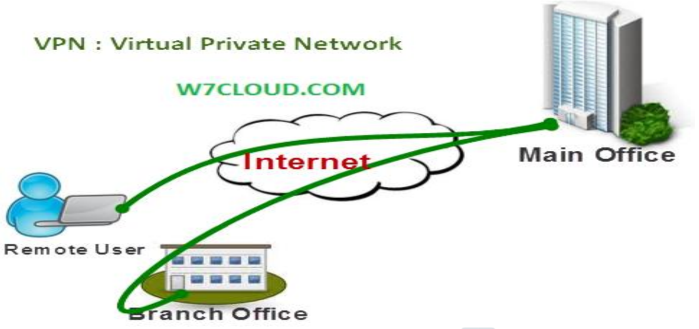

Figure 4: Virtual Private Network

Email Security: The process of preventing unauthorized access, loss, or compromise of email accounts, content, and communication is referred to as "email security." Malware, spam, and phishing attacks frequently spread via email. In order to install malware on the victim's device, attackers use deceptive messages to entice recipients to part with sensitive information, open attachments, or click on hyperlinks. Attackers frequently use email as a means of gaining access to an enterprise network and obtaining important company data, Email encryption prevents potentially sensitive information from being read by anyone other than the intended recipients by encrypting or concealing the content of email messages. Authentication is frequently included in email encryption.

Email is a common way to attack. As a result, businesses and individuals must protect their email accounts from common attacks that attempt to gain unauthorized access to the accounts or content of communications.

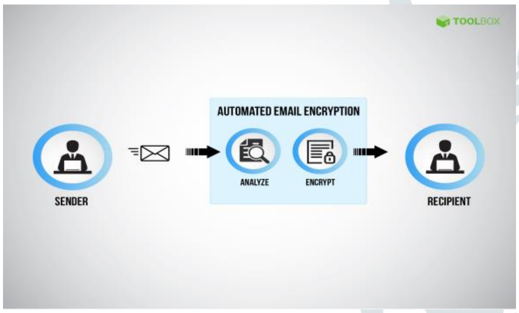

Figure 5: Email Security

Intrusion Prevention Systems: An intrusion prevention system (IPS) is a network security tool that, when malicious activity does occur on a network, takes action to prevent it, such as reporting, blocking, or dropping it. An IPS can be a software or hardware device. It is more advanced than an intrusion detection system (IDS), which only detects malicious activity but does not have the ability to take any action other than notifying an administrator. A next-generation firewall (NGFW) or unified threat management (UTM) solution may include intrusion prevention systems. They must be powerful enough to scan a lot of traffic without affecting network performance, like many network security technologies.

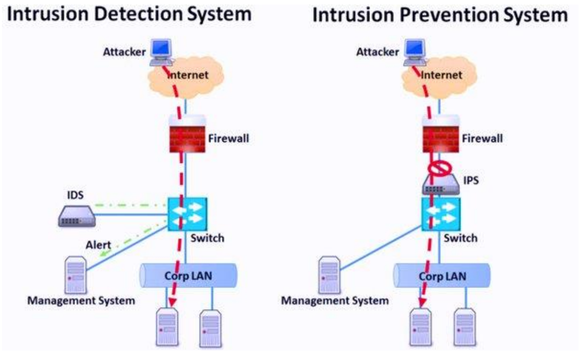

Figure 6: Intrusion Prevention System

Sandboxing: Sandboxing is a cyber-security technique in which code is run, analyzed, and coded on a system that resembles end-user working environments in a safe, enclosed environment. It is frequently utilized to scrutinize unsecure or unknown code and serves the purpose of preventing the potential threat from entering the network.

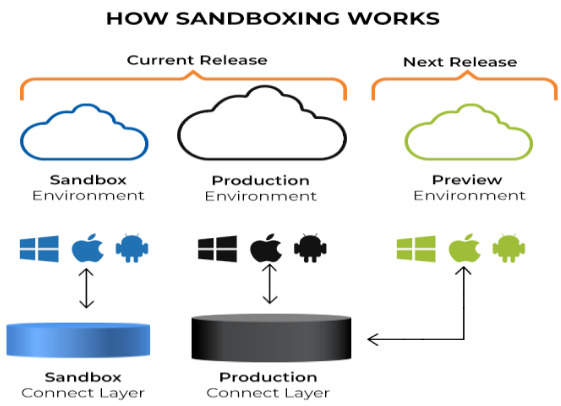

Figure 7: Sandboxing

The script is kept in a test environment when it is sandboxed, preventing it from harming the host device or operating system. This restricted test environment serves as a sort of "sandbox," as the name suggests where we can play around with various variables to see how the system works. Additionally, it is a safe environment in which any error will not directly affect a host machines.
Sandboxes are frequently used by cyber security professionals to test presumably malicious code. Applications and software may have unrestricted access to all user data and network system resources without sandboxing.

Hyper scale Network Security: Hyper-scale refers to technology architecture's capacity to adapt and grow in accordance with increasing system demand. This includes the capacity to supply and add additional system resources that comprise a larger distributed computing network. Additionally, hyper-scale is essential for building a robust and scalable distributed system. In addition, it is the consolidation of an infrastructure's virtualization, storage, and compute layers into single solution architecture.
The high-quality components that are typically found in conventional computing systems are abandoned in hyper-scale computing. Instead, it favors simplified designs that try to get the most out of the hardware. This is cheaper and allows for more money to be spent on software needs.
By connecting servers horizontally, hyper-scale computing makes it easy and quick to add or remove servers as capacity requirements change. This process is managed by a load balancer, which handles requests, monitors the amount of data that needs to be processed, and allocates resources according to available capacities. The load balancer adds additional servers as needed after constantly comparing the workload of the servers to the volumes of data that must be processed.

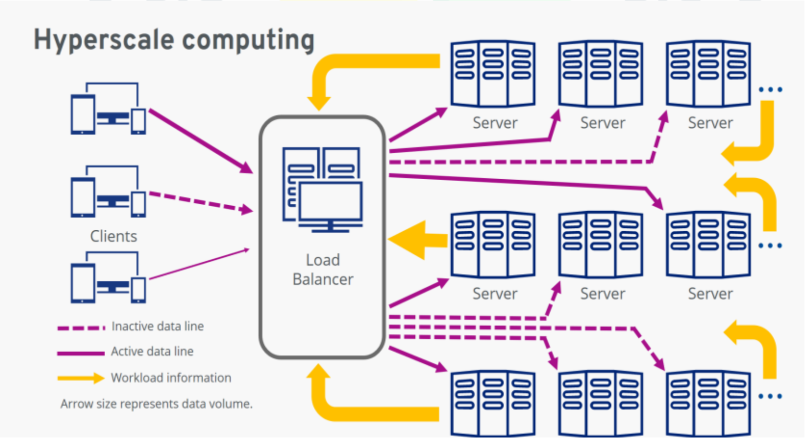

Figure 8: Hyper-scale Network Security

Data Loss Prevention (DLP): The process of identifying and preventing data breaches, exfiltration, and unwanted destruction of sensitive data is known as data loss prevention (DLP). DLP is used by businesses to adhere to regulations and safeguard their data. Protecting organizations from data loss and preventing data leakage are both referred to as DLP. A situation, in which crucial company data is lost, such as during a ransom-ware attack, is referred to as "data loss." The goal of data loss prevention is to stop the illegal transfer of data outside of an organization.

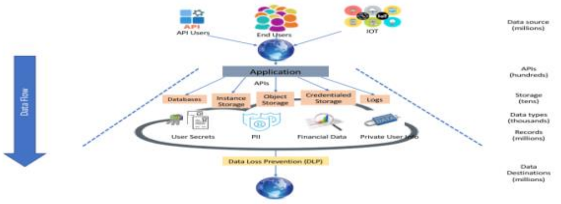

Figure 9: Data Loss Prevention

Conclusion:

Network security is therefore needed to prevent data and information which is used in day-to-day life of particular individual or an organization, to provide a network security proper methodology should be used to implement as per the requirement of the network, In all forms of network security major goal is to prevent user data and information and many inventions are methods can be seen on doing the same, as need for network is increasing we also have to adopt new technology and new methods to provide a security for the data over a network.

References:

[1]. https://en.wikipedia.org/wiki/Network_security

[2].https://www.google.com/search?q=what+is+firewall+in+computer+network&rlz=1C1CHBD_enIN946IN946&oq=what+is+firewall+&aqs=chrome.1.69i57j0i512l9.8207j0j15&sourceid=chrome&ie=UTF-8

[3]. https://www.checkpoint.com/cyber-hub/network-security/what-is-network-security/

[4].https://training.apnic.net/wp-content/uploads/sites/2/2016/12/TSEC01.pdf

[5]. https://www.forcepoint.com/cyber-edu/network-security

[6]. https://www.geeksforgeeks.org/cryptography-and-network-security-principles/

[7]. https://learn.microsoft.com/en-us/windows/win32/seccrypto/cryptography-concepts (i)

[8]. https://www.geeksforgeeks.org/difference-between-information-security-and-network-security/?ref=rp

[9]. https://www.geeksforgeeks.org/introduction-of-firewall-in-computer-network/

[10]. https://www.quora.com/What-are-computer-firewall-intrusion-detection-systems-and-intrusion-prevention-systems

[11]. https://www.comptia.org/blog/security-awareness-training-network-segmentation

[12]. https://www.kwtrain.com/blog/network-security-zones

[13]. https://www.spamtitan.com/web-filtering/network-segmentation-best-practices/

[14]. https://w7cloud.com/what-is-vpn-types-and-advantages-of-virtual-private-network/

[15]. https://www.spiceworks.com/it-security/network-security/articles/what-is-email-security/

[16]. https://www.irjet.net/archives/V5/i3/IRJET-V5I3117.pdf

[17]. https://www.fortinet.com/resources/cyberglossary/hyperscale

[18]. https://www.ionos.com/digitalguide/server/know-how/what-is-hyperscale/

[19]. https://www.imperva.com/learn/data-security/data-loss-prevention-dlp/

[20]. https://blog.shiftleft.io/why-data-loss-prevention-dlp-must-evolve-for-modern-applications-e653dc661be0