Computer Engineering and Intelligent Systems
ISSN 2222-1719 (Paper) ISSN 2222-2863 (Online)
Vol.14, No.2, 2023

Network Security Concepts, Dangers, and Defense Best Practical

Oluwasanmi Richard Arogundade
School of Business, Economics, and Technology, Campbellsville University
1 University Drive, Campbellsville, KY 42718
E-mail: oluwaaros@gmail.com

Abstract
In today's highly interconnected world, network security has become a critical aspect of protecting organizations from cyber-attacks. The increasing sophistication of attackers and their ability to exploit software and firmware vulnerabilities pose significant dangers to the security of networks. However, many organizations often neglect the essential steps required to secure their networks, leading to an increased risk of security breaches. In this research article, we aim to address this issue by investigating network security concepts, potential dangers, and practical defense strategies. We begin by exploring the different types of cyber-attacks and their sources, highlighting the various ways attackers exploit network vulnerabilities. We also examine the reasons why organizations often overlook network security and the consequences of not prioritizing it. To better understand the complexity of network security, we categorize the different security concerns using the CIA (confidentiality, integrity, and availability) triangle. This approach allows us to identify the various areas of vulnerability and their potential impact on network security. Next, we focus on the most crucial basic concepts and steps involved in various network security operations. We outline the best practices and practical approaches organizations can take to improve their network security, including implementing security policies and procedures, using encryption and authentication methods, and conducting regular security assessments. By highlighting the importance of network security and providing practical guidance on how organizations can defend against cyber-attacks, we hope to raise awareness and help prevent security breaches.
Keywords: Network, Internet, Security, Security Threats, IP Address, Network Attack, Attackers
DOI: 10.7176/CEIS/14-2-03
Publication date: March 31st 2023

1. Introduction

Undoubtedly, the internet has become an integral part of our daily lives. It has revolutionized the way we live, works, and communicate with each other. From online shopping to social media, the internet has made our lives more convenient and connected than ever before. However, with the increasing use of technology comes the threat of cyber-attacks and security breaches. As we rely more and more on technology, the risk of sensitive and confidential data being compromised also increases. The internet is undoubtedly one of the greatest innovations in human history, and its positive impact on society cannot be overstated. However, the downside of this innovation is that it has also made it easier for malicious actors to exploit vulnerabilities in computer systems and networks to steal data, cause financial harm, and disrupt business operations. Cybersecurity is therefore of utmost importance to individuals, businesses, and organizations. In today's world, where cyber threats are becoming increasingly sophisticated, it is critical to adopt excellent network security measures that can protect against potential attacks and offer access only to those who need it.

Unfortunately, detecting and preventing data risks is not always straightforward, and failing to do so can result in serious consequences, including financial losses and reputational damage. That is why network security professionals play a critical role in preventing and understanding these hazards.

To achieve effective network security, businesses and organizations must consider multiple layers of control. Protection, detection, and reaction are the three basic frameworks of network security that should underpin any networking strategy. Protection involves configuring computer systems and networks to prevent attacks, while detection involves monitoring the network to identify any suspicious activity that could indicate a potential attack. Reaction entails implementing an effective response strategy to minimize the impact of a security breach and restore the network to a safe state as quickly as possible. It is important to note that cyber threats are constantly evolving and relying on a single line of defence is inadequate. Therefore, organizations need to stay proactive and up to date with the latest security measures to protect against potential attacks.

while the internet has brought many benefits to our daily lives, it has also exposed us to significant risks. Effective network security measures are therefore essential to safeguard sensitive data and prevent cyber attacks. By adopting a comprehensive network security strategy that includes protection, detection, and reaction, businesses and organizations can minimize the risk of security breaches and protect their reputation, finances, and intellectual property.

- Protection is the first line of defence in network security. It involves configuring computer systems and networks correctly to protect against attacks. This includes securing access points, such as firewalls,

routers, and switches, using strong passwords, and regularly updating software and security patches. Protection also involves implementing security policies and procedures, such as access controls, encryption, and authentication protocols.

- Detection: is the next layer of defence in network security. It involves having good insight into the network and system, which gives you the ability to identify when your organization's network configuration has changed or when some network traffic indicates a problem. Detecting threats early can prevent attackers from causing significant damage, minimizing the impact on the network and the organization. There are many tools available to aid in the detection process, such as intrusion detection and prevention systems, log analysis, and network monitoring software.
- Reaction: this is the final layer of defence in network security. It defines your response after identifying problems and how quickly you can return to a safe state with minimum downtime. It involves having a plan in place for responding to incidents, such as isolating affected systems, containing the threat, and restoring the network to its previous state. Quick and effective reactions are critical to minimizing the impact of an attack and reducing the risk of a repeat incident.

1.1. Definitions: - What Exactly Is Network security?

In order to fully comprehend the concept of network security, it is important to first have a general understanding of security as a whole. Security is defined as the process of continuously protecting an item from illegal access, ensuring a condition or sense of safety from danger. This item can take many forms, including a person, a company, an organization, or a piece of property such as a computer system or a file (Kizza, 2017). Network security, on the other hand, is a more specific term that refers to the various procedures and preventative measures put in place to secure the underlying networking infrastructure of an organization. The main goal of network security is to monitor and prevent unauthorized access to an organization's network, resources, and assets. By doing so, the organization can safeguard against a variety of potential threats, such as cyber-attacks data breaches, and system downtime. To better understand the concept of security, it can be helpful to view it in relation to privacy. Privacy refers to the need to protect something or data from unauthorized access, while security is what guarantees that protection (Harrington, 2005).

In today's digital age, where individuals and organizations regularly engage in online activities such as browsing the web, making purchases from online stores, and uploading data via the public internet, the risk of cyber-attacks and data breaches is higher than ever. Attackers on the same network can potentially gain access to sensitive data such as personal identities, credit card numbers, account numbers, and passwords, which can lead to fraud and other malicious activities. They can also cause significant damage to an organization by taking down its infrastructure or stealing valuable assets, such as project prototypes or other intellectual property. Therefore, it is crucial for organizations to implement effective network security measures in order to prevent viruses, malware, hackers, and other intruders from accessing or modifying their sensitive data or assets. By properly securing their network infrastructure, organizations can ensure that they are adequately protected against a wide range of potential threats.

2.1. What Is an Asset in Network Security?

In the context of network security, the term "assets" refers to anything that is valuable to your organization and needs to be protected from unauthorized access, modification, or destruction. There are two types of assets in Network Security, there are tangible and intangible assets. the difference between them is that tangibles are the type of assets that your organization has that are valuable and touchable, while intangibles do not have any physical presence. meaning they are untouchable. Tangible assets are your organization's computers, servers, storage devices, routers, firewalls, backup tapes filing cabinets, etc., and intangible assets are intellectual property rights (patents), such as trade secrets, trademarks, and copyrights. Proper identification and classification of tangible and intangible assets are critical for effective network security management. It is essential to understand the value and risks associated with each asset to implement appropriate controls and protections that ensure the confidentiality, integrity, and availability of an organization's resources. For instance, if an organization's asset is a sensitive database that contains personal information, it should be protected by encryption, access controls, and other security measures that ensure the confidentiality and integrity of the data.

2.0 Types of Attacks

Attacks are categorized into passive and active attacks; active attacks are further categorized into interruption, modification, and fabrication (DOS). Modifications are further classified into replay attacks and alterations.

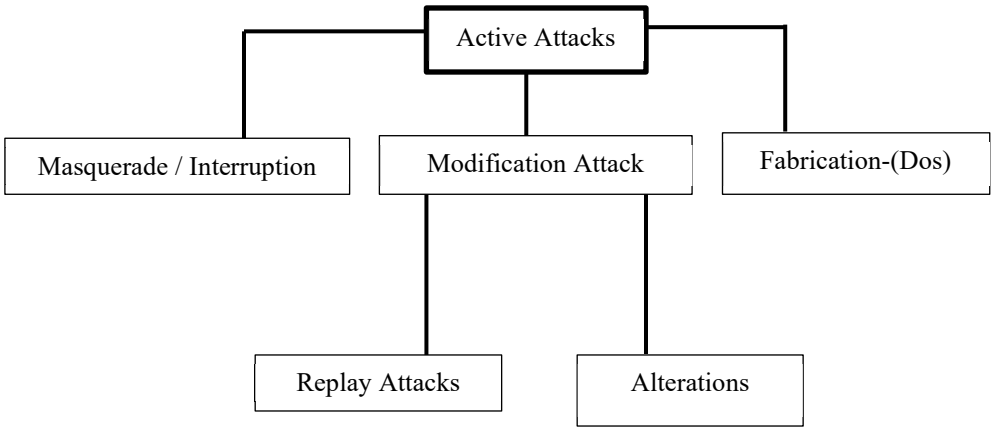

Figure 1. Categories of attack

2.1 Active Attacks

Active attacks are based on the modification of the original message in some manner, which now creates a false message. these types of attacks cannot be easily prevented; however, they can be detected. The idea of this type of attacker is to gain unauthorized access to your organization's network and compromise the integrity and availability of the system. The attacks can encrypt your data, so it becomes unusable, modify data, and they can even delete the data. Active attacks are subdivided into three types, masquerade attacks, modification attacks, and denial of service attacks.

2.1.1. Interruption or Masquerade?

When an unauthorized entity impersonates another entry, this is referred to as "masquerading." For example, let's say Adam and Mary are legitimate users of your organization, which allowed legal and authorized communication should happen between them, but then Tom comes along and masquerades or disguises himself and communicates with Mary on behalf of Adam. Due to a lack of authentication, Mary does not know whom she is talking to—not Adam—so, by chance, she releases some confidential information like a username, password, or account number. Now, Tom would get access to these credentials, and Tom can now create fake servers within the organization's network and then collect other login credentials that he will use to perform the attacks. Tom can also achieve its goal by sending phishing emails to Mary, Adam, or any other user within the network, asking them for other credentials. Because the request is coming from the same network and the same domain, it is not easy for those users to detect, and they easily comply with the demand and fall victim to phishing. Tom can also use a keylogger, which is data-stealing malware that is often disguised as a work file.

Once it is installed, it records all the user's keystrokes to obtain their usernames and passwords. Once the attacker gets those credentials, they log in to the network as a user. If those credentials are those of the network administrator, the attacker has the "golden key" and can now do all types of damage, the attacker can even take over your organization's network completely.

2.1.2. Modification Attack

Modification, as the name suggests, results in some alteration or tampering with an asset or the original message. The modification can happen in three ways: by changing existing information or inserting new information that did not previously exist. It can also happen by deletion, meaning the removal of existing information. Take a Web server, for example, if the attacker makes changes to its configuration file, it will affect the availability of that service.

Examples of modification attacks:

- Changing the contents of network communications
- Modifying data recorded in data files
- Modifying programs so that they operate differently
- Changing the configuration of system hardware or topologies of the network

Two types of modification attacks are replay and alteration attacks. A modification attack usually results in the loss of data integrity, which is a network security principle that we will discuss later in this article.

2.1.2.1. Replay Attacks

In replay attacks, a user captures a sequence of events or data and resends it. For example, let's say Adam and Mary have this business going on. It was normal for each of them to make a request for cash. Without both of them knowing it, Tom, the attacker, has been capturing the transactions. So, if Adam makes a request to Mary to transfer $200 to him, she will initiate the transaction. Unfortunately, Tom could detect the secure network communication or data transmission, intercept that transaction, and resend the message to Mary. Mary thinks it is from Adam, so she again transfers the required amount of $200. This time, however, the money was transferred to Tom, the

attacker. These attacks can come in many forms, and they are not limited to credit card usage. Let's take an example of an email conversation with the accounting department of an organization. Let's say Mary is the payroll clerk, and she emails her supervisor Adam about moving some money between accounts and asks for the credential to perform that task. Adam responds with the necessary credentials. Unfortunately, Tom, the hacker, in this case, has captured their conversation. When the hacker resends the message to Adam later, it looks like a genuine message. Tom, the hacker, has simply tricked Adam into parting with sensitive data, which now grants him access to the account.

2.1.2.2. Alterations

In the alteration, the attacker intercepts messages and alters certain information to reroute the call, which involves a change to the original message.

Using the same example, this time, when Tom intercepts the transaction, he then alters the amount to $400 before sending the request to Mary, and she will again transfer the required amount to the attacker without knowing. If the modification or change is in the case of a web server or an operating system, that will bring threats of disruption and usurpation to the system.

2.2.0. Denial-of-service attacks (DOS) and fabrication

Denial-of-service attacks It's an attempt to prevent legitimate users from accessing some services they are eligible for. For example, Mary is a legitimate and valid ABC Bank customer who wishes to access her account and withdraw funds. However, Tom is not a user of ABC Bank but a hacker who is sending invalid traffic to the bank application to disrupt the entire network of the bank either by overloading it with invalid messages or traffic to degrade the performance of the bank application, which now results in the unavailability of the service to Mary. The idea of a DoS attack is to overwhelm your organization's targeted system and stop it from responding to legitimate requests. If hackers can generate enough network traffic in the form of e-mail, Web traffic, or anything else that can consume your organization's resources, they can render the service that handles such traffic unavailable to legitimate users of the system.

- Real-life Example Scenarios
- SQL Injection
- Route Injection
- User and credential counterfeiting
- Falsification of a Log or the Audit Trail
- Email Spoofing

3.0 Passive Attacks

Passive attacks occur when an attacker or hacker gains access to a network and monitors data transmission with the intent of obtaining or stealing sensitive information; the attacker typically does not modify the data, leaving it intact.

There is no harm to the system because of these attacks; they are only interested in what the message or data is about, and these attacks are harder to detect as there is no change made to the original message or data. Passive attacks are classified into two categories: the release of message content and traffic analysis.

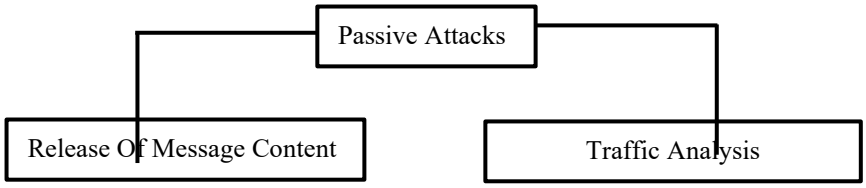

Figure 2: Passive attacks categories

3.1. Release of Message Content

This attacker happens when confidential user data are released publicly over the network. Here, the attacker is monitoring unprotected communication mediums and intercepting them. such as unencrypted data, emails, telephone calls, etc., which results in lost data confidentiality. The attacker can use a keylogger as a means of passive attack; it is often disguised as a work file. Once it is installed, it records all the user's keystrokes to obtain their usernames and passwords, which are now available to the attacker, and they can make those credentials publicly available on the internet, For example, if Mary accesses our bank account services with her credentials, while Tom intercepts those credentials and releases this confidential data to the public network, now any other person on the network can also access data.

3.2. Traffic Analysis

In this type of passive attack, the Perpetrator looks for parallels between encrypted messages and finds the original content; such activity is called traffic analysis. The attacker monitors all types of communication channels for a different range of information, such as system configuration, human identities, the locations of these identities, and encryption types. The aim of this type of attack is to examine your origination traffic pattern and learn more about your organization's vulnerability. The interesting thing about this type of attack is that the attacker is not actively trying to crack your credentials or break into your system. When a user (the sender) sends a message in encrypted form to another user (the receiver), the attacker is just waiting there, analyzing the traffic, and observing the pattern to decrypt the message. Suppose Mary accesses her bank account often, using some security algorithm to encrypt her data. Tom the hacker intercepts those data and analyzes it to discover the real details.

4.0 The most common form of Network Attacks

Network attacks are distinct from other forms of attacks in many ways, the most common form of Network Attacks are but are not limited to:

- Malware
- Phishing
- Man-in-the-Middle (MitM) Attacks
- Denial-of-Service (DOS) attacks
- SQL Injections
- Zero-day Exploit
- Password Attack
- Cross-site Scripting
- Rootkits
- Internet of Things (IoT) Attacks

4.1. Malware

The term "malware" encompasses various types of attacks, including but not limited to spyware, Trojans, viruses, ransomware, logic bombs, polymorphic viruses, and worms. Malware uses a vulnerability to breach a network when a user clicks on a "planted" dangerous link or email attachment, which is used to install malicious software inside the system, which the hacker uses to obtain information by retrieving data from the hard drive, disrupt the system, or even render it inoperable.

4.2. Phishing

Phishing attacks are extremely common and involve sending mass amounts of fraudulent emails to unsuspecting users, disguised as coming from a reliable and legitimate, source. When the user clicks on the email, it either installs malicious scripts or files or extracts data such as user information, financial information, and more.
Phishing attacks come in various forms, including spear phishing, whaling, and pharming.
Spear phishing: Attackers use Phishing as a method to directly target specific individuals or organizations.
Whaling attacks: target only the senior executives of an organization.
Pharming attacks: attackers will redirect users who attempt to access a specific website to a fake version of the website that looks identical to the original. It leverages the DNS cache to capture the end-user credentials.

4.3. Man-in-the-Middle (MitM) Attacks

This type of attack usually exploits security vulnerabilities in a network, such as unsecured public Wi-Fi, and inserts itself between a visitor's device and the network, intercepting the two-party transaction. By disrupting the transmission, attackers can steal and modify the data. It is extremely difficult to detect the type of attack since the victim of the attack believes the information is being sent to a legitimate user. Here are some examples of man-in-the-middle attacks.

4.4. Hijacking a session

An attacker hijacks a session between a trusted client and a network server. While the server believes it is conversing with the trusted client, the attacker's computer substitutes its IP address for the trustworthy client. For example, the attack may go as follows:

- A client system establishes a connection to a server.
- The attacker's computer intercepts and takes control of the client's system.
- The computer of the attacker will then disconnect the client from the server.
- The attacker's computer substitutes its own IP address for the client's and spoofs the client's sequence numbers.

- The attacker's machine maintains communication with the server, and the server believes it is still in contact with the client.

4.5. IP Spoofing

An attacker uses IP spoofing to convince a system it is dealing with a known, trusted entity, enabling the attacker access to the system. Instead of using its own IP source address, the attacker sends a packet to a target host using the IP source address of a known, trustworthy host. The target host will accept the packet and act on it.

4.6. Replay attacks

We've previously discussed replay, but let's bring it up again. The concept of replay attacks is that an attacker or unauthorized user intercepts messages or captures network traffic and transmits them again as a participant. This kind is readily defeated using session timestamps or nonces (a random number or a string that changes with time).

4.7. Denial-of-Service (DOS) attacks

The goal of DoS attacks is to achieve service denial and take a system offline, thus paving the way for another attack to enter the network or environment and launch distributed denial-of-service (DDoS) attacks. The attacker floods systems, servers, or networks with traffic to overload resources and bandwidth, rendering the system unable to process and fulfill legitimate requests. The most popular forms of denial-of-service (DOS) attacks include teardrop attacks, ping-of-death attacks, TCP syn flood attacks, botnets, and smurf attacks. For instance, an attacker could seek to take over an IRC channel by launching DoS attacks. They are so many easy-to-use DDoS tools on the internet such as Trinoo, that can be used. Those tools can be used by an individual against an organization to voice their opinions on policies they disapproved of (Marin, 2005). Occasionally businesses used DDoS tools to eliminate their rivals in the market. I have used it frequently in more in recent years for extortion (Pappalardo et al. 2005).

4.8 SQL Injections

This type of attack usually involves submitting malicious code into an unprotected website comment or search box. The attacker inserts malicious code into a server using server query language (SQL), forcing the server to deliver protected information. When attackers successfully use an SQL injection, they have access to sensitive data on your database and they can manage activities on your operating system, as well as make all kinds of modifications to your database, like inserting new data, updating existing data, and deleting data. Because of the ubiquity of older functional interfaces, SQL injection is quite popular in PHP and ASP applications. J2EE and ASP.NET applications, on the other hand, are less prone to readily exploit SQL injections because of their programmatic interfaces.

4.9. Zero-day

Zero-day attackers jump at the disclosed vulnerability in a system or network where no solution/preventative measures exist. The idea of "zero-day" is to exploit a network vulnerability before it is fixed. Our software, network, or solution will often have some security vulnerabilities.

When vulnerabilities occur, software developers and vendors will work on a "patch" to fix that vulnerability, but while this type of vulnerability is still open, the attacker takes advantage of it and launches their attack, and this is called exploit code. The phrases vulnerability, exploit, and attack are frequently used interchangeably with zero-day, and understanding the distinction is critical.

- A "zero-day vulnerability" is when software has flaws or bugs in it, and attackers discover those flaws or vulnerabilities before the vendor or developers know about them and create a patch. Because there is no patch for that vulnerability, the attacks will likely succeed and gain access.
- A "zero-day exploit" is a methodology used by the attacker to attack a network or system with a previously unknown or unidentified vulnerability.
- A "zero-day attack" occurs when an attacker uses a zero-day exploit to cause harm or steal data from a vulnerable system.

4.10 Password Attack

Password attacks occur when attackers maliciously authenticate into your network or systems. It is the most common form of cyberattack. They used different methods to bypass authentication or exploit system vulnerabilities, including dictionary attacks, password spraying, brute force, credential stuffing, etc. They impersonated a legitimate user in your organization using their credentials. Depending on the role of that user, the application, and the data they have access to, the attacker will gain entry to confidential or critical data and systems. The attacker can also use the legitimate user's identity and privileges to access another part of your organization's infrastructure.

4.11. Cross-site Scripting

An attacker inserts malicious and harmful scripts into legitimate websites' content. The malicious scripts are added to the dynamic content provided to the victim's browser. The malicious scripts or code are often composed of JavaScript code that will be executed by the victim's web browser. The attacker injects a payload containing malicious JavaScript into the database of a website. When the victim requests a page from the website, the website sends the page to the victim's browser, which now executes that malicious script as part of the HTML body. The goal of this script, in most cases, is to transfer the victim's cookie to the attacker's server, where the attacker could extract and use it to hijack the victim's session or do whatever they want with it.

4.12. Rootkits

Rootkits are typically transmitted via email attachments and unsecured website downloads. Once the attachments or files are downloaded, the rootkit will gain access to the system by installing itself on your host, which is your computer, server, etc. It can remotely change system configuration files on the server or host, Rootkits are dangerous because they are designed to hide their presence on your host or devices without you knowing.

4.13. Internet of Things (IoT) Attacks

The Internet of Things (IoT) refers to a grouping of internet-connected devices such as smart locks, light switches, cameras, smoke alarms, refrigerators, and smart speakers. IoT combines the benefits of data processing and analytics, leveraging the power of the web to make decisions for physical objects in the real world. It is a system in which intelligent objects are connected and use the internet as the basis for interconnection to gather and exchange information through "Things". (Sadhu, et al., 2022). All of them are network devices; they are online, and they are open to cybersecurity threats. We are aware that a lot of the things we use every day could be connected to the Internet, which is necessary for our survival. If it can be connected to the internet then it will be accessible via the internet. Because of the fast proliferation of IoT devices and the (often) poor attention given to embedded security in these devices and their operating systems, IoT attacks are becoming increasingly common. Your mobile and computer systems come with the same basic type of security.

However, smart TVs and wearable devices such as heartbeat trackers are prone to cyberattacks due to the lack of embedded security in these devices. The firmware of most IoT devices does not have the same level of security. In many cases, the firmware that powers up those devices is unpatched. As a result, attackers frequently regard IoT devices as easy prey.

5. CIA Triad Concept of Information Security

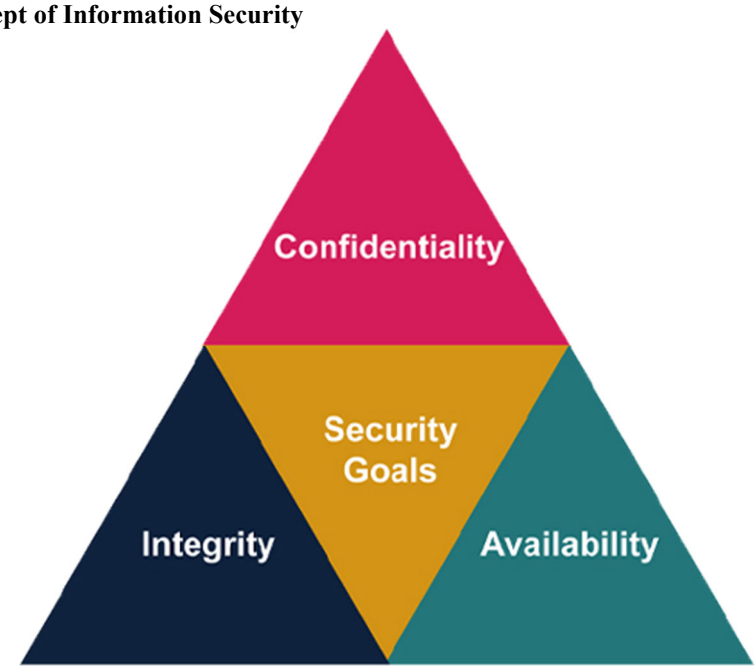

Figure 3. source: https://www.open.edu/openlearn/ocw/mod/oucontent/view.php?id=104794&section=1.1

According to statista.com ("statista.com," 2022), the average cost of a data breach for corporation organizations in the United States as of 2022 is estimated to be $9.44 million, which includes the expenses of remediation, forensic investigation, and litigation. Addressing vulnerabilities in your organization's security posture in advance and proactively can save you avoidable misery and expense.

You don't have to reinvent the wheel regarding developing a complete governance model for your business;

that is where the CIA triad comes into play, which is the basic principle of information security. Regarding network security, one of the most essential models to govern information security policy inside an organization is the CIA triad. (CIA) is the acronym for Confidentiality, Integrity, and Availability.

5.1 Confidentiality

Confidentiality is restricting information to those for whom it is intended. The term "confidentiality" refers to the capacity of only authorized individuals or systems to read sensitive or classified information. Unauthorized individuals or systems should not have access to network data. The essential strategy to avoid this is to use a VPN tunnel (Virtual Private Network) to enable data transfer securely across the network, as well as encryption standards such as AES (Advanced Encryption Standard) and DES (Data Encryption Standard) to safeguard your data. such that even if the attacker gets access to your data, they will not be able to decrypt it.

5.2. Integrity

Integrity is ensuring that transmissions and messages aren't corrupted or altered in purpose. Integrity refers to protecting data from any form of modification by unauthorized users; it is the reliability of data throughout its lifecycle while preserving both the external and internal consistency of the data. To maintain a state of data integrity or accuracy, encryption methods can be used to achieve this. The mechanism of the encryption system should be able to deter or indicate that the message has been corrupted or altered. Imagine the big problem it will cause if someone's drug prescriptions or medical records are altered.

5.3. *Availability:*

Availability ensures information and services are accessible when needed. This implies that network users should have easy access to the network when they need it. This is true for both systems and data; they need to be accessible when it is required. To guarantee network and data availability, network and system administrators should maintain regular updates for their hardware and software, and they should also have backup plans and fail-over strategies for their organization's infrastructure, just in case of failure or DDoS attacks that take down the company's infrastructure and resources. They can easily failover to other infrastructure, which will reduce the impact of such a failure or attack.

Generally, all data that you wish to keep secure needs to remain confidential, maintain the integrity and be available. confidentiality means simply keeping that a secret, meaning keeping it secret from those who are not authorized to view it. Integrity refers to preventing unauthorized parties from changing the data or by accident, and Availability means that information is available when you need it.

6.0. Procedures To Secure and Improve Network Security of Our Organizations

6.1. Physical Security Implementation

Security may seem like common sense, but it is often overlooked. All other security procedures for your network are useless if any unauthorized person gains access to your infrastructure.

Physical security should be made a part of your security policy. You should define restricted areas and non-restricted areas, and your data centre or server room should be a restricted area, anywhere your network devices or equipment, such as routers, network cards, patch panels, cables, hubs, bridges, switches, modems, and firewalls, etc. should be in a secure restricted area. All backup media and any other data-related devices should be stored in a secure, restricted area. You also want to consider human security guards at the doorway to the data centre, various kinds of locks, biometric key cards, cameras, etc. All visitors or colocation partners should be supervised even when in non-restricted areas, defining who is allowed into restricted areas by following the principle of least privilege, that is, only employees with legitimate business reasons should have access to restricted areas, the same applies to visitors or colocation partners they should only have access to their cage, which just a space where they have their equipment.

You should eliminate unauthorized network equipment, also known as "rogue equipment." it is also possible that a hacker installed those rogue equipment in your network with the aim of stealing or doing harm, but most unauthorized network equipment you will find in most organizations is from the end-users, who install a device for their convenience. Maybe it is for personal lab testing or training, and they do not realize that they could be creating a backdoor into the network. You should also disable open Ethernet jacks that are accessible to end users, as most rogue equipment requires being plugged into an Ethernet jack. Most technically advanced users, such as IT managers, pose a bigger problem regarding rogue equipment, claiming to know what they are doing when they install those devices on the network. And that is why the AUP is critical; it clearly addresses what is allowed and what is not allowed to be installed on the network or system. From the end-user perspective, you want to lock down some features on their machines like disabling the physical USB ports on their laptops or workstations.

This can help reduce many exploits that use thumb drives, such as an employee stealing confidential files or a visitor plugging in a thumb drive with malware on it to any computer and creating an attack. You also want to

configure your servers and end-user workstations with a timed auto-logout so that no one can sit down at someone else's workstation or laptop if that user forgets to log out.

6.2. Perimeter Security

Trusted and untrusted zones make the perimeter security concept. Zero trust is a notion that was initially developed by Forrester's research, and it is used by businesses to protect extremely sensitive data from online threats. To combat lateral threat movement within a network, zero trust architecture uses micro-segmentation and granular border enforcement depending on data, user, and location. The phrase "never trust, always verify" is another name for this. (Anita, 2021). The trusted zone includes every device on your network, including your router and switches. Everything outside your network, like the Internet, falls under an "untrusted zone." The single point at the perimeter where data packets can pass in and out of your network is the firewall. The role of the firewall is to stand at the border and precisely control what is permitted in and what is allowed out.

This two-zone architecture is generally adequate for small or home-based businesses, but if the businesses plan to offer or will provide servers to the public, they will create a DMZ zone and host these services in it. A firewall should be placed in front of the communication or traffic from the DMZ to the trusted zone. since the servers that host those services may be vulnerable to malicious hackers. When a packet from the untrusted network to the trusted network arrives, the first device it hits is the router at your perimeter. Securing the router is most often done using access control lists, or ACLs. You can enforce and filter traffic based on the destination IP address or destination port and the source IP address or source port. You can decide the source and destination IP addresses that are allowed to pass through the router, as well as which source and destination ports are allowed to pass through the router. You also want to ensure you properly secure the access control lists with strong passwords. Depending on the type and maker of your router, you should have lockdown and security audit features on your router. You want to use those features.

The next thing is the firewall. A firewall is a much more granular and powerful device for controlling traffic in and out of a router. Many firewalls include security features such as VPN capabilities; content filtering, which allows you to block end-users on your network from accessing certain websites; gateway antivirus; intrusion prevention; anti-spyware; logging; alerts. First-generation firewall packet filtering occurs at layers 1–2 and 3 of the OSI reference model, and the second-generation firewall is stateful packet filtering that occurs at layers 1–2 and 3–4 of the OSI reference model, layer 4 of which in the transport layer allows the use of connections As stated, the firewall will record all connections passing through it; it also determines if any packet is part of an existing connection at the start of a new connection or was not part of any connection at all. The third-generation type of firewall works at the application layer of the OSI model; filtering occurs at layers 1–2, 3–4, and 7. Layer 7 allows the functionality of deep packet inspection, which allows filtering by specific criteria for specific applications such as HTTP, HTTPS, FTP, and DNS.

Data and resources for the corporation were generally restricted to its physical boundaries, and the fundamental tenet of the perimeter security concept is that external networks are always the source of cyberattacks. The network's perimeter was secured as a result of this assumption. The foundation of perimeter security was made up of security tools and software techniques including firewalls, load balancers, VPNs, and DMZ, among others, and this was effective in defending against zero-day, phishing, denial-of-service, and malware attacks. (Anita, 2021).

6.3. Good Information Security Policies

The phrase security policy is defined as the collection of policies, laws, regulations, and procedures that govern how an organization manages, secures, and disseminates information (Nieles et al., 2017, p. 26). Every company relies on data, such valuable information can make or break a business. A good security policy should address the most likely network risks as well as the best approaches to mitigate them. Most organizations used a risk assessment or risk analysis to determine how likely specific threats were to occur. The idea of risk assessment is to give priority to the most dangerous and costly risks, should a particular risk materialize. It also depends on the laws and regulations of your company. Most corporations are subject to one or more regulations. Like medical companies are subject to the HIPAA Act (Health Insurance Portability and Accountability Act), credit card companies are subject to the PCI-SSD (Payment Card Industry Data Security Standard). Any organization processing the personal data of EU residents is subject to the EU GDPR (General Data Protection Regulation), and organizations processing information on California residents or doing business in California are subject to the CCPA (California Consumer Privacy Act), just to name a few. Risk analysis is a point-in-time snapshot of your configuration and the baseline of your company's infrastructure and applications. And from that point forward, the company is aware of some vulnerabilities that they have; those are some risks that they need to be mindful of. Once they have seen what types of risks and vulnerabilities they have, they can start using either quantitative or qualitative measurements to help us make those decisions.

Quantitative measurements are very easy because we can assign a dollar amount to them and that has a

judgment call. Like, how much money is this going to cost us if a server goes down because of an attack? How much money are we going to lose? Obviously, the more money you are at risk of losing, the more effort you want to put into catching, solving, or reducing that vulnerability or risk. If an organization's risk assessment report shows a small or low-level risk that is unlikely to materialize or occur, your organization may choose to ignore it and concentrate on situations with greater risk. But do not forget the laws and regulations that your organization is subjected to. When an organization's risk assessment report shows that a particular risk has an estimated cost per year of $20,000 and occurs maybe twice a year, and another particular risk costs $80,000 per year, depending on how many times it occurs, a higher priority will be placed on the second risk. Qualitative measurements are a little bit harder to judge because they're subjective. For example, a system may be critical to your back end, but it doesn't produce any income. Maybe it manages all your internal accounts, like a directory server. If that server goes down, what will happen? Well, employees can't access their accounts for some time. How much is your company actually losing in profit, and how much are they actually losing in revenue-generating income with a delay in work? Because we can't put a dollar sign on it, it's a little bit harder to judge.

A security policy should be written at a high level and be accessible to all staff members of your organization. It should be comprehensive rather than technology specific. This ensures that the security policy will rarely require updating, but based on the technology-specific security policy, procedures can be written, so it's assumed that as time goes on, procedures will need to be rewritten but the security policy should not. Your acceptable use policy (AUP) should be included in your policy. This policy indicates to end-users what they are allowed to do on the network or servers and what they're not allowed to do. Maybe they are not allowed to use company email for personal purposes, or maybe they are not allowed to install third-party software. In your security policy, ensure you clearly define the roles and responsibilities of IT staff, end-users, and services. like who should be in charge of maintaining the network infrastructure, database backups, renewing software licenses, overseeing data storage, compliance, and other legal documents.

What should the person in charge of backup specifically be doing daily to ensure that the backup is done properly, or what should the person in charge of the service-level agreement (SLA) be doing to ensure the company is not paying unnecessary penalties? The security policy is easy to implement in the cloud, but my focus for this article is on a physical data centre situation.

It is also crucial that you do a regular review and evaluation of your policy and procedure. your environment will continue to change, as well as the compliance standards. I recommend that your company initiate a review quarterly or annually. Usually, every new employee of an organization must sign the acceptable use policy when they're being hired to indicate that they understand it and will abide by it.

6.4. Account, Permissions, and Control Management

Enforcing password policies is relatively easy, as this functionality is built into most operating systems; anyone who has worked as a Windows administrator will have at some point used this feature. End-users will often do the most convenient thing rather than the most secure thing, so it's much easier for them to just choose a simple dictionary word, use their date of birth, or something else that they will never have to change. You should also educate the end-user about why it is not a good idea to share passwords or write a password on a sticky note behind a laptop or monitor; all this should be included in the company's security policy. best-practice requirement for a good and secure password.

- The minimum password length should be eight (8) characters; the password must contain upper- and lower-case characters, at least one non-alphanumeric character, and at least one number.
- You can also make it more complex by making the password 10 or 15 characters long. because a longer password is harder to decrypt if stolen.
- The password must be changed at least once every 90 days, and no previous passwords may be used after the password has been changed.
- The default account password for the end user must be changed or removed before the user is allowed to use the account.
- Check passwords created by the end-user against a "blacklist," which includes dictionary words, repetitive words or numbers, sequential strings, commonly used phrases, patterns, or other words that attackers are likely to guess.

In addition to the above, you want to add multifactor authentication (MFA) as another layer for verifying identity. The idea is that users must provide a combination of authenticators' codes to verify their identity before they can access their accounts or servers on your network or systems.

We must ensure that we are following the correct policy for passwords. Permissions allow an end-user to do something on a system or network. When we are giving permission, we must follow the principle of least privilege, which means a user of a system, or a network should only be able to access the necessary information required to perform their job and nothing more. This means the users or systems should be assigned only the necessary permissions to perform a legitimate role or task. If a user or service does not need access to a server or its services,

then that user or service should not have such a right. This also helps limit the possible damage an unauthorized user can cause by gaining access to a system or its resources. Access control may be at the application level or at the level of the operating system. This helps us have granular control over what a particular application, system, or account is allowed to do. For easy administration of users and accounts, you want to assign permissions to groups of accounts or users rather than to individual accounts or users. You do this by creating groups of users or services with similar roles or job functions and then assigning specific permissions to the group. And whatever permissions these groups have, that is what each of those users can do.

One other area of security that most start-up organizations overlook is remote access permissions. The network and system administrator can access a router, switch, system, or device through a console when they are physically present at the data centre or server room, but when they are not present at the data centre and they need to access servers, they will need remote access, which is only available by using an IP address. If proper security measures are not in place, an unauthorized user or attacker can capture sensitive information and access our devices.

To ensure this is not the case, we need a framework called Triple (AAA), to provide an extra level of security for devices. Triple (AAA) is the acronym for authentication, authorization, and accountability. Authentication means that a user is who they say they are; it is the way to identify the user before they can access the company's network resources. This can be done using the local database of that device (router) or via an external server like the ACS server.

For example, if an end-user with the name Mary logs in to a system or server as Mary and provides a password that belongs to Mary, the system will authenticate her, but if she provides the wrong password, the system will not. Authorization refers to the actions that the user can perform once they have been authenticated. It is used to determine what resources the end-user is allowed to access and the type of operations they can perform on those resources. Accountability means monitoring and capturing end-user activities on your company's network or systems. It is a way of holding users accountable for their actions on the system or network. capturing actions performed by users while accessing the network, server, or services. We can even monitor how long the user has had access to the network or system by using logs and auditing.

Many organizations will allow users to have the same permissions no matter where they are physically located. and this is not a secure practice; permission should be restricted based on location, sources, etc. Use a VPN if you intend to let end-users access information or data on your network from a remote location; a VPN provides secure communication over the public network. The way to understand VPN is by using an analogy. Two friends, Tom, and Mary are traveling by car to a coffee shop; Mary is using a bulletproof car with a body guide, and Tom on the other end is just driving a normal car without any bulletproof. The road to the coffee shop in this analogy is the public internet, and the bulletproof car is the VPN. Tom and Mary represent the data that goes back and forth between your network and the public network.

This data will be encrypted using a VPN. We will discuss more on the concepts of VPNs when we start talking about securing data in transit.

6.5. End-Users should Be Updated and Educated on Security Policies

Organizations commonly rely on technology security solutions when they are faced with hazards to their information security. The risks to security cannot be reduced exclusively by technical means. Information security success may be accomplished when firms invest in both technological and socio-organizational resources (Bulgurcu et al., 2010). Current statistics of the 2022 Data Breach Investigations Report as reported by Verizon.com (verizon.com, 2022) show that up to 34% of breaches are caused by human error. No matter how good the technology your organization uses to secure its network, actions performed by both end-users and IT staff can result in security breaches. Most confidential files compromised by hackers from outside your organization are mostly accidental errors caused by your end users. and this is because most users are simply not aware that their actions may pose security threats to the organization. The way to reduce these problems is to educate them and get them to start thinking about security threats. They should be educated on the acceptable use policy, and any procedures applicable to their specific job role. This education should come in the form of yearly or quarterly training. Every new employee should be required to complete basic security training while onboarding.

All employees should be required to complete a refresher security training regularly, this can be yearly or quarterly training. There should be a form of FAQ for security policies and procedures, and it should be available for all employees to be able to refer to at any time. This allows them to easily clarify questions that may arise during their day-to-day routine. You may also want to publish a security article on current threats and most recent breaches, and the causes and how they could have been avoided. You can also invest in security awareness programs to help educate and build strong security culture habits for both technical and non-technical users. Training programs provide the information, but education offers a more thorough understanding that builds better habits.

Any server or service that wants to communicate with another server or service does so via an open port. For example, for clients to be able to connect to a public web server, that server needs to be listening to HTTP or

HTTPS, and port 80 or 443 needs to be opened. For you to access a Linux server via SSH, port 22 needs to be opened. If the server or service is not listening to a specific port when a remote client tries to connect to it, the connection will fail. The principle of least privilege applies here; you only open ports for necessary services.
You also want to remove any servers and disable any services that are not in use from your network. meaning you should completely unplug those servers or devices. Port numbers are used to distinguish between different services that run over transport protocols such as TCP and UDP. Here are some common and well-known ports:

Table 1. Table of Common Network Protocols, Port Numbers, and Functions

Protocol	Port Number	Function
HTTPS	443	Secure version of HTTP for secure web browsing and data transfer
HTTP	80	Protocol for web browsing and data transfer
SMTP	25	Simple Mail Transfer Protocol for sending email messages
POP3	110	Post Office Protocol for retrieving email messages from a server
FTP	20 and 21	File Transfer Protocol for transferring files between computers
SSH	22	Secure Shell protocol for secure remote access to servers
NetBIOS	137, 138, 139	Networking protocol for communication between devices in a LAN
Telnet	23	Protocol for remote access to devices like servers, routers, and switches
DNS	53	Domain Name System for translating domain names into IP addresses
TFTP	69	Trivial File Transfer Protocol for simple file transfer over a network

6.6. Implement good patch management.

Any flaw or weakness in the network or system is considered a vulnerability. This could be an application or operating system vulnerability. When vulnerabilities are discovered, the vendors or the OEM of such devices or services create and publish a patch to fix the vulnerability. You want to ensure that all applicable patches are applied to your network as quickly as possible, that is what makes for good patch management.
Follow the basic procedures for good patch management.

- Step 1 identifies patches made available by vendors.
- Step 2 Identify the hosts on your network that need these patches.
- Step 3 downloads the patches.
- Step 4: Test the patches on a system on your network, like in a lab environment that looks like the node or server you are trying to patch. It is critical that you test the patches before introducing them into your network or production environment.
- Step 5. Deploy patches that are tested acceptable in the lab or test environment to all hosts on your network that need them. You have the option of using the configuration management system to do patch management as well.

6.7. Implement anti-virus measures

There are several IT security measures that can help the battle against cyber terrorism if they are properly implemented and managed. This comprises access control lists, firewalls, and anti-virus software that are installed, operational, and regularly updated. The most effective way to protect against malware is to install anti-virus software, which scans the computer to identify and remove the malware and provides automatic updates to enhance security (Jayasekara et al., 2022). For small businesses or companies, it is relatively easy: you simply install antivirus software on your PCs or servers to protect against malware such as viruses, worms, and Trojans. To protect all systems from malware, you should enable gateway antivirus on your firewall to eliminate the malware before it ever hits your hosts or servers.

When there is new malware, the antivirus vendors push new antivirus signatures to defend against a specific piece of malware. Most of this antivirus software upgrades its signatures automatically, but you will still have to check them regularly because those updates may fail for one reason or another. But for enterprise organizations, where you deal with a couple of thousand workstations, you ensure that all workstations have an anti-virus installed on them and that they have the latest signatures. You should have a centralized way of managing the systems. You probably want to use centralized antivirus management software. Centralized antivirus management software allows you to see every workstation on your network. You can see if each workstation has anti-virus software

installed and the latest signatures. You can schedule signature updates to occur outside business hours. You have the option of manually updating the signature or configuring the antivirus protection based on minimum criteria; if the workstation does not meet the minimum criteria, that workstation is quarantined from the network until it is upgraded to meet the minimum criteria.

6.8. Secure Data in Transit

When data are transferred across an insecure medium, you run the risk of the data being sniffed or captured by an attacker. The attacker could use a program like Paessler PRTG, Windpump, Wireshark, TCP-dump, or ManageEngine NetFlow Analyzer, just to name a few, but there are so many of these utilities to capture that data. This brings us to the concept of cryptography, which refers specifically to the practice and study of techniques for secure communication in the presence of third parties, known as adversaries.

The English word "cryptography" has its roots in the Greek words "kryptos," which means "hidden," and "grafein," which means "to write.". Cryptography is same time refer to as cryptology, which more general term that encompasses cryptography as well as other areas of study such as cryptanalysis (the study of techniques for breaking cryptographic systems) and steganography (the practice of hiding information in plain sight). In cryptography, we deal with plaintext, which is data that can be easily read by anybody. We encrypt the data into ciphertext, which makes it difficult to read by others, and we can also decrypt the ciphertext to get back the original clear text. cryptography allows us to achieve security goals such as confidentiality, integrity, authentication, and non-repudiation. Confidentiality means keeping the information secret; integrity means ensuring that the data has not been altered in transit; authentication means approving identity; and non-repudiation means a party cannot deny that they sent a specific message. Supposing you sign a contract with a vendor, your signature on that document or contract is non-repudiation; you cannot change or later disagree with the terms of the contract. Non-repudiation means that it can be proven that they actually did sign the contract. We've previously discussed VPNs and will now go through them in a little more detail. VPNs are of two types: site-to-site and client-based VPNs. To encrypt their data and safeguard it during transit, organizations might utilize a VPN or TLS/SSL. (Achar, 2022).

A site-to-site VPN allows communication securely over the public Internet. Suppose a company has two offices, one in Dallas and the other in Los Angeles. A security appliance is configured at each end of the office network, and all data going between the offices must pass through the security appliance before it reaches the internet.

Therefore, any user communicating with the other offices will have his data automatically encrypted. Client-based VPN is a piece of software installed on the end-user PC that allows the remote user to establish a VPN from his laptop to the security appliance on their office network. The VPN allows all data between the laptop and the remote network to be tunnelled and therefore encrypted. With the VPN, it really does not matter if the local connection is secure or not because, even if they have direct physical access to the server, hard disk, or data, data encryption makes it impossible for unauthorized individuals to access data (Achar, 2022). Even if an attacker sniffed the data, they would not be able to decipher the encrypted data and they would not be able to read it.

6.9. Back up your data.

Data backup involves replicating data in order to recover the duplicate set in the case of a data loss incident. Backups have two distinct functions. Data recovery after deletion or destruction is the main objective. The restoration of data from a prior period is the backup's secondary objective. This is done in line with the data retention policy, which is often defined in the long-term and how many copies of the data are required to backup. (Beňo, 2022). If you have ever experienced losing something critical due to hardware failure or application failure, or if you have a backup, but when you try to restore from that backup, it fails, it only takes one big loss to change your perspective about backup and restore, especially if the data lost is not yours but someone else's, like your company's data. What you need is a solution that backs itself up automatically. Many options are available, regarding backup strategies, but, in each case, the question you must ask yourself is: if a disaster happens now and a specific piece of data is lost, will I be able to restore it quickly from that backup? If the answer is no, you should not use such a strategy because it will keep you up at night. You also want to consider how often you are backing up and how secure the items are. In a major event like a hurricane or tornado, which is completely unpredictable and takes down your infrastructure, how quickly can you restore data from this backup solution? You want to ensure sure you choose a solution that backs up automatically without you having to remember to do it and lets you know if the backup is not running properly or when it failed. Numerous backup options are available out there to choose from; which one to use will depend on your organization's needs. You should also ensure that all backups tapes or media should not be on the same location with servers or data centers, those media need to be stored off-site location regularly, you can even store them in could such as AWS, Azure, or Google cloud and you restore your data back when it is needed. Backup Exec by Symantec is the oldest backup system I have used.

7.0 Conclusion

At this point, I want to remind you that there is nothing like total security, so continuous monitoring of your network is crucial and the key to staying secure. Ensure you apply the concept of "security defense in depth," having multiple layers of security for your infrastructure. The main idea here is that different security tools should be applied at each layer of your infrastructure. and every component of your security plan should have backups to combat failures and breaches. If one layer of security fails, the other layer of security will protect your infrastructure and resources. For example, if an intruder succeeds in breaking into the data centre, they will still need to determine the username and password of the server, and if the login also has 2-way authentication, then the intruder will have to break that as well. And if the data is also encrypted at rest, they must also break that encryption to access our data. Cyber-attacks are increasing on daily basis, so you want to ensure you are applying security patches when they are due and anti-virus signatures are up to date, train your employees about security, and ensure your organization is up to date with compliances. Configure your network firewall to allow only the required ports and hosts; use secure and strong passwords, and do not forget to use the principle of the least-privilege model in your IT infrastructure. perform frequent backups and a continual audit of your IT environment.

References

Achar, S. (2022). Cloud Computing Security for Multi-Cloud Service Providers: Controls and Techniques in our Modern Threat Landscape. CERN European Organization for Nuclear Research - Zenodo. https://doi.org/10.5281/zenodo.7084251

Average cost per data breach in the United States 2006-2022. (2022, Sep 4). statista.com. Retrieved from https://www.statista.com/statistics/273575/us-average-cost-incurred-by-a-data-breach/

Academic Lesson (2019, Aug 2). Cybersecurity for beginners | Network Security Practical Course. Retrieved from https://www.youtube.com/watch?v=qvDg17PbSnUu?.

Beňo, P. (2022). REMLABNET – BaaS, Backup as a Service in Remote Laboratories and Increase Sciences and Research's Data Security Precautions against Ransomware. International Scientific Days 2022: Efficient Sustainable and Resilient Agriculture and Food Systems – the Interface of Science Politics and Practice. Proceedings of Reviewed Articles of International Scientific Conference. https://doi.org/10.15414/isd2022.s5-2.02

Bulgurcu, B., Cavusoglu, H., Benbasat, I. (2010). Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. MIS Quarterly, 34(3), 523-548.

Choudary .A.(2022, Nov 15). What is Network Security: An introduction to Network Security. Retrieved from edureka.co. https://www.edureka.co/blog/what-is-network-security/

CIA Triad and New Emerging Technologies: Big Data and IoT. (2015, Oct 13). informationsecuritybuzz.com. Retrieved from https://informationsecuritybuzz.com/isbuzz-expert-panel/cia-triad-and-new-emerging-technologies-big-data-and-iot/

Harrington, J. L. (2005). Network Security: A Practical Approach (The Morgan Kaufmann Series in Networking). Morgan Kaufmann.

Kizza, J. M. (2017). Guide to Computer Network Security. Springer.

Madushan Jayasekara, Chamoth,(2022). Network Security: Case Study Analysis Available at SSRN: https://ssrn.com/abstract=4217769 or http://dx.doi.org/10.2139/ssrn.4217769

Marin, G. (2005). Network Security Basics. IEEE Security and Privacy Magazine, 3(6), 68–72. https://doi.org/10.1109/msp.2005.153

Nair, Anita (2021): The Why and How of adopting Zero Trust Model in Organizations. TechRxiv. Preprint. https://doi.org/10.36227/techrxiv.14184671.v1

Nieles, M., Dempsey, K., Pillitteri, V. (2017). An Introduction to Information Security. NIST Special Publication 800-12 Revision 1. Retrieved May 12, 2020 from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-12r1.pdf

Pappalardo, D., & Messmer, E. (2005). Extortion via DDoS on the rise. Network World.

Raimundo, R. J., & Rosário, A. T. (2022). Cybersecurity in the Internet of Things in Industrial Management. Applied Sciences, 12(3), 1598. https://doi.org/10.3390/app12031598

Sadhu, P. K., Yanambaka, V. P., & Abdelgawad, A. (2022). Internet of Things: Security and Solutions Survey. Sensors, 22(19), 7433. https://doi.org/10.3390/s22197433

Talking security: the basics. (1999-2022.). Open Learn. Retrieved from https://www.open.edu/openlearn/ocw/mod/oucontent/view.php?id=104794&section=1.1

What are Web Application Vulnerabilities? (n.d.). rapid7.com. Retrieved from https://www.rapid7.com/fundamentals/web-application-vulnerabilities

What is a Cyber Attack? (2021) secureterminus.com. Retrieved from https://secureterminus.com/cyber-attacks.