World Journal of Advanced Research and Reviews
eISSN: 2581-9615 CODEN (USA): WJARAI
Cross Ref DOI: 10.30574/wjarr
Journal homepage: https://wjarr.com/

(REVIEW ARTICLE)

Check for updates

Securing network infrastructure with cyber security

Muhammad Jamshid Khan *

Master of Computer Science from Virtual University of Pakistan (2015), Member of the ECE "EC-Council" (2021)

World Journal of Advanced Research and Reviews, 2023, 17(02), 803–813

Publication history: Received on 05 January 2023; revised on 16 February 2023; accepted on 23 February 2023

Article DOI: https://doi.org/10.30574/wjarr.2023.17.2.0308

Abstract

In today's digital age, securing network infrastructure has become a critical concern for organizations of all sizes. With the increasing number of cyber threats, it is essential to implement effective measures to protect sensitive information and prevent unauthorized access to network infrastructure. This article explores the various methods that organizations can use to secure their network infrastructure and maintain the integrity of their sensitive information. This article provides valuable insights into the various methods that organizations can use to secure their network infrastructure and protect their sensitive information against cyber threats. By implementing these methods, organizations can reduce the risk of data breaches, protect their reputation, and ensure the ongoing security of their network infrastructure.

Keywords: Cybersecurity; Cyber-attacks; Infrastructure; Security; Threats; Exploiting; Social engineering; Hacking; VPN; Encryption; Breaches; Phishing Attacks; MiTM; Antivirus; PAM; AIM; Reconnaissance; Exploitation;

1. Introduction

The utilization of digital technology has transformed the manner in which organizations conduct their operations and store important information. However, this greater dependence on digital systems has also elevated the risk of cyber-attacks and unauthorized access to network infrastructure. To preserve the confidentiality and reliability of sensitive information, securing network infrastructure has become a crucial concern for organizations of all sizes. Cyber threats can originate from various sources such as hacking, malware, phishing, and social engineering. These attacks can result in serious harm to organizations, including data theft or breaches, system damage or interruption, spread of malware, and harm to reputation.

This article provides an in-depth examination of the strategies and technologies used to secure network systems and fend off cyber-attacks. The article will analyse the functions of firewalls, encryption, VPNs, IDPSs, regular software updates, employee training and awareness, as well as IAM and PAM can make strong the security of infrastructure. The article also emphasizes the importance of implementing a comprehensive cybersecurity strategy to maintain the ongoing protection of sensitive information and systems. The objective of this article is to furnish valuable insights into the methods and technologies used to secure network infrastructure and defend against cyber threats. By comprehending the significance of these measures, organizations can enhance the protection of their sensitive information and systems and reduce the risk of security incidents and data breaches.

2. Methodology

The methodology used in this article is a literature review. A comprehensive review of existing research and studies on the topic of securing network infrastructure with cybersecurity was conducted to provide a broad understanding of the current state of knowledge. The literature review was used to gather information about the different cybersecurity

* Corresponding author: Muhammad Jamshid Khan *; Email: jams137@gmail.com

measures and techniques that organizations can implement to secure their network infrastructure, and to identify best practices and recommendations for organizations to enhance their cybersecurity. The goal of the literature review was to provide a comprehensive overview of the topic and to synthesize the existing knowledge on the subject.

3. Threats to Network Infrastructure

It is essential to understand the various types of threats to network infrastructure because these threats can take many different forms and attack through a range of vectors. By having a deep understanding of the types of threats that are most common, organizations can take proactive steps to protect their systems and networks from these attacks.

For example, if an organization is aware of the risks posed by phishing scams and social engineering, Organizations can implement initiatives like educating and training employees to decrease the chance of these types of attacks. If it knows that malware is a common threat, it can implement firewalls, anti-malware software, and regular software updates to reduce the risk of infection.

In addition, understanding the various types of threats to network infrastructure helps organizations to prioritize their security measures and allocate resources effectively. By knowing which threats are the most critical, organizations can focus their efforts on securing their networks against these threats, while still addressing the other risks.

In short, understanding the various types of threats to network infrastructure is essential to effective security because it allows organizations to take proactive steps to protect their systems, allocate resources effectively, and prioritize their security measures. Some of the frequent types of threats are:

3.1. Malware

Malware, which is a term derived from "malicious software," refers to any type of software that has been specifically created to damage computer systems, networks, or even individual devices. The term encompasses a wide range of malicious software, including viruses, worms, Trojans, spyware, adware, and ransomware.

Malware works by exploiting vulnerabilities in computer systems or networks to gain unauthorized access and execute malicious code. The techniques employed by malware can differ based on the category of malware and its goal. However, some common techniques used by malware include:

- Spreading through infected email attachments, software downloads, or other means of file transfer.
- Taking advantage of software or systems that have not been updated or fixed to gain unauthorized access and run harmful code.
- Impersonating legitimate software or websites to trick users into installing or running malware.
- Gaining access to sensitive information, such as login credentials or financial information, by monitoring keystrokes or capturing screen shots.
- Creating widespread chaos by infecting multiple computers or servers, initiating distributed denial of service attacks, or damaging or destroying files.
- Locking up data by encoding it and requesting payment in return for the key to decode it, which is a type of malicious software known as ransomware.

Once malware has gained access to a computer system or network, it can spread quickly to other systems and cause significant harm. In order to protect against malware, it is essential to implement robust security measures, such as antivirus and anti-malware software, firewalls, regular software updates, and user education and training.

3.2. Distributed Denial of Service (DDoS) attacks

A Distributed Denial of Service (DDoS) attack is a malicious attempt to overload a single target system with an excessive amount of traffic from multiple compromised computers. The objective of this type of cyberattack is to disrupt the normal functioning of the target system and render it inaccessible to users. The attack may be motivated by political, financial or personal interests, and its goal is to cause chaos and disruption by inundating the system with an overwhelming amount of data. The result is a system that becomes unavailable and unable to carry out its intended functions.

DDoS attacks work by overwhelming the target system with a massive amount of traffic, generated by a large number of compromised computers or devices, often referred to as a "botnet." The attack traffic is usually generated using a

variety of methods, such as sending a large number of requests to a server, creating a high volume of network traffic, or overloading the target system with a high volume of junk data.

Once a target system has been identified, the attacker infects a large number of computers or devices with malware, creating a botnet. The attacker then sends commands to the botnet, directing it to launch a DDoS attack against the target system. An excessive flood of data, initiated by a network of infected computers called a botnet, cripples the performance of the targeted system, making it inaccessible to its intended users

DDoS attacks can cause significant harm to the target system, and can result in lost revenue, reputational damage, and decreased customer confidence. To guard against the devastating consequences of DDoS attacks, deploying effective security measures is crucial. These measures can include firewalls, anti-DDoS services, intrusion detection and prevention systems, and load balancing, among others.

3.3. Man-in-the-Middle (MitM) attacks

An attacker can intercept and manipulate communication between two parties in a Man-in-the-Middle (MitM) attack, acting as a mediator between the two without their knowledge or permission. This type of cyberattack allows the attacker to access, change or obstruct the data being transmitted.

MitM attacks work by exploiting vulnerabilities in the communication channel between two parties. For example, an attacker may use fake Wi-Fi access points or phishing attacks to trick a victim into connecting to a network under the attacker's control. Once the attacker has gained control of the network, they can intercept and alter the communication between the victim and other parties.

MitM attacks can result in a wide range of harmful outcomes, including the theft of sensitive information, such as login credentials, financial information, and personal data, as well as the modification or corruption of data being transmitted.

To protect against MitM attacks, it is essential to implement strong security measures, such as using encrypted communication channels (e.g., SSL/TLS), verifying the identity of websites and networks, and using anti-virus and anti-malware software. Additionally, user education and training are important to help users identify and avoid potential MitM attacks.

3.4. Phishing Attacks

Phishing is a widespread method used by cyber criminals to obtain confidential information from individuals or organizations through deceptive means. This is achieved through the creation and use of fake emails, texts, or websites that appear to be legitimate, tricking victims into revealing their personal information such as passwords, credit card numbers, or PINs. The objective of a phishing attack is to acquire sensitive information for financial gain or to compromise the security of the targeted parties.

Phishing attacks work by using social engineering tactics to trick individuals into revealing sensitive information. For example, an attacker may send an email that appears to be from a trusted source, such as a bank or a well-known company, and instruct the recipient to click on a link to a fake website where they are asked to enter sensitive information. The fake website may look identical to the real one and may even have a valid SSL certificate, making it difficult for the victim to distinguish between the two.

The impact of a successful phishing attack can be severe, potentially leading to financial losses, identity theft, and the exposure of confidential information. To protect against phishing attacks, it is important to be cautious when receiving emails or messages from unknown sources and to verify the authenticity of links and websites before entering any sensitive information. Additionally, using anti-virus and anti-malware software, as well as enabling two-factor authentication, can also help to reduce the risk of falling victim to a phishing attack.

3.5. Unauthorized Access

Unauthorized access refers to the act of accessing a computer system, network, or data without proper authorization. This can be intentional or accidental, and it can occur through a variety of means, such as hacking, exploiting vulnerabilities, or using stolen credentials.

Unauthorized access to an infrastructure can has serious consequences, such as:

- **Data theft or breaches:** Hackers or unauthorized users can access sensitive information stored on the network, such as personal or financial data, and steal or misuse it.
- **System damage or disruption:** Unauthorized access to network infrastructure can allow hackers or malicious individuals to damage or disrupt the systems, causing downtime or system failure.
- **Spread of malware:** Unauthorized access to the network infrastructure can provide an opportunity for hackers to install malware or malicious software that can spread throughout the network and cause further damage.
- **Loss of reputation:** Data breaches or other security incidents that result from unauthorized access can harm an organization's reputation and erode customer trust.

Unauthorized access typically works by exploiting vulnerabilities in the infrastructure or by using stolen or guessed login credentials. Attackers may use a variety of techniques to gain unauthorized access, including brute force attacks, exploiting software vulnerabilities, or phishing attacks to steal login credentials.

Once an attacker has gained unauthorized access to an infrastructure, they may use a variety of techniques to exfiltrate sensitive information, install malware, or disrupt operations. In some cases, attackers may use the access to establish a "beachhead" from which they can launch further attacks.

To protect against unauthorized access, it is important to implement strong security measures, such as using strong passwords, regularly patching software, and implementing two-factor authentication. Additionally, monitoring for unusual activity, regularly backing up data, and having a robust incident response plan in place can also help to reduce the risk of unauthorized access and minimize the impact of any successful attacks.

4. Methods of Securing Network Infrastructure

There are various techniques that can be employed to ensure the security of a network infrastructure and guard against potential cyber threats:

4.1. Firewalls

A firewall acts as a barrier for a network's incoming and outgoing traffic, enforcing pre-established security regulations. It acts as a barrier between a private internal network and the public Internet, protecting sensitive information and systems from cyber threats. Firewalls are typically the first line of defence against cyber threats and are an essential component of any security strategy.

4.1.1. Types of Firewalls

- **Packet-Filtering Firewalls:** Packet-filtering firewalls are the simplest and most basic form of firewalls. They inspect incoming and outgoing network packets and allow or block them based on their source and destination addresses and ports.
- **Stateful Inspection Firewalls:** Stateful inspection firewalls, also known as dynamic packet filtering firewalls, are more advanced than packet-filtering firewalls. They inspect network packets in context and maintain a stateful view of the network connection, which enables them to enforce more sophisticated security policies.
- **Application-Level Firewalls:** Application-level firewalls, also known as proxy firewalls, operate at the application layer of the OSI model. They act as an intermediary between the client and server, inspecting and filtering incoming and outgoing traffic based on application-level protocols such as HTTP or FTP.
- **Next-Generation Firewalls:** Next-generation firewalls (NGFWs) are a type of firewall that combines features of traditional firewalls with other security technologies, such as intrusion detection and prevention, anti-virus, and anti-malware. NGFWs are designed to provide a more comprehensive and unified approach to network security.

Each type of firewall has its own strengths and weaknesses, and the best firewall for a given infrastructure will depend on the specific needs and requirements of the organization. Packet-filtering firewalls are simple and easy to configure, making them a good choice for small networks. Stateful inspection firewalls are more advanced and provide better protection against sophisticated cyber threats, making them a good choice for larger networks. Application-level firewalls offer the greatest level of security and control, but can be more complex to configure and maintain. NGFWs provide the most comprehensive protection, but can also be more complex and costly.

In conclusion, firewalls are an essential component of any security strategy, providing a first line of defence against cyber threats. Organizations can choose from a range of firewall types, including packet-filtering firewalls, stateful

inspection firewalls, application-level firewalls, and next-generation firewalls, depending on their specific needs and requirements.

4.2. Antivirus and Anti-Malware

Security software, such as antivirus and anti-malware programs, aim to identify and prevent malicious software, including viruses, Trojans, worms, and spyware, from infiltrating a computer or network. These programs use a variety of techniques, such as signature-based detection, heuristics, and behavioural analysis, to identify and neutralize malicious software.

Signature-based detection is a technique that uses known information about malware to identify it. Antivirus and anti-malware software maintain databases of virus signatures, which are unique identifiers for specific types of malwares. When a new file is encountered, the software will compare it to the database of signatures to see if it matches any known malware.

Heuristics and behavioural analysis are techniques that examine the behaviour of software to determine whether it is malicious. For example, heuristics might look for specific patterns of behaviour that are associated with malware, such as attempting to modify critical system files or attempting to steal sensitive information. Behavioural analysis, on the other hand, monitors the behaviour of a program in real-time to see if it is exhibiting malicious behaviour.

Antivirus and anti-malware software are essential tools for protecting against malware and maintaining the security of computer systems and networks. It is crucial to regularly update antivirus and anti-malware software and to utilize them along with other security measures such as firewalls, intrusion detection and prevention systems, and following security best practices for maximum protection.

4.3. Encryption

Encryption is the process of converting plaintext into ciphertext, which is unreadable without a decryption key. Encryption is used to secure sensitive information, such as credit card numbers, passwords, and personal data, from unauthorized access or interception. The use of encryption is crucial in ensuring the confidentiality of information transmitted across networks, especially over the Internet, where it may be vulnerable to interception by unauthorized individuals.

4.3.1. How Encryption Works

Encryption works by using mathematical algorithms to scramble plaintext into ciphertext. The encryption process is based on the use of encryption keys, which are a series of mathematical values that determine the encryption algorithm used to scramble the data. The encryption key is used to encrypt the data and is kept secret, while a matching decryption key is used to decrypt the encrypted data. The process of encryption transforms original data into a coded format called ciphertext, which can only be accessed with the appropriate decryption key. The encryption algorithm used and the length of the encryption key determine the security of the encryption.

4.3.2. Types of Encryptions

- **Symmetric Encryption**: is a method of data encryption where the same secret key is used to both encrypt and decrypt the data. This means that whoever encrypts the data must share the secret key with the recipient so they can decrypt it. Symmetric encryption is efficient and fast, making it ideal for encrypting large amounts of data, but it also requires secure key management to ensure the key is not misused or stolen.
- **Asymmetric Encryption:** also known as public key cryptography, is a method of encrypting and decoding data in which two different keys are used. One key is used for encrypting the data, and the other key is used for decrypting the data. The two keys are mathematically related, but they are different and cannot be used interchangeably. This type of encryption is considered more secure than symmetric encryption because it enables secure communication between parties without requiring the exchange of a shared secret key. In asymmetric encryption, a public key is made available to anyone who needs to send an encrypted message to the recipient, while the recipient's private key is kept secret and used to decrypt the message.

4.4. Applications of Encryption in Network Infrastructure

Encryption is used in several ways to secure network infrastructure, including:

- **SSL and TLS protocols:** Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protocols are encryption technologies used to secure data transmission over the internet by establishing a secure link between a server and a client. These protocols ensure that the data being transmitted is protected from unauthorized access and tampering during transmission.
- **VPNs**: VPN stands for Virtual Private Network and refers to a secure connection between a device and a network over a public network, such as the internet. VPNs are used to provide remote access to a private network, to secure data transmitted over public networks, and to bypass network restrictions, such as firewalls or censorship. The encrypted connection creates a secure tunnel that protects sensitive data from being intercepted or viewed by unauthorized parties. It provides privacy and security for online communication by encrypting data transmitted over the internet.
- **Email encryption**: Email encryption refers to the process of converting plaintext email messages into encrypted ciphertext that can only be deciphered with a specific decryption key. This ensures the confidentiality and privacy of email communication by preventing unauthorized access to the contents of the email.
- **Disk encryption**: Disk encryption refers to the process of encoding information on a computer's hard drive-in order to protect sensitive information from unauthorized access. It converts plaintext data into encrypted code, making it unreadable without a decryption key.

Encryption is an essential tool for securing network infrastructure and protecting sensitive information from unauthorized access. It is important to use encryption correctly and keep encryption keys secure to ensure the security of encrypted data.

4.5. Virtual Private Networks (VPNs)

VPN is a method of establishing a secure and private connection between a device and a network through a public network, like the internet, by using encryption. It is utilized for various purposes including remote access to a secure network, protection of data being sent over public networks, and bypassing network limitations like firewalls or censorship.

4.5.1. How VPNs Work

VPNs work by encapsulating network data in an encrypted tunnel between the device and the private network. The encryption is performed by a VPN client running on the device and a VPN server running on the private network. The encrypted data is transmitted over the public network and decrypted at the VPN server, which then forwards the data to its final destination on the private network.

4.5.2. Applications of VPNs in Network Infrastructure

VPNs are commonly used in network infrastructure to:

- **Provide remote access to a private network**: allowing employees to securely connect to the network from remote locations.
- **Secure data transmitted over public networks**: such as the Internet, by encrypting the data in transit.
- **Bypass network restrictions:** such as firewalls or censorship, by routing data through a different network.
- Connect multiple private networks into a single, virtual network.

4.5.3. VPNs Types

There are many types of VPNs, including:

- **Remote Access VPNs:** Use to access private networks remotely.
- **Site-to-Site VPNs:** which connect multiple private networks into a single, virtual network.
- **Intranet VPNs:** which connect multiple branches of a single organization into a single, virtual network.
- **Extranet VPNs:** which allow partners or customers to securely connect to an organization’s network.

It's crucial to employ VPNs in the right manner and set them up correctly to guarantee the protection of encrypted information.

4.6. Intrusion Detection and Prevention Systems (IDPSs)

Intrusion Detection and Prevention Systems (IDPSs) are security solutions designed to detect and prevent unauthorized access, use, disclosure, disruption, modification, or destruction of an organization's network and data. IDPSs monitor

network traffic and identify potential security threats, such as malware, unauthorized access attempts, or malicious network activity, and then take appropriate action to prevent or mitigate the threat.

4.6.1. How IDPSs Work

IDPSs work by monitoring network traffic for signs of security threats. There are two main types of IDPSs: signature-based and anomaly-based. Signature-based IDPSs use a database of known security threats, such as malware signatures or attack patterns, to identify potential threats. If a signature or attack pattern is detected, the IDPS takes appropriate action, such as blocking the traffic, alerting security personnel, or isolating the affected device.

Anomaly-based IDPSs use machine learning algorithms to identify deviations from normal network behaviour, which may indicate a security threat. For example, an IDPS may detect a sudden spike in network traffic or a large number of connections to a single device, which may indicate a malware infection or a DDoS attack.

4.6.2. Applications of IDPSs in Network Infrastructure

IDPSs are commonly used for the following operations

- IDPSs are used to monitor and secure networks against potential threats and attacks.
- They analyse network traffic in real-time and identify any suspicious activity or malicious traffic.
- They can be used to prevent data theft, network intrusion, and unauthorized access to sensitive information.
- IDPSs provide an added layer of security in combination with firewalls, antivirus software, and other security measures.
- They can also assist in detecting and preventing known and unknown cyber threats, such as malware, viruses, and zero-day exploits.
- IDPSs can provide alerts and reports on security incidents, enabling organizations to take quick action to address potential threats.

4.7. Identity and Access Management (IAM)

Identity and Access Management (IAM) is a vital aspect of cybersecurity that deals with the control and protection of digital identities and access to confidential information and systems. IAM encompasses a range of processes, technologies, and policies that help organizations control who has access to their systems and data and what they are allowed to do with that access. This includes authentication (verifying the identity of users), authorization (determining what actions users are allowed to take), and access control (enforcing those permissions).

The objective of IAM is to control and secure digital identities and access to confidential information and systems, ensuring only authorized users have access and preventing unauthorized access which could lead to misuse or loss of sensitive data. This is accomplished through a combination of access controls, password management, and other security measures.

4.8. Privileged Access Management (PAM)

Privileged Access Management (PAM) is a security framework that aims to secure and control access to sensitive data and systems within an organization. It is used to manage and monitor the privileged access of users, particularly those with administrative or elevated access, to the network infrastructure. This includes the use of strong authentication, authorization, and auditing procedures to minimize the risk of data breaches, theft, or unauthorized access to sensitive systems.

The main objective of PAM is to reduce the attack surface and prevent potential threats, such as malware infections, insider attacks, and social engineering, from exploiting vulnerabilities associated with privileged access. This is accomplished through a combination of security technologies and best practices, such as multi-factor authentication, password management, session monitoring, and role-based access control.

PAM solutions typically include features such as password vaulting, session management, and privileged activity reporting. These features enable organizations to securely store and manage privileged credentials, monitor and control user sessions, and generate detailed reports on privileged activity to help identify potential security incidents.

Recent research has shown the importance of PAM in securing network infrastructure. A study by Forrester Research showed that *90% of data breaches were caused by privileged access abuse, highlighting the need for effective PAM solutions*

to prevent this type of attack. Additionally, a report by Gartner found that *by 2025, 99% of cloud security failures will be the customer's fault, suggesting that PAM is increasingly critical in securing cloud infrastructure*.

In conclusion, PAM is a vital component of any organization's security strategy and helps secure the network infrastructure by reducing the risk of data breaches, theft, and unauthorized access to sensitive systems.

4.9. Regular Software Updates

Regular software updates play a crucial role in securing network infrastructure as they help fix vulnerabilities and patch security holes. Regular software updates ensure that the software systems used in the infrastructure are equipped with the latest security features and protection against newly discovered threats. The failure to apply software updates in a timely manner can make the infrastructure vulnerable to attacks and compromise the security of sensitive information.

According to a recent study by the Cybersecurity and Infrastructure Security Agency (CISA), "*outdated software is a common cause of cybersecurity incidents"*. In the study, it was found that 85% of all cyber-attacks in the previous year exploited vulnerabilities that had a patch available for at least three months. The study highlights the importance of regularly updating software to mitigate the risk of cyber-attacks.

In addition to security patches, software updates often bring new features, improved performance, and bug fixes that can enhance the overall functionality of the infrastructure. By regularly updating the software, organizations can ensure that they are using the most up-to-date and secure version of the software.

Regular software updates are a critical component of securing network infrastructure. Organizations should have a comprehensive software update management strategy in place to ensure that software is updated promptly and regularly. The objective of this approach is to reduce the likelihood of cyber-attacks and maintain the confidentiality, reliability, and accessibility of the information stored in the infrastructure.

4.10. Penetration Testing

Penetration testing is a simulated cyber-attack performed on a computer system, network, or web application with the goal of identifying vulnerabilities and weaknesses that could be exploited by malicious actors. It involves a comprehensive evaluation of the security posture of the target system and uses various techniques, such as probing and exploiting vulnerabilities, to assess the level of risk and evaluate the effectiveness of the existing security measures. The results of the testing are then used to improve the overall security posture and prevent potential real-world attacks.

Penetration testing is a crucial component of IT infrastructure security and should be performed regularly. A comprehensive pen testing plan should include several stages, such as,

- **Reconnaissance:** This is the initial stage of pen testing where the tester gathers information about the target system, including its IP addresses, domain names, operating systems, and any other relevant details. This information is used to create a map of the target's infrastructure and identify potential attack vectors.
- **Scanning:** In this phase, the person performing the testing employs various methods and tools to look for weaknesses in the target system. This involves performing port scans, network scans, and scans for vulnerabilities to determine open ports, services, and potential attack methods.
- **Exploitation:** In the exploitation stage, the tester attempts to penetrate the target system by exploiting any vulnerabilities identified during the previous stages. The tester may use automated tools or manual techniques to gain unauthorized access to the target and perform various actions, such as installing malicious software, stealing sensitive data, or disrupting normal operations.

To ensure that the pen testing process is thorough and effective, it is important to use experienced pen testers and to choose a testing methodology that aligns with your specific security goals and risks. In addition, the results of pen testing should be used to improve the overall security posture of the infrastructure and to implement best practices for secure configuration and ongoing monitoring.

There are various methods and tools available for pen testing, such as,

- **Black box testing:** is a type of testing where the tester only has access to the inputs and expected outputs, without any knowledge of the internal workings of the system. This type of testing focuses on verifying the functionality of the system and is based on the requirement specifications.

- **Grey box testing**: is a type of testing where the tester has limited knowledge of the internal workings of the system. This type of testing combines elements of black box and white box testing, and typically includes an understanding of the system architecture and data flows.
- **White box testing:** is a type of testing where the tester has complete knowledge of the internal workings of the system. This type of testing focuses on the internal logic and structure of the code, and is typically performed by developers or internal personnel.

Each type of testing has its own unique advantages and disadvantages, and the choice of which type of testing to use depends on the specific requirements of the system being tested. Pen testing is an essential aspect of securing IT infrastructure and should be performed regularly to identify and mitigate potential security risks.

4.11. Employee Awareness and Training

The concept of Employee Awareness and Training encompasses the process of informing employees about the significance of cybersecurity and their responsibility in safeguarding the IT infrastructure. The goal is to raise awareness of potential threats and encourage safe and secure behaviour within the organization. This is critical in securing the IT infrastructure as employees can often be the weakest link in a company's cybersecurity defence, due to lack of knowledge and poor security practices.

Studies have shown that a significant number of cyberattacks are the result of employees falling for phishing scams, using weak passwords, or accessing sensitive data on unsecured networks. Regular employee awareness and training programs can help reduce these risks by providing employees with the knowledge and skills needed to identify potential threats and respond appropriately.

Employee awareness and training programs typically cover topics such as password security, phishing scams, data protection, and social engineering. They may also include interactive simulations and hands-on exercises to help employees better understand the potential threats they may face and how to prevent them.

According to a recent report by Gartner, "*Providing ongoing security awareness and training to employees is a critical component of a successful cybersecurity program*". The report suggests that organizations should provide annual, mandatory cybersecurity training for all employees and regularly assess the effectiveness of their training programs.

The importance of educating and training employees about cybersecurity is crucial for protecting the IT infrastructure. By giving employees the necessary understanding and abilities to recognize and handle potential security risks, organizations can lower the threat of cyber-attacks and enhance their overall security situation.

5. Conclusion

To sum up, ensuring the protection of network infrastructure through cybersecurity measures is a crucial and continuous concern for businesses of all sizes in today's digital environment. The ever-evolving and increasingly sophisticated nature of cyber threats necessitates a comprehensive approach to securing sensitive data and systems. This article has discussed several significant security strategies that companies can adopt to secure their network infrastructure, such as firewalls, encryption, VPNs, IDPSs, IAM, and PAM. Firewalls play a crucial role in protecting an organization's network from external threats by monitoring and controlling incoming and outgoing traffic. Encryption enhances security by converting sensitive information into coded form, stopping unauthorized access. VPNs offer a secure connection for remote employees, giving them the ability to connect to their organization's network from any location. IDPSs are monitoring tools for network activity, instantly warning administrators about possible dangers. A complete security plan should also include IAM and PAM, which are essential elements of cybersecurity. IAM controls access to an organization's systems and resources, while PAM manages privileged access to sensitive data. Regular software updates ensure that systems are up-to-date with the latest security patches and protections. Employee awareness and training programs are also essential to educating employees on safe computing practices and reducing the risk of human error that can lead to security breaches. Organizations must continually assess and improve their security measures to stay ahead of evolving cyber threats. By implementing the recommended security measures and continuously monitoring their network infrastructure, organizations can greatly reduce the risk of unauthorized access and prevent potential data breaches.

Compliance with ethical standards

Acknowledgments

I acknowledge the valuable contributions of the published works and research studies that were consulted during the course of this research project. The insights and knowledge gained from these sources helped to inform and shape my research efforts. I would also like to express my gratitude to the research participants who generously gave their time and insights to this study.

Disclosure of conflict of interest

The author declares no conflict of interest.

References

[1] Best practices for stopping malware and other threats. Broadcom, https://techdocs.broadcom.com/us/en/symantec-security-software/endpoint-security-and-management/endpoint-protection/all/Using-policies-to-manage-security/best-practices-for-stopping-malware-and-other-threats.html

[2] How to get rid of malware. Kaspersky, https://www.kaspersky.com/resource-center/threats/malware-protection

[3] Handling Destructive Malware: United States Computer Emergency Readiness Team (US-CERT), https://www.cisa.gov/uscert/ncas/tips/ST13-003

[4] Understanding Denial-of-Service Attacks: United States Computer Emergency Readiness Team (US-CERT), https://www.us-cert.gov/ncas/tips/ST04-015

[5] What is a DDoS Attack? - DDoS Meaning: Kaspersky, https://usa.kaspersky.com/resource-center/threats/ddos-attacks.

[6] What Is a DDoS attack?: Akamai, https://www.akamai.com/our-thinking/ddos

[7] Securing End-to-End Communications. : United States Computer Emergency Readiness Team (US-CERT), https://www.cisa.gov/uscert/ncas/alerts/TA15-120A

[8] What is Phishing? Attack Techniques & Prevention Tips: ITGovernance, https://www.itgovernance.co.uk/phishing#:~:text=Phishing%20works%20by%20sending%20messages,as%20their%20credit%20card%20number.

[9] Good Security Habits. : United States Computer Emergency Readiness Team (US-CERT), https://www.us-cert.gov/ncas/tips/ST04-003.

[10] Cryptography and Network Security, Principles and Practice: by William Stallings (7th Edition).

[11] Applied Cryptography: Protocols, Algorithms, and Source Code in C: by Bruce Schneier (2nd Edition).

[12] NIST Special Publication 800-57 Part 1, Recommendation for Key Management (Rev. 4) (available at https://csrc.nist.gov/publications/detail/sp/800-57-part-1/rev-4/final)

[13] A Beginners Guide to VPNs – A Complete VPN Guide for 2022: Joe Robinson, https://www.privacyaffairs.com/beginners-guide-to-vpn/

[14] Handbook of Research on Cybercrime and Digital Forensics, Technological and Societal Perspectives: edited by Justin C.P. Wan, Jianying Zhou, and Jian Chen (Information Science Reference, 2017).

[15] Network Security Assessment: Know Your Network: by Chris McNab (O'Reilly Media, 2013).

[16] The 2021 State Of Enterprise Breaches (April 8th, 2022), https://www.forrester.com/report/the-2021-state-of-enterprise-breaches/RES177333

[17] Is the Cloud Secure? (gartner.com October 10, 2019), https://www.gartner.com/smarterwithgartner/is-the-cloud-secure

[18] Understanding Patches and Software Updates, Cybersecurity and Infrastructure Security Agency, 2021: https://www.cisa.gov/tips/st04-006

[19] The State of Cybersecurity and Digital Trust, Accenture, 2016: https://www.accenture.com/t20170510t000709__w__/us-en/_acnmedia/pdf-23/accenture-state-cybersecurity-and-digital-trust-2016-executive-summary-june.pdf

Author's short Biography

Muhammad Jamshid Khan is a highly experienced Senior Network and Cybersecurity Engineer. With a Master's degree in Computer Science from Virtual University of Pakistan and certification in Ethical Hacking from EC-Council, he possesses a strong foundation in technology and expertise in Network and Cybersecurity. Currently serving as a Senior Network Engineer at Sopra Steria Asia, Khan is responsible for providing comprehensive solutions to clients. His commitment to staying up-to-date with the latest technology advancements in his field makes him a valuable asset to his colleagues and clients. Outside of work, Khan enjoys traveling and studying to expand his knowledge and skills. His dedication to personal and professional growth, combined with his passion for Network and Cybersecurity, has allowed him to build a successful career in the technology industry.