NOLEGEIN Journal of
Management Information Systems

ISSN: 2581-6810
Volume 5, Issue 2, 2022
DOI (Journal): 10.37591/NJMIS

http://mbajournals.in/index.php/JoMIS/index

Review NJMIS

Cyber Security Instruments and Methods for Data Safeguard

Pinal Jain

Abstract

Learning and understanding cyber security how to effectively use it are crucial in current environment, which is dominated by technology and network connections. Nevertheless, working system, crucial lines, if no security is present to protect it. No matter if the organization uses IT or not, it needs to be protected in the same way. With the advancement of modern cyber security technology, the bushwhackers are not behind. They are using more advanced hacking techniques and focusing on the vulnerabilities of many different businesses. Cyber security is essential because organizations in the service, political, fiscal, medical, and economic sectors gather, process, and store enormous amounts of data on PCs and other devices. Crucial information of any kind, including financial data, intellectual property data, specialized data, and other forms of data, may account for a sizeable chunk of that.

Keywords :- Cyber security, *technology ,network connections* , information security , privacy of data

BACKGROUND

Figure 1 In the world we currently inhabit, all knowledge is stored in a highly digitalized format. Privacy and information security are now likely to be key priorities in every firm. The information is the most valuable thing there is, yet there is always a risk of security breach. Cybersecurity was created as a result to protect our data from online dangers. Cyber and security are frequently used as subcategories of cybersecurity. The term “cyber” technology broadly refers to systems, networks, software and data. On the other side, security is concerned with protecting systems, networks, applications, and data. The goal of cybersecurity is to stop attacks, harm, and unauthorized access to networks, computers, software, and data.

Cyber security is a critical component of any data protection strategy. Cyber security tools and techniques are used to protect data, networks, and systems from unauthorized access, malicious attacks, and other threats. Cyber security tools and techniques include antivirus software, firewalls, encryption, network segmentation, intrusion detection, and application security.

***Author for Correspondence**
Pinal Jain
E-mail: Pinaljain19997@gmail.com

Research Scholar, Thakur Institute of Management Studies, Career Development & Research (TIMSCDR), Mumbai, India

Received Date: March 17, 2023
Accepted Date: April 04, 2023
Published Date: April 14, 2023

Citation: Pinal Jain. Cyber Security Instruments and Methods for Data Safeguard. NOLEGEIN Journal of Management Information Systems. 2022; 5(2): 20–27p.

Figure 1. what is cyber security?

© MBA Journals 2022. All Rights Reserved

INTRODUCTION

Cyber Security Tools and Techniques for Data Protection are methods used to protect sensitive data from unauthorized access and malicious attacks. These tools and techniques can range from basic data encryption and firewalls, to more advanced tools such as Intrusion Detection Systems, Identity and Access Management Systems, and Network Monitoring.[1]

Data encryption is an important tool used to protect data from unauthorized access and malicious attacks. Encryption scrambles data into an unreadable form, making it difficult for attackers to access or modify. Firewalls are another important tool used to control access to a network and its critical data. Firewalls can also be used to monitor the system for suspicious activity and alert administrators of any malicious activity.[2]

Intrusion Detection Systems (IDS) on a system are made to spot any harmful behavior. An IDS will find malicious activity like port scans, and even malicious code. Identity and Access Management Systems (IAM) are also important tools used to control who can access what resources. These systems ensure only authorized users have access to the data that they need to do their jobs.

Network Monitoring is another important technique for data protection. This involves monitoring all network traffic for suspicious activity. Network monitoring tools can detect malicious attacks and alert administrators of any suspicious activity.[3]

These are just some of the many cyber security tools and techniques used to safeguard sensitive information from unauthorized access and malicious attacks. Organization must always consider the use of these tools and techniques to ensure their data is secure.[4]

THREATS IN CYBERSPACE

Malignant

Malignant is a term used to describe malacious piece of code, and is software made to damage, or take unauthorized access to system. Examples include worms, virus, trojan. Malware can be spread through email, malicious websites, file-sharing networks, and other online sources. It can also be spread through physical media, such as USB sticks and CDs. Malware can be used to steal data, disrupt the operation of a computer system, and even take control of a computer system. Malware can also be used to spread false information or target specific individuals or organizations for malicious purposes. The following are the different types of malware (Figure 2):

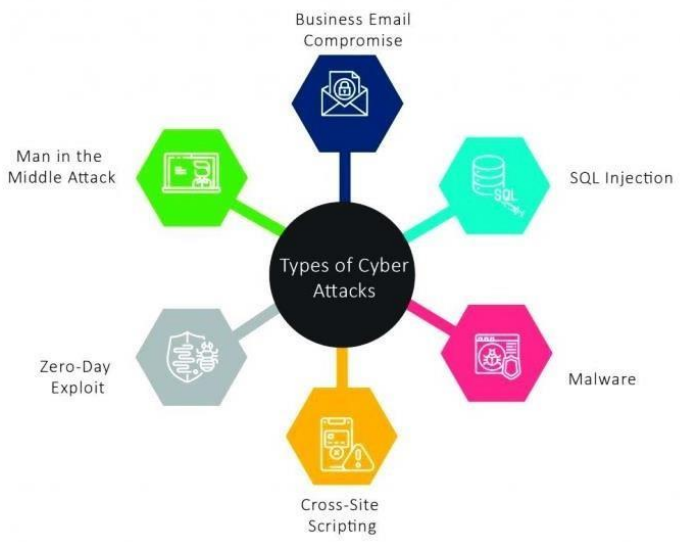

Figure 2. Types of cyber attacks.

© MBA Journals 2022. All Rights Reserved

Ransomware

Encryption is a feature of randsomeware software, which prevents a target from accessing its data unless a ransom is paid. The victim organization is rendered partially or entirely inoperable until it pays; however, there is no guarantee that payment will result in the delivery of the necessary decryption key or that the provided decryption key will function properly.[5]

Worms

It is a piece of software that, in the absence of human intervention, copies itself and spreads it from system to device. They no longer need to connect to any programme in order to steal or damage the data.

Adware

It is a marketing tool that displays classified advertising on our device and spreads malware. It is a bad application that was set up without the user's consent. This software's primary objective is to make money for its creator by displaying advertisements on users' browsers.

Botnets

Cybercriminals can control them thanks to a number of internet-connected devices that have malware installed on them. Without the user's consent, it enables fraudsters to obtain credentials leaks, unauthorised access, and information theft.

Spyware

It is a piece of software that covertly keeps track of what users do on their computers. Adware, for instance, can seek to intercept deposit card details that fraudsters might use for illicit purchases, cash withdrawals, etc.

Trojans

It's a particular type of malware or code that impersonates a legitimate software programme or file in order to trick us into downloading and running it. Its main goal is to damage or steal our machine's data or engage in other risky behavior on our network.

Virus

Malacious software programmes known as computer viruses are created with the intention of replicating themselves and spreading from one machine to another. Those can be spread through email attachments, malicious links, or through downloading infected software. They can cause a variety of problems, such as data loss, system crashes, and even identity theft. To protect yourself from computer viruses, you should always install and regularly update antivirus software, avoid clicking on unknown links and attachments, and be cautious when downloading files from the internet.[6]

Phishing

Phishing is a type of cyber-attack where criminals try to trick victims to providing crucial data or financial details by posing as a legitimate entity. It typically involves sending emails, text messages, or other online data that come from reputable resource In most cases, the attacker will use a fake website or email address to try and gain the victim's trust. Phishing attacks can also be used to spread malicious code, like viruses and Trojans, or to collect data for use in identity theft.[7]

Man-in-the-Middle Attacks

Man-in-the-middle battles are a sort of cyberattack in which an evil individual pretends to be both the sender and the recipient and enters a communication between two people. The bad actor is then able to eavesdrop on the conversations between the two parties and possibly change them. Access to sensitive data, including passwords, credit card numbers and other private information, is made possibly by this kind of attack. MITM attacks can be carried out in a number of methods, including via public Wi-Fi hotspots, unsecured wireless networks and even malicious software.[8]

© MBA Journals 2022. All Rights Reserved

Denial of Service Attack

The goal of a denialof-service attack is to prevent the intended users from accessing a computer or network resource. DoS attacks can be carried out in a number of ways, such as by sending malicious packets to a target system or saturating it with traffic. A DoS attack aims to send too many requests to the target system, which could result in it crashing or going unresponsive. DoS assaults can have a big effect on businesses since they can result in lost sales, reputational harm and disgruntled clients.[9]

Zero-Day Exploits

A zero-day exploit is a computer security exploit that takes advantage of a vulnerability in software or hardware on the same day that the vulnerability is discovered. It is an attack that takes place before any patch or fix for the vulnerability is released, leaving the system completely exposed to malicious activity. As most vulnerabilities are discovered by security researchers, the malicious actors behind zero-day exploits often purchase the information from those researchers for a high price. Once the exploit is used, the affected system is vulnerable until the vendor releases a patch to fix the vulnerability.

SQL Injection

SQL injection attack which can be used to exploit security vulnerabilities present in a web application's code. It involves inserting malicious code, such as SQL commands, into input fields and using it to manipulate a database in order to gain access to confidential information. SQL Injection attacks can be used to execute system commands, edit, remove or circumvent authentication The goal of an attacker is to gain unauthorized access to data in a database and, potentially, execute malicious code on a database server.

Social Engineering

Social engineering is a term used to describe a type of attack on a computer system that targets the human element of the system. The attack that focuses on manipulating person who reveal confidential assests, or tricking them into performing certain actions, such as downloading malicious software. Social engineering attacks can be used to gain access to a system, steal data, or disrupt operations. A successful social engineering attack can be devastating for an organization, so it is important to understand how it works and how to protect against it.[10]

METHODS AND APPLICATIONS FOR DATA PROTECTION

Firewalls and Intrusion Detection Systems (IDS) have two of the most important components of any network security system. Firewalls act as a gatekeeper, controlling the flow of traffic between the internal network and the external network by blocking or allowing certain types of traffic based on predetermined rule. Network traffic is watched by an instrusion detection system (IDS) for any abnormal activity, such as attempts at unauthorized access or harmfulcode. It then alerts the system administrator of any suspicious activity. Firewalls and IDS systems can be used together to provide comprehensive protection against malicious attacks Figure 3.

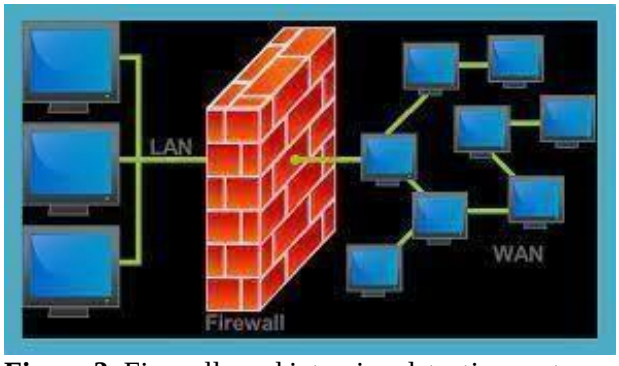

Figure 3. Firewalls and intrusion detection system.

© MBA Journals 2022. All Rights Reserved

Data Encryption Techniques

1. ***Symmetric key encryption:*** Data can be encrypted using symmetric key encryption, which uses the same key for encryption and decryption. Sensitive data is protected with this sort of encryption also referred to as secret key encryption.
2. ***Asymmetric Key Encryption****:* Asymmetric key encryption is a type of encryption where two different keys are used, a private key and a public key. Using the public key for data encryption and the private key for data decryption.
3. ***AES Encryption:*** The symmetric encryption method known as the Advanced Encryption Standard is used to secure sensitive data. It is used by a range of organizations from governments to banks to encrypt data.
4. ***RSA Encryption****:* RSA is an asymmetric encryption algorithm that is used to secure digital communications. It is used for a range of applications from secure web transactions to digital signatures.
5. ***Hash Encryption****:* Hash encryption is a type of encryption that uses a mathematical algorithm to create an encrypted string of data. It is used for data integrity and data verification.

Network Security Monitoring (NSM)

It is the process of continuously monitoring a network for security threats. It involves the implementation of automated tools and processes to detect, analyze, and respond to suspicious activity. These tools and processes are used to identify and stop malicious activity, as well as potentially mitigate the damage caused by successful attacks. NSM can be used to detect and mitigate threats such as malware, denial-of-service attacks, and other forms of malicious activity. Also, it can be used to find security flaws such improper system configuration or illegal network access. NSM can also be utilized to spot suspicious activities or rule infractions and take appropriate action.

Multi-factor Authentication

Its solutions are security measures that require users to provide more than one form of authentication to access a system. Examples of multi-factor authentication solutions include hardware-based tokens, biometric authentication, one-time passwords, and SMS-based authentication.

Application Security Best Practices

1. Implement authentication and authorization of users who access the application.
2. Encrypt both data at rest and in transit.
3. Deploy the application in a secure hosting environment.
4. Use secure coding best practices and tools to detect and mitigate vulnerabilities.
5. Perform regular security testing and vulnerability assessments.
6. Monitor and log application usage and access.
7. Restrict access to sensitive functions and data.
8. Implement a web application firewall (WAF) to protect against malicious requests.
9. Regularly patch and update your applications.
10. Train developers and users in security best practices.

Penetration Testing and Vulnerability Assessments

They are both important security measures used to ensure the safety and security of information systems. Penetration testing is a type of security testing that is used to evaluate the security of information systems by simulating a malicious attack on the system. It is designed to find potential vulnerabilities in the system, and to identify ways to exploit those vulnerabilities. Vulnerability assessments, on the other hand, are used to identify and assess the vulnerabilities in a system without trying to exploit them. Vulnerability assessments will help to identify any weaknesses in the system, and recommend solutions to fix them. Both penetration testing and vulnerability assessments should be used to ensure the security of information systems, as they can provide valuable insight into the security of the system.

© MBA Journals 2022. All Rights Reserved

SECURE SOFTWARE DEVELOPMENT LIFECYCLE

1. ***Planning:*** During the planning phase of the secure software development life cycle, the project team should begin by determining the general requirements of the software, such as its purpose, functionality, and any potential risks or vulnerabilities associated with it. The team should also define any security objectives and identify any applicable regulations that must be adhered to.
2. ***Requirements:*** During the requirements phase, the team should develop a set of detailed requirements for thesoftware, including any security requirements. This includes user authentication and authorization, data privacy, and secure communication.
3. ***Design:*** During the design phase, the team should create the architecture and design of the software, including any necessary security measures. This includes creating secure user interfaces, encrypting data in transit, and using secure coding techniques.
4. ***Implementation:*** During the implementation phase, the team should begin coding the software and integrating any necessary security measures. This includes implementing authentication and authorization controls, data encryption, and secure coding best practices.
5. ***Testing:*** During the testing phase, the team should test the software to ensure that it meets all security requirements. This includes testing for vulnerabilities and implementing any necessary fixes.
6. ***Deployment:*** During the deployment phase, the team should deploy the software in a secure manner. This includes ensuring that all security measures are in place and working correctly.
7. ***Maintenance:*** During the maintenance phase, the team should monitor the software to ensure that it remains secure. This includes patching any discovered vulnerabilities, responding to security alerts, and updating security protocols as needed Figure 4.

Figure 4. Software life cycle.

METHODOLOGY TOOLS & TECHNIQUES USED IN CYBER SECURITY

1. ***Risk Assessment:*** Risk assessments are used to identify potential threats and vulnerabilities, as well as measure the potential impact of those threats on an organization's systems and data.
2. ***Penetration Testing:*** Penetration testing simulates real-world attacks on an organization's systems to identify and address vulnerabilities in the network architecture and system configurations.
3. ***Security Auditing:*** Security audits are used to assess an organization's security policies, procedures, and systems to ensure they are compliant with industry standards.
4. ***Intrusion Detection System:*** Network traffic is monitored by intrusion detection systems for suspicious activity and when malicious activity is found administrators are notified.

© MBA Journals 2022. All Rights Reserved

5. ***Firewalls****:* Firewalls are used to protect an organization's systems and data by controlling incoming and outgoing traffic.
6. ***Encryption****:* Encryption is used to secure data in transit and at rest, protecting it from unauthorized access or modification.
7. ***Identity and Access Management****:* Identity and access management (IAM) systems are used to control user access to systems and data, ensuring only authorized users have access.
8. ***Incident Response Planning****:* Incident response plans are used to develop and document processes for responding to cyber security

IMPORTANT CLOUD SECURITY ISSUES

Confidentiality

Confidentiality dictates that only authorised individuals or systems have access to sensitive or classified information. The data being delivered across the network shouldn't be visible to unauthorized users. To gain access to your information, the attacker may try to obtain the data via a variety of internet tools. Use encryption measures to safeguard your data so that even if the attacker has access to it, they are unable to decrypt it. This is a key strategy for avoiding this. Example of encryption standards include DES and AES. You can secure your data via a VPN tunnel. Secure data transfer over networks is made possible via virtual network.

Integrity

The subject of integrity will be examined next. Making sure the data hasn't been changed is the aim here. Data corruption is the result of failing to maintain data integrity. To check whether our data has been changed we use a hash technique. The SHA and MD5 types are employed. In comparison, SHA is a 160-bit hash, while MD5 is a 128-bit hash if we're using SHA-1. Additionally, we could use SHA-0, SHA-2 and SHA-3 SHA techniques.

Availability

It follows that users ought to have simple access to the network. Both systems and data are affected by this. To ensure availability, the network administrator must keep equipment up-to-date, do routine maintenance, have a fail-over plan, and stay clear of network bottlenecks. Due to attacks like DoS or DDoS that exhaust a network's resources, the network may become inoperable. The impacts can be highly noticeable to the businesses and people who rely on the network as a tool for commerce. In order to stop such attacks, the proper actions should be taken Figure 5.

Figure 5. Security issues.

CONCLUSION

Cyber security instruments and methods for data safeguard are essential in today's digital world. Cyber security instruments include firewalls, intrusion detection systems, encryption software, secure

© MBA Journals 2022. All Rights Reserved

web servers, and more. Cyber security methods include risk management, incident response plans, threat intelligence, and other proactive measures. By taking a proactive approach to cyber security, organizations can protect their data and systems from malicious actors.

REFERENCES

1. AlMadahkah AM. Big data in computer cyber security systems. International Journal of Computer Science and Network Security (IJCSNS). 2016 Apr 1;16(4):56.
2. Dhillon G, Smith K, Hedström K. Ensuring core competencies for cybersecurity specialists. InCybersecurity Education for Awareness and Compliance 2019 (pp. 121-133). IGI Global.
3. Bada M, Nurse JR. Developing cybersecurity education and awareness programmes for small-and medium-sized enterprises (SMEs). Information & Computer Security. 2019 Jun 11;27(3):393-410.
4. Arce D. Cybersecurity for Defense Economists. Defence and Peace Economics. 2022 Nov 6:1-21.
5. Boss SR, Galletta DF, Lowry PB, Moody GD, Polak P. What do systems users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors. MIS quarterly. 2015 Dec 1;39(4):837-64.
6. Sinha P, kumar Rai A, Bhushan B. Information Security threats and attacks with conceivable counteraction. In2019 2nd International Conference on Intelligent Computing, Instrumentation and Control Technologies (ICICICT) 2019 Jul 5 (Vol. 1, pp. 1208-1213). IEEE.
7. Agag GM, Khashan MA, Colmekcioglu N, Almamy A, Alharbi NS, Eid R, Shabbir H, Abdelmoety ZH. Converting hotels website visitors into buyers: How online hotel web assurance seals services decrease consumers' concerns and increase online booking intentions. Information Technology & People. 2020 Jan 14;33(1):129-59.
8. Rajawat AS, Bedi P, Goyal SB, Shaw RN, Ghosh A. Reliability Analysis in Cyber-Physical System Using Deep Learning for Smart Cities Industrial IoT Network Node. AI and IoT for Smart City Applications. 2022:157-69.
9. Wikipedia Contributors. Computer security [Internet]. Wikipedia. Wikimedia Foundation; 2023 [cited 2023 Apr 4]. Available from: https://en.wikipedia.org/wiki/Computer_security
10. Mo Y, Kim TH, Brancik K, Dickinson D, Lee H, Perrig A, Sinopoli B. Cyber–physical security of a smart grid infrastructure. Proceedings of the IEEE. 2011 Sep 12;100(1):195-209.

© MBA Journals 2022. All Rights Reserved