IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 2, June 2022
Impact Factor: 6.252

Data Protection using Cyber Security Tools and Techniques

Ms. Anjali Ramnayan Yadav
Student, Department of MCA
Late Bhausaheb Hiray S S Trust's Hiray Institute of Computer Application, Mumbai, India

Abstract: *It's critical to understand what cyber security is and how to apply it successfully in moment's world, which is driven by technology and network connections. However, systems, vital lines, If there's no security to secure it. Every organisation, whether it's an IT establishment or not, must be shielded in the same way. The bushwhackers, too, don't lag before with the development of new cyber security technology. They're employing bettered hacking tactics and fastening on the weak points of numerous businesses. Because service , political, fiscal, medical, and commercial, organisations collect, exercise, and store vast quantities of data on PCs and other bias , cyber security is vital. Sensitive information, whether fiscal data, intellectual property, particular information, or other types of data, can regard for a significant portion of that.*

Keywords: CIA TRIAD, Cyber Threats

I. INTRODUCTION

We are currently living in a very world where all the knowledge are maintained in an exceedingly digital form. Nowadays, Privacy and security of the information could be a top priority in any organization. Nothing is more valueable than the info but the danger of a security breach is ever-growing. So, cybersecurity came into the existence for safeguarding our data from cyber threats. Cybersecurity are often divided into two categories: cyber and security. The term "cyber" refers to a good range of technology, including systems, networks, programmes, and data. Security, on the opposite hand, is worried with the safeguarding of systems, networks, applications, and data. Cybersecurity is aimed toward preventing attacks, damage, and illegal access to networks, computers, programmes, and data.

1.1 Definition

Cybersecurity refers to a method for defense of our digital data. Today we send or receive any quite the info through an data system. After all, data is what a criminal is searching for. The network, servers, and computers are simply conduits for data. Effective cybersecurity lowers the chance of cyber-attacks and protects businesses and individuals from unwanted access to systems, networks, and technology. As attackers get increasingly innovative, it's vital to define cybersecurity and grasp the foundations of cybersecurity.

How does data Security make working so easy?

- If there were no security and safety tools, a business or society could suffer extensive damage.
- Cyber security will now play an important role in preventing our data or system from being hacked or damaged.
- By using tools and techniques for cyber security, our work has become easier.
- In today's linked world, our digital data is at low risk just because of cyber security.

1.2 Types of Cyber Threats

1. **Malware:** It is nothing but a malicious software, which is the most frequent cyber attacking tool. It is used by the attackers to harm a reliable user's system. The following are the essential kinds of malware created by using the hacker:
2. **Virus:** It is a malicious piece of code that spreads from one machine to another. It can smooth documents and spreads all through a laptop system, infecting files, stoles information, or harm device.
3. **Spyware:** It is a software program that secretly documents records about person things to do on their system. For example, adware may want to seize deposit card small print that can be used with the aid of the

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 2, June 2022
Impact Factor: 6.252

cybercriminals for unauthorized shopping, cash withdrawing, etc.

4. **Trojans:** It is a kind of malware or code that seems as professional software program or file to idiot us into downloading and running. Its predominant reason is to corrupt or steal information from our machine or do different unsafe things to do on our network.

5. **Ransomware:** It's a piece of software program that encrypts a user's archives and facts on a device, rendering them unusable or erasing. Then, a economic ransom is demanded by means of malicious actors for decryption.
6. **Worms:** It is a piece of software program that spreads copies of itself from system to gadget barring human interaction. It does now not require them to connect themselves to any software to steal or injury the data.
7. **Adware:** It is an marketing software program used to unfold malware and shows classified ads on our device. It is an undesirable application that is established barring the user's permission. The fundamental goal of this software is to generate income for its developer by using displaying the commercials on their browser.
8. **Botnets:** It is a series of internet-connected malware-infected gadgets that enable cybercriminals to manipulate them. It permits cybercriminals to get credentials leaks, unauthorized access, and information theft except the user's permission.
9. **Phishing:** Phishing is a kind of cybercrime in which a sender looks to come from a proper business enterprise like PayPal, eBay, monetary institutions, or pals and co-workers. They contact a goal or aims by using email, phone, or textual content message with a hyperlink to persuade them to click on that links. This hyperlink will redirect them to fraudulent web sites to furnish touchy information such as private information, banking and credit score card information, social safety numbers, usernames, and passwords. Clicking on the hyperlink will additionally set up malware on the goal gadgets that permit hackers to manage units remotely.
10. **A Man-in-the-Middle Attack:** A man-in-the-middle assault is a kind of cyber chance (a structure of eavesdropping attack) in which a cybercriminal intercepts a dialog or records switch between two individuals. Once the cybercriminal locations themselves in the center of a two-party communication, they appear like true members and can get touchy statistics and return specific responses. The predominant goal of this kind of assault is to obtain get right of entry to to our commercial enterprise or purchaser data. For example, a cybercriminal should intercept facts passing between the goal system and the community on an unprotected Wi-Fi network.
11. **Distributed Denial of Service(DDOS):** It is a kind of cyber chance or malicious try the place cybercriminals disrupt focused servers, services, or network's ordinary visitors via enjoyable authentic requests to the goal or its surrounding infrastructure with Internet traffic. Here the requests come from countless IP addresses that can make the machine unusable, overload their servers, slowing down extensively or briefly taking them offline, or stopping an organisation from carrying out its integral functions.
12. **A Brute Force Attack:** A brute force assault is a cryptographic hack that makes use of a trial-and-error approach to bet all feasible combos till the right records is discovered. Cybercriminals commonly use this assault to reap private records about centered passwords, login info, encryption keys, and Personal Identification Numbers (PINS).

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 2, June 2022
Impact Factor: 6.252

13. **SQL Injection Attack:** SQL injection is a frequent assault that happens when cybercriminals use malicious SQL scripts for backend database manipulation to get admission to touchy information. Once the assault is successful, the malicious actor can view, change, or delete touchy corporation data, consumer lists, or non-public client important points saved in the SQL database.
14. **A DNS Attack:** A DNS assault is a kind of cyberattack in which cyber criminals take gain of flaws in the Domain Name System to redirect web site customers to malicious web sites (DNS hijacking) and steal statistics from affected computers. It is a extreme cybersecurity hazard due to the fact the DNS gadget is an crucial component of the net infrastructure.

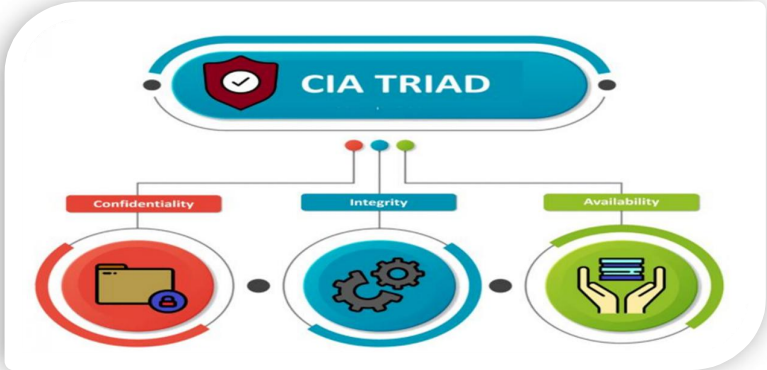
II. GOALS AND OBJECTIVES

The majority of the business operations run on the net exposing their data and resources to various cyber threats. Since the info and system resources are the pillars upon which the organization operates, it drives lacking maxim that a risk to those individuals is certainly threat to the group itself. A threat will be anywhere between a minor bug in an exceedingly code to a fancy cloud hijacking liability.

Risk assessment and estimation of the value of reconstruction help the organization to remain prepared and to seem ahead for potential losses. Thus knowing and formulating the objectives of cybersecurity exact to every organization is crucial in protecting the valuable data. Cybersecurity may be a practice formulated for the safeguard of complex data on the net and on devices safeguarding them from attack, destruction, or unauthorized access.

The main objective of cyber security is to secure or protect our data from cybercriminals or attackers. For implementing the abjective of cyber security, CIA model is formed. CIA stands for Confidentiality , Integrity and Availability. This model is aimed to guide strategies for security.

2.1 CIA TRIAD



2.2 Confidentiality

It is about confining data access to help unwanted exposure. It entails that the data is only accessible to those who are authorised to use it, as well as no informations is revealed to unintended ones. Data encryption & Confirming Biometrics are great illustration of keeping information private

2.3 Integrity

The particularity of being full or complete is appertained to as integrity. This principle assures that the data is precise, dependable and safe from unwanted trouble actors or unintentional stoner revision.

2.4 Availability

This approach ensures that information is constantly available and helpful to its authorised druggies. It guarantees that authorised druggies have fast, reliable access & there should not be notices like as Denial of Service (DoS) .

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 2, June 2022
Impact Factor: 6.252

III. METHODOLOGY

Tools and Techniques Used in Cyber Security

1. **Password Security:** This technique verifies the user's credentials like Username & Password and stores in the security domain.
2. **Authentication:** In this, authentication of data takes place. Before downloading any documents, we check whether the data is from genuine source or not. Process of authentication is done by using Anti-virus software.
3. **Firewalls:** Firewalls play vital role in securing our networks. A firewall is a software program application or piece of hardware that helps display out hackers, viruses, and worms that attempt to reach your pc over the Internet. All messages entering or leaving the net bypass via the firewall present, which examines each message and blocks these that do now not meet the precise safety criteria.
4. **Anti-Virus Software:** Antivirus software program is a computer program that detects, prevents, and takes motion to disarm or remove malicious software programs, such as viruses and worms. Most antivirus applications include an auto-update function that allows the program to down load profiles of new viruses so that it can test for the new viruses as quickly as they are discovered. An anti virus software program is a must and primary necessity for each and every system.
5. **Malware Scanners:** This is software program that usually scans all the documents and documents current in the gadget for malicious code or harmful viruses.
6. **Digital Signatures:** This is a numerical or mathematical technique which validates the authenticity and integrity of a message, software or digital files.

IV. CONCLUSION

Cyber security has became one of the most important aspects in our digital era. Risks of cyber threats are increasing continuously. So, It is critical to know how to apply it in order to protect our digital data & computer networks.

The upcoming of cybersecurity will in one intelligence be like the current: challenging to describe and potentially limitless as digital competencies have interaction with humanoid throughout in fact all features of policies, society, the family, and outside.

Computer safety is a substantial subject matter that is becoming more vital due to the fact the world is becoming fairly interconnected, with networks being used to carry out indispensable transactions. The cutting-edge and disruptive technologies, along with the new cyber tools and threats that come to mild every day, are difficult companies with no longer solely how they impenetrable their infrastructure, however how they require new systems and talent to do so.

REFERENCES

[1]. https://www.bitdegree.org/tutorials
[2]. https://cltc.berkeley.edu/
[3]. https://www.codecademy.com/learn/introduction-to-cybersecurity
[4]. http://www.crossdomainsolutions.com/cyber-security/tools-techniques/
[5]. https://www.careerera.com/blog/what-is-the-goal-of-cyber-securityeducba.com/what-is-cyber-security/
[6]. IEEE Security and Privacy Magazine – IEEECS "Safety Critical Systems – Next Generation "July/ Aug
[7]. 2013.
[8]. Mrs. Ashwini Sheth, Mr. Sachin Bhosale , Mr. Farish Kurupkar (2021)RESEARCH PAPER ON CYBER SECURITY G.NIKHITA REDDY , G.J.UGANDER REDDY(2014) A STUDY OF CYBER SECURITY CHALLENGES AND ITS EMERGNING TRENDS ON LATEST TECHNOLOGIES
[9]. Saloni Khurana(2017) A Review Paper on Cyber Security
[10]. Tim Weil(2020)IT Risk and Resilience— Cybersecurity Response to COVID-19 Susan Konyeha(2020) Exploring Cybersecurity Threats in Digital Marketing
[11]. Adamu Abdullahi Garba , Aliyu Musa Bade , Muktar Yahuza , Ya'u Nuhu (2020)Cybersecurity capability maturity models review and application domain
[12]. Simon Vrhovec, Damjan Fujs, Luka Jelovˇcan, Anˇze Miheliˇc (2020)Evaluating Case Study and Action Research Reports: Real-world Research in Cybersecurity