e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:04/Issue:08/August-2022 Impact Factor- 6.752 www.irjmets.com

CYBER SECURITY: THE NEW ERA OF PROTECTION

Srinjoy Saha[*1], Sanhita Kar[*2], Chayantika Roy[*3], Sneha Nej[*4], Meghna Das[*5], Soumita Mullick[*6], Debrupa Pal[*7]

[*1,2,3,4,5,6]BCA IInd Year, Department Of Computer Application, Narula Institute Of Technology, Kolkata, West Bengal, India.

[*7]Debrupa Pal, Assistant Professor, Department Of Computer Application, Narula Institute Of Technology, Kolkata, West Bengal, India.

ABSTRACT

In today's technological world securing the information is become one of the toughest challenges. So that's why in IT (Information Technology) field cyber security plays a significant role and its goal to protect our Internet-connected systems, including hardware, software, and data from cyber-attacks. So, this paper mainly focuses on the cyber security and the techniques that we can use to protect our device. Apart from this, it also focuses on cyber-crime, types of cyber-attack, cyber security goals and ethics.

Keywords: Cyber Security, Cyber-Crime, Security Techniques, Cyber Ethics, Ransomware, Iot.

I. INTRODUCTION

Now days Cyber security is the most concerned matter as day-by-day cyber threats and attacks are overgrowing. Today a huge percentage of commercial transactions are done online and many more sensitive informations are passing through online, so this field requires a high range of security. Hackers and attackers are becoming smarter and more creative with their technique to attack the systems. So now all IT or non-IT firms have understood the importance of Cyber Security.

II. CYBER CRIME

Cybercrime is a criminal activity that uses a computer or a networked device as tools. In other words, it refers to any illegal activity carried out using computers or the internet. A group of high skilled computer experts (often called 'Hacker') is considered to be the culprits of such crimes. Unfortunately, these culprits utilize their skill in an evil way that can ruin everything. Cybercrime may harm someone's security and also the financial health [1].

Table 1: Some of the latest cyber-attacks (April,22 – June,22)

Date and place	Crime Information
15th April,2022 Chennai	The cybercrime department of the Chennai police arrested six people for cheating Rs 79 lakh.
12th May,2022 Kolkata	Bidhannagar cybercrime police arrested fifteen men for New Town call center fraud.
23rd May,2022 Hyderabad	Cybercrime department of Hyderabad filed a case of extortion after a techie using a dating app was blackmailed by a woman met online.
2nd June,2022 Mumbai	A 26-year-old Airoli (a residential and commercial area of Navi Mumbai in the Indian state of Maharashtra) woman has become a victim of cyber fraud and loses Rs 23,000.
29th June,2022 Bengaluru	A 51-year-old doctor loses Rs 1.6 Lakh while trying to purchase cement sacks via online.

CLASSIFICATION OF CYBER CRIME: Cybercrimes further classified into 4 major categories as following the below:

Cybercrime Against Individual: Cybercrimes committed against persons or individual include various crimes like transmission of harassment using e-mails and cyber-stalking. Posting and distributing obscene material is one of the most important cybercrimes known today.

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:04/Issue:08/August-2022 Impact Factor- 6.752 www.irjmets.com

- Cybercrime Against Property: Cybercrimes against all forms of property include credit card fraud, intellectual property crimes include software privacy like Illegal copying of programs, distribution of copies of software and copyright infringement like using copyrighted material without proper permission[2].
- Cybercrime Against Organization: Cybercrime against organization mainly includes unauthorized access of computer, password sniffing, malware attacks, network intrusions. Cyber-attacks can also damage the business reputation and trust of customers. This could potentially lead to loss of customers and loss of sales.
- Cybercrime Against Society: Cybercrime against society includes trafficking in intellectual property, stealing identities, or violating privacy and use of computer resources to terrorize people and carry out the activities of terrorism etc[3].

III. TYPES OF CYBER ATTACKS

Nowadays, there are many varieties of cyber-attacks that can damage a computer system, network or infrastructure. If we know the various types of cyber-attacks, it becomes easier for us to protect our networks and devices. Some of the well-known techniques are –

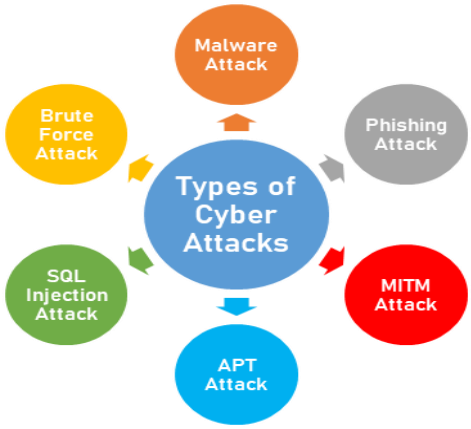

Figure 1: Types of Cyber Attacks.

- Malware Attack: Malware is short for "Malicious Software", it is one of the most common cyber-attack where malware developed by cybercriminals to steal or delete data and exploit any programmable device, server, client or network. After downloading any suspicious attachments online, user's system could have gotten corrupted by certain malicious viruses embedded within the attachments. Example of common malware include Trojan horses, spyware, worms, adware etc[4].
- Phishing Attack: Phishing is a social engineering cyber-attack where the hacker usually sends fraudulent emails that appear to be coming from a reputable source. This is done to install malware on the victim's infrastructure or to steal sensitive data like credit card information and login credentials.
- MITM Attack: A man-in-the-middle (MITM) attack is a type of eavesdropping attack where the hacker gains access to the information path between user's device and the server. The hacker's computer takes over an IP address, by doing so the attacker secretly intercepts and relays messages between two parties. This commonly happens with unsecured wi-fi networks and also through malware[5].
- APT Attack: Advanced persistent threat (APT) attack is a carefully planned and designed cyber-attack where continuous and sophisticated hacking techniques are used by a group of skilled hackers to gain unauthorized access to a computer network and remain undetected for a prolonged period of time.
- SQL Injection Attack: SQL injection is also known as SQLI, it is a code injection technique that hackers use to gain unauthorized access to sensitive data, such as passwords, credit card details or personal user information. By using this, malicious SQL statements are inserted into an entry field for execution. After that, hackers can view, edit and delete tables from databases.
- Brute Force Attack: A brute force attack is a hacking method where hackers try to guess the login info, credentials and encryption keys by using trial-and-error approach. In this type of attack, hackers try to work out all the permutations and combinations of passwords of the victim. It is also used for discovering hidden web pages.

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:04/Issue:08/August-2022 Impact Factor- 6.752 www.irjmets.com

IV. CYBER SECURITY GOALS

The cyber security goal is to provide a risk free and secure environment in which data networks, and devices can be protected from cyber-attacks[6]. The purpose of cyber security is to protect information from theft, compromise or attack. Cyber security can be measured by at least one of three goals-

- Protect data privacy.
- Protect data integrity.
- Promote data availability to authorized users.

These goals from the Confidence, Integrity, Availability (CIA) triad, which is the foundation of all security programs.

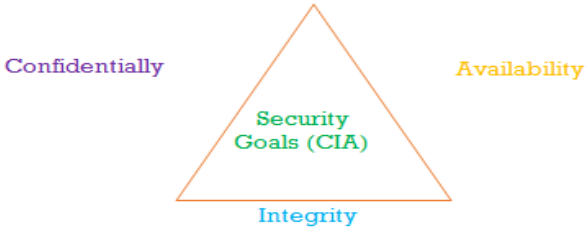

Figure 2: The CIA triad.

A) Confidentiality: Keeping sensitive information private. Tools of confidentiality-

- Encryption
- Access control
- Authentication
- Authorization
- Physical security

B) Integrity: It is data, network and system continuity. Tools of Integrity-

- Backups
- Data correction codes

C) Availability: Authorize refers to users who can freely access the systems, networks and data they need to perform their daily task. Tools of Availability-

- Physical protection
- Computation redundancies

V. CYBER SECURITY TECHNIQUES

Cyber security is an important part of any business. There are many types of cyber security techniques. Some of them are described below:

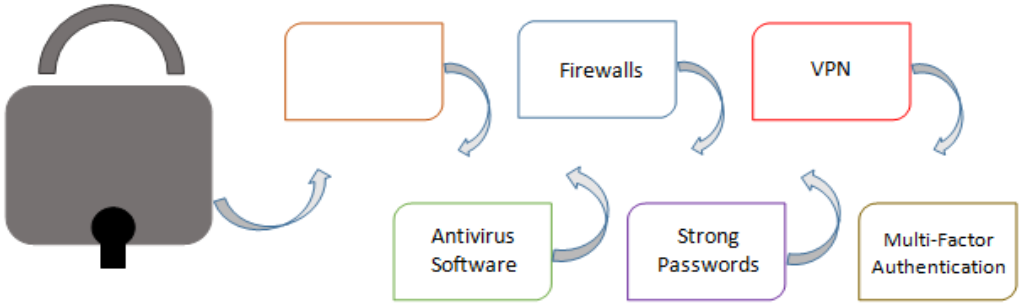

Figure 3: Cyber Security Techniques.

- Software Update: Software updates are not only just getting the latest features but also about a lot more features for our device or computer. There are some important updates that allow us to keep our device safe from cyber threats. So, we should keep our software up to date.
- Antivirus Software: Viruses can come from multiple sources and can cause harm to our system, as well as allow unwanted third-party access. Antivirus software scans, detects, prevents and deletes viruses on a device or computer system.

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:04/Issue:08/August-2022 Impact Factor- 6.752 www.irjmets.com

- Firewalls: A firewall is a security program that creates a gate between our device and the internet. Using firewall is also important when defending our data against malicious attacks. Windows and Mac OS come with their respective firewalls vastly named Windows Firewall and Mac Firewall.
- Strong Passwords: Strong passwords are critical to online security. Passwords are important in keeping hackers out of your data. Verizon's 2019 Data Breach Investigations Report found that 80% of all hacking related breaches are the result of weak passwords. We should consider our password the crazy, complex, mixture of uppercase letters, symbols and numbers. We shouldn't use same password twice. We can also use a password manager to keep track of all our passwords.
- VPN: Using a public wi-fi without using a VPN (Virtual Private Network) is risky. A VPN is a great tool when working outside our secure office network and it allow us to safely transmit and receive data. By using VPN software, the traffic between our device and the VPN server is encrypted. This means it's much more difficult for a cybercriminal to obtain access to our data on our device.
- Multi-Factor Authentication: Multi-factor authentication (MFA), or two-factor authentication, adds an extra layer of security to a standard password. According to NIST, an SMS delivery should not be used during two-factor authentication because malware can be used to attack mobile phone networks and can compromise data during the process.

VI. CYBER ETHICS

Cyber Ethics refers to the basic ethics and etiquette that must be followed while using a computer system. Cyber Ethics is the ethics applied to the online environment.

Importance -

- To promote moral and social values in society.
- To protect personal & commercial information such as login & password, credit card and account information. It also controls unwanted internet main and ads (Spam).
- To suppose dishonest business practices and to protect and encourage fair competition.
- Controlling plagiarism, student identity fraud and use of copyrighted material etc.
- To make ICT easily available to all people including the disabled and deprived.
- Never share your personal information with anyone as there is a good chance that others will misuse it and eventually you will run into a problem.

VII. CONCLUSION

In today's IT world cyber security is one of the most important things for securing the high internet penetration as cybersecurity threats are harmful to the country's security. Several scientific researches preserve their precious documents with code security locking. The fear lies as such locks are decoded by those cyber criminals who hack everything leaving the store empty. The threats of it are really hard to deny, so it is important for us to learn how to defend our IoT (Internet of Things) devices from these attackers. Cyber-crimes are continuously spreading, for protecting the cyber or the internet, there are some security tools which are used in corporate world. Not only government and IT companies but also people should be aware about proper use of anti-virus for virus and malware free network security system.

VIII. REFERENCES

[1] Cyber Security: Understanding Cyber Crimes – Sunit Belapure Nina Godbole.
[2] A Look back on Cyber Security 2012 by Luis corrons – Panda Labs.
[3] Foundations of Computer Security – David Salomon.
[4] The Art of Invisibility – Kelvin Mitnick.
[5] Network Security: A Hacker's Perspective – Ankit Fadia.
[6] Social Engineering: The Science of Human Hacking – Cristopher Hadnagy.