International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Assessing Vulnerability and Emerging Trends in Cyber Security: A Survey

Bibin John[1], Jay Uchagaonkar[2]

[1,2]Department of Information Technology, St. Francis Institute of Technology, Mumbai- 401103, India
bibinjohn21@student.sfit.ac.in[1], uchagaonkar54jay@student.sfit.ac.in[2]

ABSTRACT-

Cyber security concept deals with the procedure of defending computers, mobiles, electronic devices, data and network from cyber attacks. These attacks are usually directed at altering, or distorting sensitive information; coercing users for money; or interrupting processes. Cyber security can be described as the process, technologies, and methods to help preserve the integrity, confidentiality of systems, data and network, against cyber-attacks. The main purpose of cyber security is to protect all important organizational assets from both internal and external threats as well as disruptions caused due to natural causes. It can be prevented by being acquainted with the various tools & resources, types of protocols, etc. In addition, people should know the preventative measures to protect our systems. All our highly sensitive information is of great value to hackers which is why it is important to protect it using strong cyber security measures. This technical paper examines the main definition equipment for the term 'cyber resilience' by trustworthy sources.

Keywords- Cyber Security, Cyber attacks, Cyber crimes, Malware, Virus, Phishing, Encryption

I. INTRODUCTION

In today's era, human lives have been greatly integrated with the digital world. It is possible to send and receive any form of data i.e an e-mail or an audio or video just by the click of a button. While transmitting this data, the fact that how secure data is, would have crossed our minds. The solution lies in cyber security. As global usage is increasing rapidly, with over 5 billion users across the world, this field requires a high quality of security for achieving transparency and safe transactions. The scope of this field is boundless such as securing the data in the IT industry but also used in various other fields like cyber space etc. Even the latest concepts like cloud computing, mobile computing, net banking etc also require high level security. Since these technologies contain some important information regarding any person, securing it has become essential. The main objective is to protect the devices using various protocols and to establish various measures against cyber attacks. There are various approaches that are used to prevent cyber attacks and thereby enhance security for devices. With the rise of online activities and applications, cyber-attacks are increasing day by day. To secure the devices, cyber safety technologies have been developed. Cybersecurity is the method for defending internet-connected devices and services from malicious attacks by cybercriminals, hackers, and spammers. This practice is used by various institutions to protect against ransomware attacks, phishing plots, identity theft, digital espionage and financial losses.

In today's world, it can be observed that our day-to-day lives are very much dependent on technology. Their benefits range from instant access to information on the net to the latest applications and concepts like the Internet of Things. This paper mainly focuses on challenges faced by cyber security while using the latest technologies. The surveyed paper also focuses on the latest trends in the field of cyber security.

II. LITERATURE REVIEW

Cyber Security is the collection of instruments, strategies, security concepts, suggestions, measures, instructions, and technologies that could be useful while safeguarding the cyber environment, firm, and user resources. To oppose the threats of cyber-attacks, authorities need to encourage security top applications and to acquire security technology. [1] Hackers could possibly acquire easy access to data processed using big data technologies unless an effective cyber security in big data is achieved [4]. Cyber security is an issue that affects everyone throughout the world. Hackers are getting savvy and are devising new ideas to create harmful software for abusing data of businesses, individuals and governments. Regardless of requisite security precautions, cyber-attacks [1] are on the rise. As long as these people stay careless and unaware, their position in enhancing cybersecurity, the country of cybersecurity will stay weak[1]. An approach for tracking social data that can be used to launch cyber-attacks is presented in the reviewed paper[5].

In public opinion, cyber security is frequently confused with other ideas such as privacy, information exchange, intelligence collecting, and surveillance. People from various professional backgrounds work in this field [3]. While recent attacks have become more advanced and targeted to specific individuals based on the hacker's goal, such as espionage, financial gain espionage or retribution, opportunistic untargeted attacks are still common. "Opportunistic attacks" are defined as attacks that target victims based on their vulnerability to attack[4]. Cyber crime can manifest itself in the form of cyberbullying and online harassment, which are referred to as cyber enabled crimes, or through security risks that affect the entire system, such as ransomware infections, malware infections and theft and misuse of personal data, which are referred to as cyber dependent crimes [3]. One of the articles that this paper took into consideration mainly focuses on whether there is a violation in the accessible study of the cyber domain and the required skills for the top-notch work of cyber security. The main theme was to focus on the background arena which actually ensures cyber safety. This type of criminality has been tremendously costly to the economy, with estimations of around $575 billion lost annually across the globe, according to the report. An in-depth examination of various cyber crimes in India has been conducted in this article. According to the author, fraud cases are on the rise, with the majority of victims being in the age limit of 20 to 29. As a result, awareness campaigns are essential in India to prevent or minimize cyber crime [3]. This technical paper is conducting a deep analysis on the current situation on cyber attacks and tools for its prevention.

III. STATISTICS

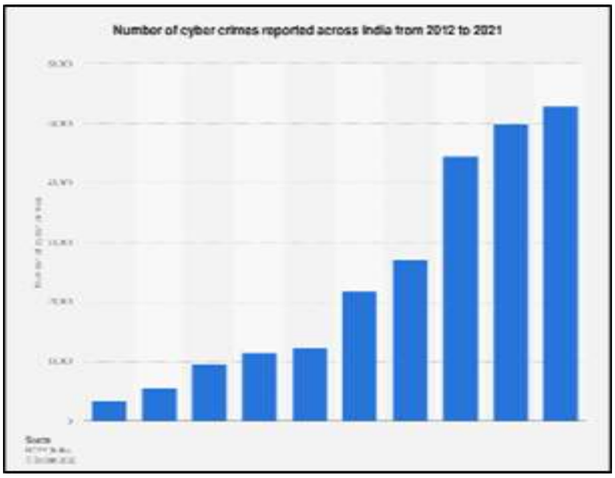

Fig. 1. Recent trends on cyber crimes[7]

The above graph has the information regarding the cyber crimes reported in India from 2012-2021. It can be observed that India saw a notable rise in cyber crimes in 2021. In the same year,over 52,000 cyber crime incidents were registered where the two states Karnataka and Uttar Pradesh accounted for the highest share during the measured time period. It was stated that in 2017, the market in India collectively lost over 18 billion U.S. dollars due to cyber attacks. In a country like India, it is highly likely that these figures could be under-reported due to a lack of awareness about cyber crime and the mechanisms to classify them accordingly. Recent government initiatives such as a dedicated online portal to report cyber crimes could very well be the main reason behind a sudden spike in online crimes reported from 2017 onwards.[6]

India reported 52,974 cyber crimes in the year 2021, i.e a growth of around 6% from the previous year. Nearly 1,500 cybercrime cases are reported every day, of which only 30 are reported to the cyber cell,which is just 2%. The situation of those arrested for those crimes remains the same. Cyber cells across the country had a total of 94,770 cases in 2019 and 2020 and only 23,363 of those had chargesheets filed.

Even among the cases that completed litigation, the rate of sentence stood at just 42.5. Out of the 1,155 cases that completed trial in 2021, only 491 concluded in a conviction. Meanwhile, 591 cases, which is greater than half of the total, ended in an liberation and another 87 cases got released. The national capital in 2021 observed a 111 % increase in these crimes as compared in the year 2020 ,with the NCRB data mentioning molestation to be the cause behind maximum number of cases.[6]

According to the National Crime Records Bureau(NCRB) data for the year 2021, most of these crimes involved internet fraud, online harassment, publication of explicit content etc.

IV.CYBER ATTACKS AND ITS TYPES

A cyber attack is launched by cybercriminals using one or more computers against one or many computers or networks. It can maliciously disrupt computers, steal data, or use a breached computer as a launch point for other attacks.

Following are the various types of Cyber Attacks:

A: Malware Attack

Malware attacks are one of the most frequent types of attacks.the word itself cites to malicious software viruses like worms,trojans,worms,spyware,etc.

In this type of attack the malware or the virus breaches a network through some vulnerability where when the user clicks an unsafe link, it gets downloaded in the computer as an email attachment which harms the computer in many ways like corrupting the data of the computer and also like sharing personal information of the computer with the attacker.

B: Phishing Attack

Phishing attacks are the most well known cyber attacks. In this type of attack the attacker enacts to be a trusted contact of the victim where he/she sends bogus mails where the victim gets trapped in these types of mails.

Innocent victims get trapped in these types of mails where he/she clicks on the malicious link or opens the mail attachment,through which the attacker gets to gain the access of the confidential information and account deatils.By using this type of phishing attack an attacker can also set up a malware in the victim.

C: Password Attack

The password attack deals with cracking the password of the user,wherein the attacker cracks the password to access the confidential credentials of the victim.The attacker uses tools like Hashcat,Cain,Aircrack,etc.

There are various types of password attacks those are as follows:

- Brute force attacks
- Dictionary attacks
- Keylogger attacks

D:SQL Injection Attack

SQL stands for Structured Query Language.A SQL injection attack occurs on a website having a database when the attacker manipulates a SQL query. By injecting a malicious code into a vulnerable website search box, the attacker makes the server reveal crucial information. which results in an attacker getting access to the database and being able to view, edit, and delete tables in the databases.As a result also these attackers can also get administrative rights through this.

E: Cryptojacking

This type of attack takes place when the attackers access someone else's computer for stealing cryptocurrency. This is done by accessing a website or by manipulating the people to click on a malicious link.

These types of attackers use online advertisements with a javascript code attached to it,where this code actually is made to steal the cryptocurrency from the user.

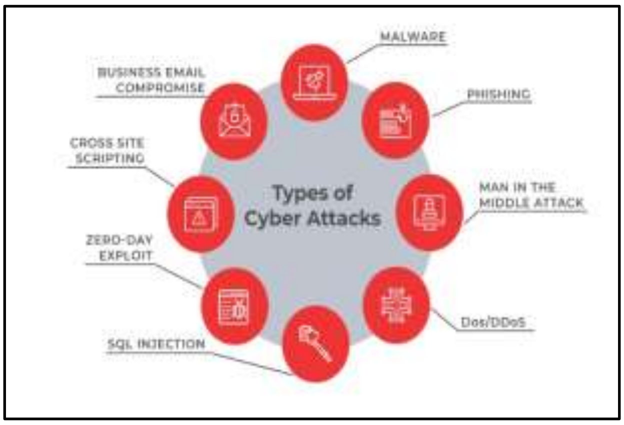

Fig. 2. Types of Cyber Attacks[6]

V. CYBER SECURITY TOOLS

Protecting devices from cyber attacks is very critical. People need to take cybersecurity more seriously. In the virtual world, some of the real security threats faced in the virtual world include hacking, malware, viruses,etc. It is essential that every business is fully aware of the various security challenges and it is necessary to keep themselves secure.

There are many different aspects of cyber defense that need to be considered. Cybersecurity Analysts use various tools in their jobs, which can be categorized into following types: Network security monitoring, Encryption, Web vulnerability, Penetration testing, Antivirus software, Network intrusion detection, and Packet sniffers.

A. Network security monitoring tools

Network security monitoring tools refers to the tools designed to ensure the protection and integrity of a system. There are various types of network security tools out there, with each one having a separate and specialized purpose. These tools allow us to perform real-time network monitoring, advanced access control and prevent data leakage. The aim of these tools is endpoint security i.e. a place where machines display their network information. Argus, Splunk, and OSSEC are few examples of this category.Splunk is a SIEM tool that gathers, analyses, and corresponds to large amounts of network and machine data whereas OSSEC is a free software open source Host-based Intrusion Detection System (HIDS). *Encryption*

Encryption is the method of sending data in a way that can't be accessed by third parties. The information is delivered through a very complex algorithm running on both ends. Encryption software uses a key or string which is made up of numbers to lock and unlock data. It protects data by scrambling text so that it becomes unreadable to unauthorized users. Utilizing encryption software, for instance a password manager which generally uses high-quality encryption, and makes it inaccessible to the unauthorized user. This helps to safeguard sensitive data but also allows us to access it whenever you want. This software helps protect computer systems and networks from cyberattacks and helps maintain user confidentiality. Examples include AxCrypt and VeraCrypt. AxCrypt is a file encryption program. With a single click, it can encrypt a file, a large folder or a collection of files using advanced encryption standard-256 or AES-256 file encryption whereas VeraCrypt is an open-source program that runs on multiple operating systems. It conceals encrypted data twice, using a single encryption key. As it is an open-source tool, there is an option to also change or upgrade the tool whenever you want.

B. Antivirus software

Antivirus is a tool that is designed to detect, protect and remove viruses on digital devices. Originally, it was created to remove computer viruses, but now it has become a general term to describe software that uses advanced technologies to protect against a variety of threats, including spyware, and even never-before-seen zero day attacks. This software is designed to find viruses and other malware, including ransomware, worms, spyware and trojans. Examples of tools include Norton 360, Bitdefender Antivirus, and McAfee Total Protection.Norton and Bitdefender are amongst the most popular antivirus products out there, with both products reaching millions of consumers all around the world. Norton's protection is based on machine learning, which leads to excellent malware detection rates.

C. Packet Sniffers

Packet sniffers are applications that read data packets traversing the network within the Transmission Control Protocol also known asInternet Protocol layer. These tools are used to sniff internet traffic in real-time, monitor the data and on its basis, evaluate and diagnose performance problems. However hackers can use packet sniffing to conduct unauthorized monitoring of our internet activity. Packet Sniffers will help the administrators to monitor their network. It will also help us to detect the reason for a network issue, troubleshooting network issues, traffic analysis, network security & bandwidth management. Examples of tools include Wireshark, Tcpdump, and Windump. Wireshark has many uses, which includes reviewing networks that have performance issues. IT Professionals often use Wireshark to trace connections, view suspected network transactions and identify bursts of network traffic whereas Windump is a classic network protocol analysis software with Unix version named tcpdump. It is used to capture all data packets between two devices and checked for intrusion detection by analysts.

VI. CHALLENGES & SOLUTIONS

With the advent of digitalization, there is a significant rise in cyber crimes being registered. Union Minister of State for Electronics and Information Technology informed the Parliament that around 13.91 lakh cyber security incidents were reported in the year 2022. When we consider the legal framework concerning Cyber law in India, the IT Act 2000 forms the parent legislation that covers various forms of cyber crimes, its compliances and punishments to be inflicted thereby. However, there are some judgements that have evolved the Cyber Law jurisdiction to a great extent.

Recently, India's premier medical institute AIIMS Delhi was the subject of a major cyberattack in November 2022 which paralyzed overall operations at the institute. It was reported that as many as five servers of AIIMS Delhi were impacted in the incident and 1.3 Terabytes (TBs) of data was encrypted by the attackers. As per a report, cyberattacks on Indian govt agencies more than doubled in 2022. Sub-standard firewalls are deployed to protect user data in many cases, yet both state and non-state actors are looking to exploit vulnerabilities in the system.

Even though authorities are trying to curb such attacks, it's the user's responsibility too to safeguard critical data. Even if we don't have expensive cybersecurity solutions, we still can follow some basic steps such as using a firewall before going online. Using antivirus programs can protect our devices against unauthorized software that may threaten our system. Along with it, anti-spyware packages can provide real time protection by scanning all information and blocking threats. Make sure to use complex passwords, more secure often means longer and more complex. Avoid using recognizable words or combinations such as birthdate or other information connected to you. It is a good practice to always install new updates to the operating system and keep your apps up-to-date. Remember to backup your information periodically to avoid any data breach or loss. Other safe practices include using virtualization, securing your network, using two factor authentication and not using unsecured public Wi-Fi.

In case an individual becomes a victim of these cyber crimes then they should remain calm and should also understand that these things happen in today's digital era and they are not alone in this situation. National Cyber Crime Reporting portal (Helpline No. - 1930) is used to register complaints against cyber crimes where the victim can register a complaint regarding the incident. The victim should immediately register a complaint regarding the incident and should not delay any further.

VII. CONCLUSION

The term cyber security is something which is becoming more and more dominant lately, as the world is becoming highly interconnected to each other and also with networks being used to carry out lakhs of transactions in seconds.So, it becomes very much important to secure these types of transactions. Also the data of an individual also becomes an important aspect in today's technological world. The surveyed paper has reviewed all the basic aspects of cyber security, how cyber attacks are undertaken, need for cyber security and the basic concepts of cyber security tools. The paper analyzes the current trends of cyber crimes around the world, especially India. The current study shows that the number of cyber crimes reported is increasing rapidly. An cyber attack, particularly if carried out by a skilled and experienced hacker, may consist of repeated stages. Understanding the types of attack, and the stages involved, will help to better defend individuals. Some people consider cyber security a complex topic, but we made it our priority to explain all important concepts in an effective manner. People are not aware of the various types of cyber crimes and ways to prevent it. In this paper, all the basic classifications of cyber attacks have been covered with proper examples. The surveyed paper has presented an overview on various cyber tools at our dispensation such as encryption tools, anti-malware and antivirus softwares.

VIII. REFERENCES

[1] A. Verma, R. Surendra, B. S. Reddy, P. Chawla and K. Soni, "Cyber Security in Digital Sector," 2021 International Conference on Artificial Intelligence and Smart Systems (ICAIS), Coimbatore, India, 2021, pp. 703-710, doi: 10.1109/ICAIS50930.2021.9395933.e

[2] Igor Skrjanc, Seiichi Ozawa, Tao Ban and Dejan Dovzan, "Large-scale cyber-attacks monitoring using Evolving CauchyPossibilistic Clustering" in Applied Soft Computing, Elsevier, vol. 62, pp. 592-601, 2018

[3] N. Virvilis, A. Mylonas, N. Tsalis and D. Gritzalis, "Security Busters: Web browser security vs. rogue sites", Comput. Secur., vol. 52, pp. 90-105, 2015

[4] Dr. Yusuf Perwej, Kashiful Haq, Firoj Parwej, M. M. Mohamed Hassan ,“ The Internet of Things (IoT) and its Application Domains”, International Journal of Computer Applications (IJCA) ,USA Volume 182 – No. 49, April 2019

[5] https://blog.ecosystm360.com/cyber-attacks-threats-risks/.

[6] Types of cyber crimes available online at https://www.statista.com/statistics/309435/india-cyber-crime-it-act/

[7] Graph on Number of Cyber Crimes recorded across India: Mrs. Ashwini Sheth1 , Mr. Sachin Bhosale2 , Mr. Farish Kurupkar,. “Research Paper on cyber security" Contemporary Research in India (ISSN 2231-2137):Special Issue:April,2021

[8] H. Arora, T. Manglani, G. Bakshi and S. Choudhary, "Cyber Security Challenges and Trends on Recent Technologies," 2022 6th International Conference on Computing Methodologies and Communication (ICCMC), Erode, India, 2022, pp. 115-118, doi: 10.1109/ICCMC53470.2022.9753967.