International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 09 Issue: 04 | Apr 2022 www.irjet.net p-ISSN: 2395-0072

A Comprehensive Review of Cyber Security, Threats and Cyber Attacks

Aditya P. Rajpara[1], Sejal Thakkar[2]

[1]Department of Computer Engineering, Indus University, Ahmedabad, India
[2]Asistant Professor CE Department IITE Indus University

Abstract - Today, cyberspace hosts the majority of economic, commercial, cultural, social, and governmental activity and relationships at all levels, including people, non-governmental organizations, and government entities. In the world of information technology, cyber security is critical. The first thing that springs to mind when we think of cyber security is "cyber-crime," which is on the rise. To tackle cybercrime, several governments and corporations are using several measures. Despite several efforts, cyber security continues to be a major concern for many individuals. Cyber-attacks are an issue for governments all around the world, and protecting sensitive information from them is tough. A variety of companies use a variety of ways to scale back the results of cyberattacks so as to realize this goal. Cyber security monitors real-time data on the most recent IT data. This article will examine the challenges, weaknesses, and strengths of the proposed methods that have been proposed by researchers around the globe to prevent cyber-attacks or reduce the damage caused, as well as the complexities, weak points, and strengths of the proposed techniques that have been proposed by researchers all over the world to prevent cyber-attacks or minimize the damage.

***Key Words*: Cyber-Crimes, Cyber-Attacks, Cyber Security, Cyberspace.**

1. INTRODUCTION

The Internet is the most rapidly expanding infrastructure in modern society. But due to these emerging technologies, we are not able to protect our privacy effectively. As a result, network security has become an issue recently. Making the Internet safer (and protecting Internet users) has become an integral part of the development of new services and government policy. The Internet has created a huge international network that has generated billions of dollars annually for the world economy. Diverse parts of citizens' lives are connected with this space, and any instability, insecurity, or obstacles in this space will have a direct impact on different aspects of the life of residents. Until governments comes back with a transparent definition of a cyber-attack that's accepted and favored by the international community, it'll definitely be terribly troublesome for consultants to deal with the advanced and numerous dimensions and aspects of the difficulty. The availability of a thorough definition of a cyber-attack will surely have an immediate impact on the legal environment in which to continue and identify the consequences of this type of threats. For decades, the Internet has performed a giant function in worldwide communication and has grown to be more and more incorporated into the lives of human beings all throughout the world. The Internet has created a great worldwide community that has generated billions of greenbacks yearly for the worldwide economy. Most media sports are transferred to this area, maximum economic exchanges are carried out in this area, and a large percentage of residents' time and sports are spent interacting in this zoneis. Nevertheless, our online world has posed new protection-demanding situations for governments. Our online world has caused robust and vulnerable actors, together with governments, prepared and terrorist corporations, or even people in this area. Cyber threats consist of cyber warfare, cybercrime, cyber terrorism, and cyber espionage. This divides cyber dangers from traditional threats to national security. There are diverse possibilities for intense, and now and then, vast bodily or financial damage. There isn't any doubt that the dearth of a clean and complete definition now no longer obscures the main criminal path. This also leads to variation in interpretation and practice, and, in the end, to the success of sometimes contradictory criminal conclusions. As a result of the importance and necessity of obtaining an appropriate definition, "cybersecurity" can be defined as a strategy for reducing security issues in order to safeguard the reputation of the firm, commercial damage, or economic damage. It is important to note that this is not a one-time process and it's a never-ending process. The owner of the business has to keep everything up-to-date in order for it to stay in compliance with the mandate.

2. FUNDAMENTAL CONCEPTS

The true objective of cybersecurity is to keep your information safe from theft and tampering. Consider three essential cybersecurity objectives in order to do this.

1. The confidentiality of information is safeguarded.
2. Preservation of Information Integrity
3. Restricting access to information to only those who have been approved.

The CIA triad model is intended to guide data security strategies within the confines of a society or corporation. This model is similarly mentioned in place of the AIC (availability, Integrity, and Confidentiality) triad to sidestep the mistake with the Central Intelligence Agency. The CIA

standards are ones that most societies and businesses practice once they have connected a new request, made a record, or when assuring access to information.

Fig -1: CIA Triad

1) Confidentiality

Assuring that your complicated data is only accessible to authorized people and that no information is leaked to undesired parties. If your key is private and will not be shared, who will have access to it? This will jeopardize your confidentiality.

Confidentiality Protection Techniques:

- Encryption of data
- Two-factor or multi-factor authentication
- Biometrics Verification

2) Integrity

Ensure that all of your data is accurate and reliable and that it does not vary from one fact to another during the program.

Methods of ensuring integrity are:

- No one illegal should have access to the records as this violates privacy. As a result, there will be controls for operator contact.
- Appropriate backups must be available in order to return quickly.
- A version supervisor must be present to monitor who has altered the log.

3) Availability

There will be no denial of service messages whenever the operator requests a resource for a section of the statistics (DoS).

The evidence must be accessible in its entirety. For example, if an attacker takes control of a website, it might cause a DoS, which makes it difficult to access.

3. CYBER CRIMES

Any unlawful conduct that involves a computer as its principal means of commission and theft is referred to as cybercrime. The United States Department of Justice has broadened the definition of cybercrime to encompass any criminal behavior that involves the storing of proof stored on the computer. Cybercrimes encompass crimes made possible by computers, such as network intrusions and the spread of computer viruses, as well as computer-based variants of existing crimes, such as identity theft, stalking, bullying, and terrorism, all of which have become important people's and government's concerns. In simpler terms, cybercrime is when someone steals a person's identity, sells contraband, stalks victims, or uses harmful software to disrupt operations. Cybercrime will grow in unison with technology's rising importance in people's lives.

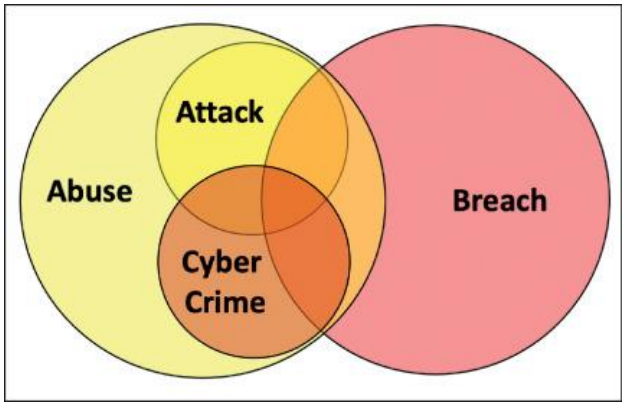

Chart -1: Intersection of attack, crime and breach

4. CYBER SECURITY

Data privacy and security are always the highest security areas of focus for any company. We currently live in a world where every data is digitally saved or stored in cyberspace. On social networking sites, users may interact with family and friends in a secure atmosphere. Cybercriminals will continue to attack social networking sites in order to collect personal information from home users. A person should take all essential security steps not just when using social networking sites, but when using a bank.

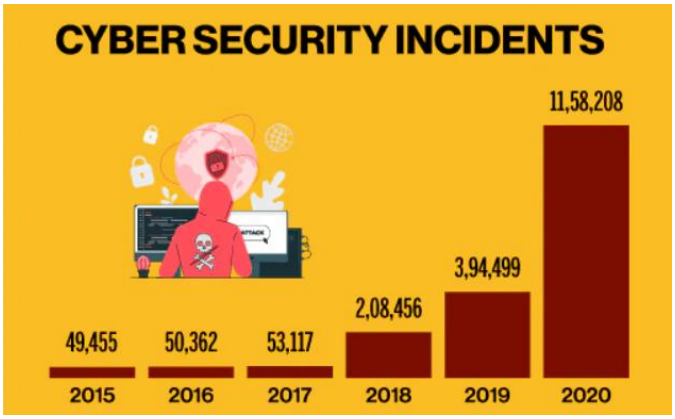

Chart -2: Incidents in cyber security

The comparison of cyber security incidents reported in India between 2015 and 2020 demonstrates the cyber security dangers. As crime rates rise, so, too, do security precautions. According to Silicon Valley Bank's countrywide poll of technology and healthcare professionals, organizations feel cyber assaults pose a severe danger to both their data and their business succession.

1] This year, 98 percent of organizations are maintaining or expanding their cyber security efforts, with half increasing resources committed to online threats.

2] The majority of businesses are planning for cyber assaults when they occur, not if they occur.

3] Only one-third are entirely confident in the protection of their information, and even fewer are confident in their business partners' security procedures.

The number of malware specimens for Macs would continue to rise, but at a considerably slower rate than for PCs. Because Windows 8 will allow users to construct programs for nearly any device (PCs, tablets, and smartphones) running Windows 8, harmful applications similar to those for Android will be feasible; hence, these are some of the projected developments in security.

Network, server, intranet, and computer systems are all protected by cyber-security specialists. To improve your security, you must first understand the different types of cyber security. Malware or hacking are examples of disruptors that can affect a computer network's security. Physical and digital data are protected from unauthorized access, disclosure, misuse, unlawful alteration, and deletion by information security. Organizational security is founded on three fundamental principles: confidentiality, integrity, and availability. Best practices in cybersecurity go beyond these ideas. The lack of qualified workers to undertake the job is a significant barrier in cyber-security. Each plan must be individually devised and implemented for each organization. The conflict between the security situation and the demand for cyber performance is significant. Rapid data flow to cyberspace almost always reduces the overall system's security. For technology professionals who want to prove production, security indicators are often in direct conflict with each other because they reduce, prohibit, or delay user access; In addition, they consume indications that indicate vital system resources and react to managerial attention. The objectives of the applicable regulatory body dictate the substance of the security policy. The national security goals are not the same as the business security goals. It is not ven possible to expect resource providers to adhere to the customer security policy unless a formal contract is in place. In companies, it is common to have a centrally centralized security unit that is responsible for cyber-security policy and related standards and solutions.

5. CYBER SPACE THREATS

Any destructive attack that tries to obtain unauthorized access to data, disrupt digital activity, or damage data is considered a cyber security hazard. Cyber threats include corporate espionage, hacktivists, terrorist organizations, hostile nation-states, criminal organizations, lone hackers, and dissatisfied workers.

In recent years, a number of high-profile cyber-attacks have resulted in the exposing of critical data. For example, the Equifax data breach in 2017 exposed the personal information of approximately 143 million people, including birth dates, addresses, and Social Security numbers. Hackers got access to Marriott International's networks in 2018 and stole the personal information of roughly 500 million customers, according to the company. The inability of the firm to build, test, and retest technological measures like encryption and authentication permitted the cyber security danger in both cases.

6 Types of Cyber Threats

Cyber security experts should be well-versed in the following sorts of cyber security risks.

1. Malware

Malicious software includes spyware, ransomware, viruses, even worms. Whenever a user clicks on a broken link or document, malware is activated and destructive software is installed. As per Cisco, once the virus is activated, it can:

- Critical network components have limited access (ransomware)
- Install more potentially hazardous applications.
- Send data from the hard disc to obtain information without being discovered (spyware).
- Individual parts are disrupted, rendering the system unworkable.

2. Phishing

Phishing attacks employ forged communication, such as an email, to deceive the recipient into opening it and following the instructions contained inside, such as submitting a credit card number. The goal, according to Cisco, is to "collect personal data such as credit card and login passwords or infect the victim's PC with malware."

3. Denial of Service

A denial of service attack floods a computer or network with requests, making it unable to reply. A distributed DoS assault achieves the same result as a single DoS attack, except it originates through a computer network. Cybercriminals typically use a flood attack to disrupt the "handshake" protocol and carry out a DoS. Additional ways may be employed, and some hackers take advantage of the downtime to conduct further attacks. A botnet, according to Jeff Melnick of Netwrix, an information technology security software company, is a type of DDoS in which a hacker may infect millions of machines with malware and control them. Botnets, also known as zombie systems, are computer networks that are designed to assault and overcome a target's processing capability.

4. Man in the Middle Attack

A man-in-the-middle (MITM) attack occurs whenever attackers insert themselves into a two-party transaction. Cisco claims that after stopping transmission, they can filter and collect data. When a visitor connects to an unsecured public Wi-Fi network, MITM attacks are common. After erecting a firewall between both the visitor and the network, the attackers employ malware to download software and steal data.

5. SQL Injection

When malicious code is injected into a SQL server, SQL injection is a type of cyber-attack. Data is leaked when a system is infected. It's as easy as putting the malicious script into a vulnerable website's search field.

6. Zero-day Exploit

The zero-day (0-day) exploit is a cyber-attack that targets a security flaw that the software developer or antivirus suppliers are unaware of. The attacker discovers the software flaw before anybody else is interested in fixing it, writes an exploit, and uses it to launch an attack. Such assaults are highly likely to succeed since no defenses are in place. As a result, zero-day attacks are a significant security concern.

Web browsers, which are typical targets because of their widespread use, and email attachments that exploit flaws in the program that opens the attachment, or in specific file formats such as Word, Excel, PDF, or Flash, are common attack vectors.

6. CONCLUSION

In the third millennium, cyberspace and associated technologies constitute one of the most important sources of power. National security can no longer be defined by the threat posed by citizens' declining quality of life. The second is the removal of cyber threats' geographical component. In the past, cyber-attacks created vulnerabilities to military threats. Cyber threats are intermittent, multifaceted, and multidimensional, and their level of harm is quite high since they are related to critical networks and infrastructure. They cannot be contained only by traditional measures, such as the deployment of military and police power, and governments alone are unable to combat them; strong bilateral collaboration between governments and the private sector is recommended.

"Cybersecurity" surveys increased in the late 2010s. That gesture is more likely to quicken than slow, but its timing varies extensively among our situations. In our undertaking, we left the repercussions of a straight, armed military "cyberwar" to the cross. The purpose of these situations is to provide an opinion on some of the ups and downs that might result. It is clear that cyberwar or at minimum cyber battle will continue to occur because hostilities will erupt, and the internet, like the sea, land, space, and air, is a difficult field. Furthermore, others already have put an inordinate amount of effort into cyber-fighting situations that can be cast off together with this document. We recognize that major warfare between influential conditions fought primarily or even exclusively in cyberspace would be a break that could send a significant amount of the driving forces that we highlight in significant ways. The internet is one of the most complex environments that humans have created, yet it is nonetheless static (for the time being) - an engineering environment made up of numerical machines built and programmed by societies. Acceptance, like satisfaction, is dysfunctional in the situation. Another notion is that downside risks are simpler to envision than upward prospects.

Computer security is a broad issue that is growing increasingly relevant as the world becomes increasingly linked, with networks being used to conduct crucial activities. With each New Year that passes, cyber-crime and the protection of information continue to split along distinct routes. Organizations are being tested not only in terms of how they defend their infrastructure, but also in terms of how they require new platforms and intelligence to do so, thanks to the latest and disruptive technologies, as well as the new cyber tools and threats that emerge every day. Although there is no ideal answer to cybercrime, we should do everything we can to reduce it to ensure a safe and secure future in cyberspace.

REFERENCES

[1] https://www.sciencedirect.com/science/article/pii/S2352484721007289W.-K. Chen, *Linear Networks and Systems* (Book style). Belmont, CA: Wadsworth, 1993, pp. 123–135.

[2] https://www.researchgate.net/publication/352477690_Research_Paper_on_Cyber_SecurityB. Smith, "An approach to graphs of linear forms (Unpublished work style)," unpublished.

[3] https://www.researchgate.net/publication/260126665_A_Study_Of_Cyber_Security_Challenges_And_Its_Emerging_Trends_On_Latest_Technologies.

[4] https://images.squarespace-cdn.com/content/v1/5ef07334254666386ed45a91/1608262717294-MSU10IM5OR3JH523TK7Y/CIA+Triad.png?format=1000w

[5] https://images.app.goo.gl/MgDezi2B9cKtU8H87

[6] https://images.app.goo.gl/Qbr2ydnNKEF7p8Fc8

[7] https://onlinedegrees.und.edu/blog/types-of-cyber-security-threats/

[8] https://www.researchgate.net/publication/331914032_On_Cyber_Crimes_and_Cyber_Security

[9] https://www.slideshare.net/amirkhan452/chapter2docx-251434147

[10] https://www.coursehero.com/file/p5c44ij/These-differences-can-be-characterized-in-terms-of-threats-to-whichever-property/