Cyber Security Issues And Challenges - A Review

Dr C Thiyagarajan[1], Nandhini B[2]
[1]Associate Professor, Dept of Computer Application (MCA)
[2]Dept of Computer Application (MCA)
[1, 2] PSG College of Arts & Science, Coimbatore, Tamil Nadu, India.

Abstract- *Information security now requires the use of cyber security. One of the biggest issues today is ensuring the security of the information. The Internet has unquestionably opened up a new form of exploitation known as cybercrime due to the unfettered availability of free websites. Numerous steps are being taken by both the public and business sectors to control these cybercrimes. Cybersecurity management continues to be a major concern. This study focuses on the different issues with cyber security in the present day. Additionally, it draws attention to developing cyber security technology, ethical issues, and trends that are altering the field's aspects.*

Keywords- Cyber Security, Cyber Crime, Cyber Ethics

I. INTRODUCTION

Almost everyone is aware of the Internet's remarkable expansion. With the click of a button, anyone can send and receive any type of data, including text, images, videos, and audio files. However, the sender has no way of knowing whether the message was sent to the recipient securely without any data leakage. Many modern technologies are part of the rapidly developing internet technology in today's technological environment. However, it is believed that these new technologies are unable to effectively prevent the misuse of private information, which is why cybercrime is on the rise right now. More than 60% of all commercial transactions are now completed online, thus this industry needed a high level of security for the most reliable and transparent transactions. As a result, cyber security is currently a hot topic in the IT industry. The scope of cyber security includes many additional areas, such as cyber space, in addition to only protecting data in the IT business. High levels of information security are necessary for the newest technologies, including cloud computing, green computing, mobile computing, e-commerce, and net banking.

Any illicit action that uses a computer as its main tool for commission and theft is referred to as cybercrime. The concept of "cybercrime" as used by the U.S. Department of Justice has been broadened to include any criminal action that keeps evidence on a computer. The growing list of cybercrimes includes offenses made possible by computers, like network intrusions and the spread of computer viruses, as well as computer-based variations of already-committed offenses, like identity theft, stalking, bullying, and terrorism, which have become major problems for individuals and nations. Cybercrime is typically understood to be any crime performed utilizing a computer or the internet to steal someone else's identity, sell illegal goods, or stalk someone.

Computer science, criminology, economics, engineering, information systems, management, medicine, neurophysiology, psychology, sociology, and other fields all have a stake in cyber security, with the majority of these fields focusing on technical or psychological issues. It allows for talks regarding motivations and behaviors, as well as advantages and disadvantages of cybercrime and security.

On the basis of individual perceptions of their own behaviors toward potential security breaches in both work and non-work environments, people or organizations can drive end-user security behavior through the use of cyber security. The current research on cyber security focuses on three key areas: person behavior toward information security in non-work settings, employee behavior toward information security in work settings, and organization information system security policy (ISSP) compliance and related challenges.

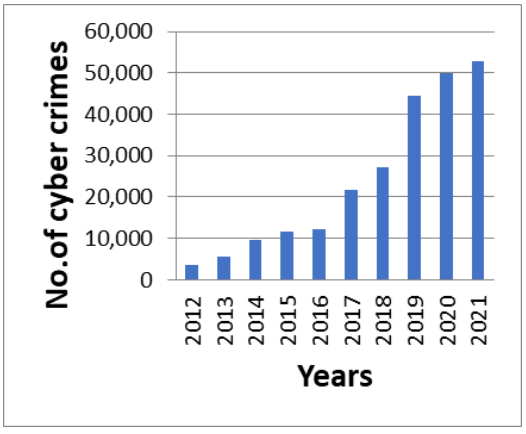

Fig1Crimerateofcyberattacks

II. KINDS OF CYBER ATTACKS

Following are the types of Cyber attacks observed:

1. Denial of Service Attacks(DOS):

The most typical Denial of Service attack comprises a deluge of external communication requests on the target resource.Due to the overload, the resource is either unable to react to legitimate traffic or responds so slowly that it is virtually out of supply. A particular laptop, a port or service on the targeted system, the entire network, a specific network segment, or any system component are frequently the resources targeted during a DoS attack.

Human-system communications and human-response systems may likewise be the subject of DoS attacks. DoS attacks may target specific system resources, such as state information, configuration details, and process resources. Additionally, a DoS attack is frequently created to: run malware that uses up all of the processor, preventing usage; cause errors in the machine's computer code or its order of operations, putting the machine in an unstable state; exploit software vulnerabilities to rob the system of resources; and crash the software completely. The overwhelming resemblance among these instances is that the system in issue responds inconsistently as a result of the Denial of Service assault, and maintenance is either prohibited or severely constrained.

2.Remote to Local Attacks:

In a remote to local (R2L) assault, an attacker sends packets to a system across a network and then uses the machine's vulnerability to gain unauthorized access to the machine on a local level. It occurs when an attacker who has the ability to transmit packets to a system across a network but who lacks an account on that machine discovers a vulnerability and uses it to get local access to that machine as a user.

TCP ACK flood:

Numerous protocol ACK packets are delivered to the victim during this attack in order to take advantage of its system and network resources. An open port or a closed port, depending on the OS, might respond to a protocol RESET message, causing a lot of traffic and effort for the victim and the victim's network. An variation of this attack involves bombarding the target with protocol ACK packets that contain random sequences, random port ranges, and supply information processing that is faked.

3. Signature based Approach:

Mishandling discovery via a signature-based approach functions similarly to current antivirus software. The semantic description of an attack is examined in this method, and specifics are employed to form attack signatures. The attack signatures are set up such that they may be looked up using detailsfrom audit data logs generated by computer systems.

Protocol Flooding:

We were most likely discussing a protocol SYN flood assault whenever we discovered protocol flooding attacks. It is possible to execute a protocol flooding attack without utilizing the protocol's multilateral handshaking, though. Additionally, a protocol flooding attack could be carried out by utilizing several TCP finite states or flags.

Ping of Death:

The TCP/IP specification allows for a maximum packet size of up to 65536 octets (1 computer memory unit = eight bits of data), with the majority of the packet made up of content and a minimum of twenty bytes of scientific header data and zero to several bytes of optional data. It is well known that when some systems receive oversized scientific packets, they can behave inconsistently. According to certain accounts, this behavior is specifically triggered by web management Message Protocol (ICMP) packets sent via the "ping" command.

The "ping" command is used to create large ICMP datagrams (which are encapsulated within a datagram), taking advantage of the fact that many ping implementations send ICMP datagrams that are solely composed of the eight bytes of ICMP header data by default, but allow the user to specify a larger packet size if desired. A criminal sends a victim an ICMP ECHO request packet that is significantly larger than the allowed maximum packet size. The victim is unable to construct the packets because the received ICMP echo request packet is greater than the standard scientific packet size. As a result, the OS may also crash or restart. An assault on a standard TCP/IP implementation could be The Ping of Death.The DoS attacker generates a scientific packet that is larger than the maximum 65,536-byte size allowed by the science standard during this attack. When this large packet finally arrives, it breaks any systems using a weak TCP/IP stack.

Teardrop:

The Teardrop is an earlier attack that still exists and relies on subpar TCP/IP implementation. It operates by

keeping stacks occupied as they piece together science package pieces. The problem here is that while though data packets are typically being split up into smaller pieces, each fragment still has the header and field from the original data packet that informs the TCP/IP stack of how many bytes are inside. This information is used to send the packet back along once everything is in working order. However, with Teardrop, our stack ends up being covered in overlapping science-related fragments. If the stack doesn't comprehend to throw these trash packet fragments out, it will fast fail since once it tries to assemble them, it cannot succeed.

The majority of systems are currently able to handle Teardrops, and a firewall will reciprocally block Teardrop packets for slightly increased network delay since this causes it to ignore all broken packets. Of course, a system will still fail if we have a propensity to bombard it with many Teardrop broken packets. There are numerous varieties available to carry out this kind of attack, including Targa, SynDrop, Boink, Nestea Bonk, TearDrop2, and NewTear.

Land:

A LAND attack consists of a continuous stream of TCP SYN packets with the supply science address and TCP port range set to the same price as the destination address and port range (i.e., those of the attacking host). Some TCP/IP implementations are unable to handle this theoretically impossible circumstance, causing the package to wander in circles as it attempts to resolve persistent connections to itself.

Echo/Chargen:

The person generator (chargen)administration is expected to produce a surge of characters without any problem. It's essentially utilized for testing capabilities. Distant clients/gate crashers will manhandle this help by depleting framework assets. Satirize network meetings that appear to return from that neighbourhood framework's reverberation administration would be ablebe directed at the chargen administration toward structure a "circle."This meeting will make tremendous measures of information be passed in an unending circle that makes weighty burden the framework. Whenever this ridiculed meeting is pointed at a distant framework's reverberation administration, this forswearing of administration assault will cause weighty organization traffic/above that impressively dials back the organization. It ought to be noticed that an assailant needn't bother with to be on our subnet to play out this assault as he/she can manufacture the source locations to these administrations no sweat.

Naptha Attack:

The number and sort of assets that partner miscreant will focus for a refusal of-administration assault square measure a few and differed. The Naptha work features an assortment of them that some particular protections exist. As a rule, any framework that empowers significant assets to be consumed while not certain is sub subject to refusal of-administration assaults.Naptha and comparable organization goes after square measure extra hazardous for some reasons: They can be done "unevenly" - that is, the miscreant will consume tremendous measures of a casualty's confined asset while not equivalent asset consumption. In blend with elective weaknesses or shortcomings, they'll be done secretly. They can be encased in dispersed refusal of-administration devices.

Cyber Morals:

Digital morals are only the code of the web. Rehearsing digital morals are great opportunities to involve the web in a right and safeguarded manner. The underneath are a couple digital morals one should follow while utilizing the web.

Morals 1: To convey and connect individuals with one another with the aide of web. Texts and email connect to remain in associate with the relatives and companions, divide information and data with individuals between the country with the particular association and from one side of the planet to the other.

Morals 2: Web is estimated as world's driving library with data on all the point in a particular branch of knowledge, consequently involving this data in a legitimate and lawful manner is dependably fundamental.

Morals 3: Individuals can't work different people mail account with their passwords.

Morals 4: under no circumstances attempt to send any sort of malware to other's frameworks and make them fraudulent and harm.

Morals 5: Don't share the individual subtleties to anybody as there is a decent chance of different people misusing the mail account lastly that individual should be in an issue.

Morals 6: When the individual is in online don't profess to the next individual and never attempt to make any phony record on a few others as it would turn into a difficulty.

III. CONCLUSION

The new universe of data society with worldwide organizations and the internet will unavoidably produce a wide assortment of social, political, and moral issues. Numerous issues connected with human connections and the local area become clear, when most human exercises are carried on in cyberspace.Some fundamental moral issues on the utilization of IT on worldwide organizations comprise of individual protection, information access freedoms, and destructive activities on the Web. These fundamental issues have been settled somewhat utilizing mechanical methodologies, like encryption strategy, SSL, advanced IDs and PC firewalls. Other than these security advancements, legitimate regulations are likewise required in the internet to address many nations, which are integrated into one worldwide organization. Rules and techniques ought to be carried out so worldwide data can be taken advantage of in a socially and morally delicate way for our future advantage and applications. Network protection is a huge issue that is turning out to be more fundamental on the grounds that the world is turning out to be incredibly interconnected, with networks being utilized to do basic transactions. Everyone has an alternate thought in regards to security strategies and levels of dangers. The key for building a solid organization is to characterize what security need of the time and use. Whenever that has been characterized, all that happens with the organization can be assessed regarding that strategy. Thus it assumes an essential part in data security.

REFERENCES

[1] A. Sternstein, “Pentagon Disconnects iPhone, Android Security Service, Forcing a Return to BlackBerry for Some,” Presented at NextGov, Dec. 3, 2013.
[2] International Telecommunication Union (ITU), “Global Cybersecurity Index (GCI) 2017,2017, https://www.itu.int/dms_pub/itu-d/opb/str/DSTR-GCI.01-2017-PDF-E.pdf.
[3] Chang, L. Y. C. (2012). Cybercrime in the Greater China Region: Regulatory responses and crime prevention across the Taiwan Strait. Cheltenham: Edward Elgar Publishing.
[4] Etter,B. (2001), The forensic challenges of ECrime, Current Commentary No. 3 Australasian Centre for Policing Research, Adelaide.
[5] Etter B. (2002), The challenges of Policing Cyberspace, presented to the Netsafe: Society, Safety and the Internet Conference, Auckland, New Zealand.
[6] Eric J. Sinrod and William P Reilly, Cyber Crimes (2000), A Practical Approach to the Application of Federal Computer crime Laws, Santa Clara University, Vol 16, Number 2.
[7] Seamus O Clardhuanin , An Extended Model of Cybercrime Investigations, International Journal of Digital Evidence, Summer 2004, Vol 3, Issue 1. 2004.
[8] Farmer, Dan. & Charles, Mann C. Surveillance nation. Technology Review; Vol. 106, No. 4, 2003: Pp. 46.
[9] Harrison, A. Privacy group critical of release of carnivore data. Computerworld; Vol. 34, No. 41, 2006: Pp. 24