Review on Cyber Security and Cyber Crimes

Amritpal Kaur[1], Monika Sharma[2]
Mody University of Science And Technology

Abstract*- In today's growing world cyber security is very necessary,as technology provides many services to us, there are some effect also like security threats and cyber attacks. To secure the information from hacker and the cyber attacks we will require the cyber security. Cyber security is a process to secure the networks, computer program and data from the unwanted access or users that goal to access users data for personal uses and benefits. For protection of data many organizations develop a software. These softwares help us to protect the data and information. Cyber security plays a huge role in developing a technology and additional services like internet . Cyber security comes into mind whenever there is hearing about the cyber crimes. This paper describe the cyber security, cyber attacks, types of cyber attacks, and major area in cyber security.*

Keywords- cyber security, cybercrimes, attacks, threat

I. INTRODUCTION

Cyber combines from relating the information, virtual reality and the internet. Cyber security is a necessary process it help in securing data from threats and frauds such as data misuse and theft of personal information, it also safe our system from virus. Cyber security is used for security which is offered through online services to secure our data and information.[1]As the large amount of people are connecting to the internet, security threats are also increased. [6] Cyber security was designed to help learners develop a deeper understanding of modern information and system protection technology and methods. In information technology data security or information security is one of the great challenges for the world[2].Cyber crime has led to the loss of billions of dollars,malfunctioning of computer system, destruction of complex information, the compromise of network integrity and confidentiality.

II. MAJOR AREAS OF CYBER SECURITY

2.1 Cyber crime

cyber crime and computer oriented crime, is crime that involve a computer and a network. [3]Cyber crime is also called computer crimes ,any criminal and illegal activity that includes computer or network connected device. Cyber crime department divide it into three different categories.

- Crimes in which system or computing devices are target for frauds and theft to gain the access in system networks and data.
- Criminal activity in which computer is used as a weapons,for example denial of services(DOS) attacks.
- Crime in which computer is used to store illegal data

2.2 Application security

Application security hold within the measures that are taken in the development of the life cycle to prevent the application from the threats and frouds

Application types are:-

- User Authentication.
- Auditing and logging.
- Input parameter validation.

2.3 Information security

Information security secure the information from unauthorized access and illegal activities to avoid identity theft. Technique used to prevent this:-

- Identification.
- Authentication.
- Cryptography.

2.4 Disaster recovery

Disaster recovery is a technique that involves performing the risk estimate and establishing priorities, developing the recovery strategies in any type of disaster

2.5 Network security

Network security involves the action to secure integrity, reliability, usability and for safety of network. Network security targets a variety of issues and threats and stop them spreading and entering into system and network.

Network security factors are

- Anti virus.
- Firewall, to stop the illegal access to the system and network.
- Intrusion prevention system
- For secure remote access there are (VPN) virtual private network.

3. Cyber Attacks

A cyberattack is carefully using of computer system, technology depends on the networks and activity.[4]Cyber attacks use the damaging code for changing the data or codes, that may results the disturbing in the importance arrangements and leads the cyber crimes,like identity and information frauds(theft).

Cyber Attacks are also called computer network attack (CNA).

Types of attacks in cyber security

3.1 Identity theft

Identity theft is process of obtaining the information illegally about someone else. Thieves and hackers try to stole the information like name, number ,address, password credit card number and email address etc.When hacker stole your personal information then use this information for different purpose like Financial frauds, such as a bank fraud, credit card fraud and the tax rebate fraud.They can use your information for other crimes like entering a country illegally, trafficking drugs, smuggling etc.

Prevention from identity theft

- whenever you are writing or entering any personal information on the server and internet,make sure that connection is secure and private.[7]
- whenever you are purchasing anything from internet, never store your personal information and credit card number on that server and websites.
- A good antivirus is always active in your system.
- Be aware from the fake sites and services.

3.2 Malware

Malware is a combination of mal and ware from the (malicious and software)

Malware is a term used for variety of hazards such as worms, trojans and viruses.malware is defined as a malicious code that theft data or destroy data and information from the system.Malware mostly entered in the system through downloading the software and files online and attachments in the email.

Types of malware

Virus:-

Damages the personal files and information. Spyware:-
Software that will collect the personal information

Worms:-

Malware that can repeat itself across the networks.

Trojans horse:-

Malware that looks and operates as a real program and software.

Browser hijacker:-

Software that modifies the web browser and services.

Prevention from this:-

The one of the best way to stay safe from malware is to avoid clicking on the links, attachments and downloading the files from the unknown services and senders.

3.3 Spyware

spyware is a term which is used to describe and explain the software and files that are intentionally installed on a systems or computer that are used to monitor what others users are doing. It is term designed for get the information secretly about the user activity. These kind of programs are used to monitor and track users choice and habits for better targeting them with the help of advertisements. Spyware is installed into the user system without knowing them.

Prevention from the spyware

The system is affected with the spyware by visiting the infected website, downloading inected software etc.

- Download the data and files from the reputation and well known sites.
- Always maintain the antivirus and anti spyware up to date.

- For the protection and security use the antivirus and firewall.

3.4 Phishing

phishing attacks are attacks that are sent through email or pop messages and they will ask the users for clicking on links and enter their personal information and data.It will attract the user according to their interest and when user click on the link then the hanker will able to enter the system and stole the data and personal information from the system.

3.5 Denial of services

A DOS attack always target on disturbing the services of server and network. Attackers send large amount of data and traffic via a network,unless(until)the server and network become overloaded and stop functioning

The common DOS attacks is DDOS (distributed-denial-of-service) it will also send the high volume data and traffic on services until server and network stop working.

DOS attacks are of two types

- Flooding services
- crashing services .

3.5.1 Flooding services

Flooding attacks are accor when a system found very big amount of traffic on the websites and server to load or buffer cause them slowing down and block or stop ultimately.

Some flooding attacks are:-

- Buffer overflow attack
- Icmp flood
- Syn flood

3.5.2 Crashing services

This type of attacks will target the users system and services for crashing. In that type of attacks takes the advantages of input and data for the sequently crash the system so it will not accessed and used by the users.

3.6 Password sniffing

When hankers not able to guess your password then they try they another method called Password sniffing. In this the attacker use the software and try to access you data and information but the software is running on their own machinen,they are trying to get your password and username when they get the access in it they are able to get access in your system and network.

3.7 Website defacement

Website defacement are the attacks usually done on the websites. These attacks on the websites that cause changes in the appearance of the web pages and sites.It is basically done by hackers and destroyers ,they will replace the webpage and server with their own webpage and site. There are different desaires of attackers which lead to deface the website,one of them is a political motivation.the attackers who do this type of activities are called “hacktivists” they may change the data and text of the webpage with other data,message,content according to their own choice.

IV. CYBER SECURITY TECHNOLOGIES

4.1 Identity management

The username and password both are the big issues in access control.[5]

4.2 Authentication

All the files and documents should be authenticated in their original form, from a secure and trusted source .

4.3 Malware scanner

The system should have a software for scanning the files and documents form malicious code.

4.4 Firewall

Firewall is used for monitoring the traffic of both sides and alert or inform the user from illegal and unauthorized access.

V. CONCLUSION

Cyber threats and crimes are bigger problem to solve especially when they are hidden malicious activities and files. These files not only affect the system and data but also the reputation of the organization and individual, so to prevent the system from illegal activities and theft of personal information, the cyber security is designed. In this paper we have studied the cyber security, and the areas of the cyber security. As we know there are many cyber threats so we also learn about the cyber security attacks and the prevention from them.

REFERENCES

[1] Yadav, shilpashree, tanuarora, yashika, cybercrime and security, volume4, issue8, year 2013.

[2] Vaishnavi J. Deshpande, Dr. Rajeshkumar Sambhe, Cyber Security: Strategy to Security Challenges- A Review, volume3, issue 9, year 2014.

[3] Major area of cyber security and definition of cyber security are retrieved from the review of: https://economictimes.indiatimes.com/definition/cyber-security.

[4] Cyber security attacks are retrieved from the review of : https://www.computerhope.com/jargon/s/spyware.htm.

[5] Ravi Sharma, Study of Latest Emerging Trends on Cyber Security and its challenges to Society, International Journal of Scientific & Engineering Research, Volume 3, Issue 6, June-2012

[6] Cyber security: challenges for society- literature review Atul M Tonge, Suraj S. Kasture , Surbhi R Chaudhari, 2013

[7] Thomas H. Karas and Lori K. Parrott, Judy H. Moore , Metaphors for Cyber Security ,Sandia National Laboratories P.O. Box 5800 Albuquerque, NM 87185-0839.