A STUDY ON CYBER SECURITY AND CYBER CRIMES

S. Shobana[1], Y. Srividhya[2], Mrs. V. Uthra[3]

ABSTRACT

Cyber Security is an activity of safeguarding our personal data, system and networks from illegal access. The main objective of this paper to study cyber security threats and provide some guidelines to safeguard individual data. At present, cybercrimes are increasing at high rate. Cybercrimes are criminal activities committed via internet and steps are taken to prevent them. People who indulge in these malpractices are called hackers and crackers. People must understand that it is difficult to navigate in this cyber world without security. This paper aims at describing different types of hacking and illustrating the importance and challenges of cyber security.

Keywords : cyber threats, cyber ethics, cyber complaints, and IoT

I INTRODUCTION

Cyber Security plays a major role in Information Technology. It is security offered through online service to secure one's online information. We need cyber security nowadays, since along with technology challenges to safeguard private information are also growing. Internet has become a part of life for social communication. internet banking, online shopping and booking of tickets for flight, train, bus etc. in a convenient manner. In this digital era every little thing is digitalized. Hence one should be more conscious of preventing data from unauthorized access and use which may lead to destruction of hardware and software. To solve these types of problem every individual must be trained in cyber security to save him from increasing cybercrimes [1].

II CYBER THREATS

Cyber threats are an illegal act of damaging, stealing or destroying data. Threats like viruses, data breaches and denial of service are some of cyber attacks.[2]

Cyber Security Threats Fig:1

Botnets

A botnet mainly consists of internet- connected devices, each of which runs from one or more bots. The word botnet is a combination of robot and networks. These are mainly used with a negative or malicious connotation. It can be used to steal data, and send spam messages, etc. It accesses the device by allowing the attacker and his connection.

Hacking and cracking

If the computer system is accessed by somebody for destroying or altering information or data, then it is said to be hacking and the person who does this crime is called a hacker. Cracking is less harmful than hacking. Cracking is the same practice of bypassing computer safeguards. To gain access to them, it may be good or bad [3].

[1, 2] II BSc(cs) UG Students
[3] Assistant Professor Department of Computer Science
Sri Ramakrishna College of Arts and Science for Women,

Malware

The word malware is short for malicious software. It refers to some of the programs which are specifically engineered to compromise computer or other devices. In some cases, malvertising can infect the computer with malicious software even when visiting legitimate sites. The main thing in malware is a threat to the deviceand cyber security. There are eight types of malware, namely virus, worm, Trojan, ransomware, adware, spyware, file-less malware. [4]

Viruses

It is malicious program that is spread through email attachment, shared media or downloads with the intention of damaging one's computer as well as the computers in one's contact list.

Worms

Worms are like viruses. The worm of computer is considered as standalone malware computer program, which replicates itself to spread to another computer. Mainly worms often use parts of an operating system, which are automatic. It is invisible to the user. The worms are necessary to become active on an infected system.

Trojan Horses

It is legitimate software. It is mainly employed by cyber-thieves. The examples of Trojan horses are Backdoor, Exploit, Rootkit, Trojan-Banker, Trojan-Ddos, Trojan downloader, Trojan dropper, and Trojan game thief. It will not replicate computers or by infecting files. The antivirus program cannot be detected or removed fully.

Ransomware

It may lock the system, which is not very difficult for a knowledgeable person to reverse. The main type of malware from crypto virology, it threatens the victim's data while publishing or block access to it unless a ransom is paid. There are 181.5 million ransomware attacks in the first six month of 2018. Then considering crypto wall is estimation by the US Federal Bureau of Investigation. It is making them inaccessible.

Adware

Adware is unwanted software. It remains hidden in your computer and displays advertisement on screen, often within a web browser. The advertisement is produced by adware through pop-up windows or bars.

Spyware

It gathers information about a person or organization without his knowledge. To remove spyware there are some antivirus and anti-spyware. We can set browser security to enhance privacy level. Avoiding clicking on pop-up ads. is a good habit.

Every gathered information from the monitored device is accessible on your cell phone.

Spam

Spam involves the messages which are unwanted, often unsolicited advertising, mainly to many recipients. There is some example in SPAM while sharing any post of our email address, which must be protected. Avoiding clicking to reply spam message and using personal or business email address will offer protection against spam [5].

Pharming

Pharming is a cyber-attack which is intended to redirect a websites traffic to another fake site. In pharming, the hackers can use to steal persona and sensitive information from victims on the internet. This is known as DNS cache poisoning. Pharming has been called” phishing without lure”.

Phishing

Phishing is contacted by email and a cybercrime. The examples of phishing are generic greeting, forget link, request for personal information, sense of urgency, etc. The main type of phishing are vishing, smishing, search engine phishing, spear phishing and whaling. Vishing mainly refers to phone calls and smishing. SMS phishing and SMiShing are the easiest types of phishing attack.

Distributed denial-of-service

It is said to be DOS attack, which is nothing but cyber attack. The network resource becomes unavailable and temporarily or indefinitely disrupted. The denial of service is a resource with superfluous requests and it is accomplished by flooding. There is an attempt to overload systems and it is used to prevent some or all the legitimate requests from being fulfilled.

Online Defamation

Defamation is considered as false. A false concept or statement must harm someone's reputation. There are many false statements posted across the internet. A statement not only is false but also harms the user or user company's reputation, and mainly online defamation is very harmful.

Wi-Fi Eavesdropping

Wi-Fi Eavesdropping can involve unsecured Wi-Fi network, when unsecured transmission of data allows the theft of anything that's encrypted, from passwords to financial information. It is considered as personal or business-related

Cyber Bullying

The protection of cyber-bullying is to keep the password a secret from others. Kids must try to think about who sees what is posted online, and keep their parents in loop. It is practice where an individual or group uses the internet. The emotional and social harm inflicted by cyber bullies grows out of, or leads to, physical bullying in the online world.

Cyber Stalking

It is often accompanied by the real time or the offline stalking. Hence, both are motivated by a desire to control, intimidate or influence a victim. It is a criminal offence which is under various laws such as anti-stalking, slander and harassment. Anti-stalking, slander and libel may be used to threaten, embarrass or harass.

III IMPORTANCE OF CYBER SECURITY

Mainly, hardware like mobile phones, laptop, desktop etc. and software like work application need cyber security during data in transit and at rest. The essential thing in cyber security is to understand that everyone is at risk of cyber-attack. Cyber criminals have become more highly professional. If people are serious about security, they must install security the necessary app for prevention [6].

IV CHALLENGES IN CYBERSECURITY

There are main five sources of challenge in cyber security. They are Ransomware Evaluation, AI exp IOT threats, Block chain Revolution and server-less apps.

Ransomware Evaluation

Ransomware Evaluation attacks the areas which are growing fast in cybercrime. Mostly the number of attacks has risen by 30% this year. In fact, in 20% business, there is no recovery solution. When a malicious attack comes one fifth of business will get spoiled by recovering the data information and applications from customer information servers.

AI Expansion

AI Expansion is mainly considered as robot. Robots don't take breaks as humans do. They don't need hourly payment for development of several safeguards.

In case, Artificial intelligence doesn't need to sleep, it must be set against malware.

IOT Threats

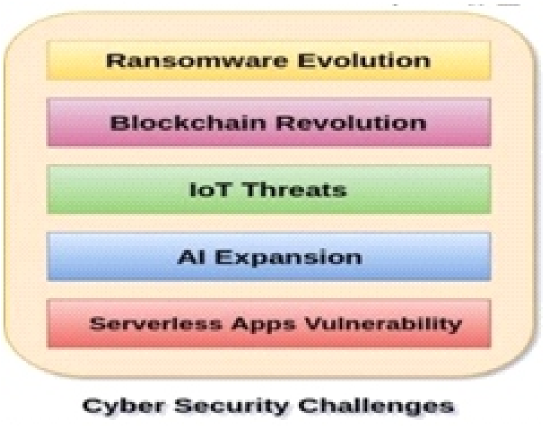
When a greater number of people are plugged-in, every single device is connected to internets. The refrigerator call tells you when the milk runs out. We can easily control TV with mobile phones.

Block chain Revolution

With the popularity of crypto-currencies like bitcoin and ethereum. it is difficult to predict the block chain system of other developments that will offer cyber security.

Server-less Apps' vulnerability

These apps will usually invite cyber attacks. Of course, the software integration into the types of application which gives the main user the best chance of defeating cybercriminals cannot directly defend the customer [7].



Cyber Security Challenges Fig :2

V CYBER LAWS

There is rapid growth of internet and cyberspace. Cyberspace includes network, computer, data storage devices, software, websites, internet, emails and electronic device such as cell phones, ATM machines etc. and are governed by a system of laws and that regulation is called cyber law. Cyber law deals with all cybercrimes, intellectual property, electronic or digital signature and data privacy and protection. Some of cyber laws are:

1. Digital SignatureAct,1997
2. TelemedicineAct,1997
3. Computer Crime Act,1997
4. Communication and Multimedia Act,1998 [8].

VI CYBER COMPLAINTS

Over the last decade there has been a rise in internet. It has resulted in increase in cybercrimes and cases of online cheating. The victim of cybercrime can file complaint at the local police station and seek remedy. Complaints can also be filed against online abuse of social media platforms such as Snapchat, Twitter, Facebook, Instagram and YouTube. There are some links to file cybercrime complaints in India through online portal. To complain about social media online transaction, internet, fake call, ransomware, malware, data theft, email, and mobile application proofs such as screenshot, copyright document and softcopies. For cheating related to internet banking victims should give bank ID, his statement and bank records [9].

VII CONCLUSION

Cyber security is the quickest and most effective way which is needed to safeguard against attackers and it is designed to counter the lifecycle of vulnerability management. Routine security assessment is a regular security. It can be used to develop preventive measures against future attacks. It may increase the awareness of internet users. Backup of important data on a daily basis will help safeguard user interests. Backup should be stored on both on-side and off-side servers, whenever it is possible. Portable devices are very popular with use of encryption software and hardware, which are available to meet the business needs. There are no permanent solutions for cybercrimes but we can minimize the harm and guard against future crimes [10].

REFERENCE

1. http://www.dissertationhomework.com/essays /security/the-importance-of-cyber- security-in-modern-internet-age

2. https://www.secureworks.com/blog/cyber-threat-basics

3. https://www.slideshare.net/mobile /techexpert2345/types-of-malware

4. https://en.m.wikipedia.org/wiki/Spamming

5. https://www.transunion.com/blog/identity-protection/why-is-cyber-security-important

6. https://www.globalsign.com/en/blog/cyber security- trends-and-challenges-2018/?gclid=CjwKCAjw7uPqBRBlEiwAY Dsr19Z1C9JTeyvYLhYeCamyE5VwKYyn vC1aFFsK-6XlJGLW-DJ4ch_WRxoCYUgQAvD_BwE

7. https://www.slideshare.net/mobile/fariez91/cyber-law-78597

8. https://ifflab.org/how-to-file-a-cyber- crime complaint-in-india/

9. https://www.slideshare.net/mobile/EngAkoush/cyber-crime-security-60980220