International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 06 Issue: 06 | June - 2022 Impact Factor: 7.185 ISSN: 2582-3930

CYBER SECURITY AND ITS CRIMES

Naresh M

Abstract

Cybercrime is a very complicated and dynamic phenomena. All the consumers, public and private businesses arethreatened by cyber thieves who are more skilled. As a result of this threats, more andmore defence layers are required. As the businesses have started to use computers in their daily operations,cybercrime hasbecome more complicated, as have the financial consequences. One of the cyber-criminal case studies is Parliament assault. In this article, we've addressed cyber crime and Cyber-Security, as well as the various typesof cyber crimes that we encounter, as well as prevention and detection measures such

Keywords – Cyber-crime, Cyber-security, Anomaly detection, Case Study, Regulation Acts, few online safety tips.

INTRODUCTION

"Men have been caught in a series of technical traps ever since they began toutilise technology to modify their lives." A good example of a technology trap is cybercrime. Cyber criminality is referred to as cyber crimes, computer crimes, electric crimes and e-crimes. "Cyber" stands forcyberspace. The electrical medium of a computer network. "Cyber crime is defined as computermediated behaviour that is

Triipwires, config checking tools, Honey pots, anomaly detection systems, and operating system commands. We also talk about the laws that are in place to combat cybercrime, as well as internet safety advice.

In this paper, we are going to see what measures can be used to prevent the cyber crimes. And it also includes few onlinesafety tips to prevent the data from being stolen. It consists of different legal

actsagainst the cyber crime and laws to preventthe theft of data. Here we also cover the types of cyber crimes,it includes hacking ,phishing ,denial of service attacks(DOS),credit card fraud,salami attack,cyber stalking either illegal or illicit in the eyes of certain parties and can be carried out via international electronic networks," according to Wikipedia. "Criminal behaviour that necessitates the use of a computer or network" is how cybercrime isdefined. The following are the two categories of cybercrime:

1. **1.**Cybercrime in its broadest sense:Crimes against computer systems and their data that are carried out using electronic means.

2. Cybercrime (computer-related crime) in a broader sense: Any illicit activity involving the use of computer networks, whether directly or indirectly, to obtain and distribute data.

Why Cyber Security?

Users can safeguard their data on the network and in the system thanks to computer security. Among other things, it protects the computer system against a variety of harmful technologies. (virus, worms, bugs). It also assists in network monitoringand protection against various threats. So, to secure our data from various types of sniffing stolen problems, we should utilise computer security solutions on some level. Assuring the confidentiality, integrity and availability of computer systems and resources requires computer security. If confidentiality is not maintained, valuable business information and sensitive personal data may be jeopardised. Without integrity, we have no way of knowing whether or not the data we have is the same as what was initially delivered. If computational resources aren't available, we may limit user access to them (i.e., A virus that disables your keyboard and mouse).

CYBER CRIMES CLASSIFICATIONS

1. Hacking
2. DOS (Denial of service attack)
3. Computer forgery
4. Virus Dissemination
5. Phishing
6. Credit card fraud
7. Cyber stalking
8. Threatening
9. Spoofing
10. Salami Attack

HACKING: Illegally accessing a computer and making changes to the data so that it may be accessed again and again, as well as modifying the system's purpose or function, all without the permission or knowledge of the system's owner/user.

DENIAL OF SERVICE ATTACK: -

Denial of Service (DoS) attacks is a crude method of overloading the target computer's resources, preventing other computers from reaching the server. In order to bring down a server, hackers use a number of techniques. As network administrators understand how to minimise the impact of one tactic, hackers come up with other and more potent techniques to infiltrate networks.

VIRUS DISSEMINATION: This sort ofcriminal activity involves

installing new programmes such as viruses, worms, or logic bombs to gain unauthorised access to a computer system Computer sabotage is defined as the illegal alteration, suppression, or deletion of computer data or functionalities through the Internet in order to disrupt the system's regular operation.

CREDIT CARD FRAUD: The most prevalent targets for fraud are intangible assets represented as data, such as money on deposit or hours worked.

Computer fraud is rapidly replacing cash in modern business. Organized criminal crimes have regularly targeted credit card information, as well as personal and financial information on credit cards.

PHISHING: Personal information like as account names, passwords, or credit card details may be obtained by distributing "spoof" e-mail messages that seem legitimate but are really a scam to get people to hand over their personal data to scammers.

LITERARTURE SURVEY

Paper No.	978-1-5386-4985-9
Title of the paperand authors Year of publish	Cyber crimeand prevention and detection 2015
Types of issue resolved	It reduces the risk of cyber crime
objectives	Respond to resolve and recover from cyber incidents

Paper No.	987-4799-2195-8
Title of the paper and authors Year of publish	Cyber crime2014
Types of issue resolved	Prevention of cyber crime
Objectives	To overcome internet crimes

PRECAUTIONS TO PREVENTCYBER CRIME

1. Firewalls : From the outside, these people are the network's gatekeepers. A firewall should be placed at every point where the computer system interfaces with external networks, such as the Internet, a separate local area network at the customer's location, or the telephone company switch.

2. Password protection: Every time a PC user logs on, they should beprompted to enter a password that only they and the network administrator know. Easy-to-guess words, phrases, or figures, such as birth dates, a child's name, orinitials, should be avoided by PC users. Instead, they should usecryptic words or numerals with a mix of upper and lowercase letters. For example, "The Moon Also Rises" letters. The system should also force all users to update their passwords every month or so, and new users should be barred from the system if they use the same incorrect password three times in a row.

3. Encryption: Even if the outsiders manage to get past a firewall, encrypted data on a network can ne kept safe. Microsoft Windows NT, Novel NetWare, and Lotus Notes all include built-in encryption mechanisms that encrypt any data that is sent over the network. There are separate encryption packages that may be purchased by companies for usage with certain applications. Every encryption application uses the public-private key approach. For each transmission, a unique secret key is used to scramble and encode the data. Receipients decode the message's secret code by utilising the sender's public key in conjunction with their own private encryption key.

4. Never give up your credit card information to a site that isn't encrypted..

Online safety tips:

1) 1) To Install anti-virus software and keep it up to date to protect yourself from infections. You may get anti-virus software online or in shops; the best can identify both old and new infections.

2) If you expect or are familiar with the contents of a file attached to an email, only open it. Include a message detailing the attachment if you're sending one. Any e-mail with a virus notice should never be forwarded. It's possible that it's a hoax designed to transmit a virus.

3) Verify the website with whom you are conducting business. Protect yourself from "WebSpoofing." Do not follow email links to websites.

4) Create passwords containingatleast 8-10 characters to keep yourdata safe. They should not be any dictionary words. And it should contain uppercase and lowercase characters.

5) Send credit card details to only secured sites.

DIFFERENT LEGAL ACTS AGAINST CYBERCRIMES

The India Information Technology Act of 2000.

The Philippines Electronic CommerceAct No 8792 of 2000

The Philippines Cybercrime Prevention Act of 2012 No.10175 USA

Cyber Intelligence Sharing and protection Act of 2011(CISPA).

USA Cyber Security Enhancement Actof 2009(S.773).

CONCLUSION

The internet is a valuable resource and a very efficient method of communication, but it is also a target for hackers and other malicious actors, just like any other medium. The development, implementation, and management of intrusion detection technologies are all necessary steps in the fight against cybercrime. Everybody should be careful and take precautions; people, institutions and the government should all do so at this time.

REFERENCES

[1] http://www.infosecwriters.com/text _ resources/pdf/BPlad na_Cybercr ime.pdf

[2] http://www.itu.int/osg/spu/c ybersecurity/docs/Background_Pa per_Comparative _Analys is_Cyb ersecurity_Initiatives_ Worldwid e.pdf

Internet Resources

[1] http://en.wikipedia.org/wiki/Security

[2] http://en.wikipedia.org/wiki/Data_ security

[3] http://en.wikipedia.org/wiki/Inform ation_security

[4] http://en.wikipedia.org/wiki/Computer_ security

[5] http://www.cyberlawclinic.org/case study. asp

[6] http://www.cyberlawsindia.netcases/html