IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

NCAIT 2017

JSS Academy of Technical Education

Vol. 4, Special Issue 8, May 2017

Cyber Crime, Security and Prevention

Prasanna Kumar N[1], Prem Vikas[1], Rekha P M[2]

UG student, Department of Information Science and Engineering, JSSATE, Bengaluru, India[1]

Assistant Professor, Department of Information Science and Engineering, JSSATE, Bengaluru, India[2]

Abstract: The main reason for new forms of crime labeled cyber crime is the speedy growth of the internet and computer technology over the past few ages.Cyber is the imaginary space, which is created when the electronic devices communicate, similar to network of computers, Cyber crime refers to anything done in the cyber space with a criminal intent. These could be either the criminal activities in the traditional sense or could be activities which are newly evolved with the growth of the technology. Cyber crime includes acts such as hacking, uploading obscene content on the Internet, sending obscene e-mails(spamming) and hacking into a person's e-banking account to withdraw money(**phishing)** The concept of cyber crime is not very different from the concept of conservative crime since both include conduction of unauthorised action or omission, which breaks the rules of law. Cybercrime has been one of the common practices made by the computer experts. this paper its mentioned about some of the impacts of the cybercrime. This paper gives detailed information regarding cybercrime, its types, modes of cybercrime and security measures including prevention to deal effectively with cybercrime.

I. INTRODUCTION

We are living in the modern era based on the technology. Our daily life depends on it, live with it. So, internet is a common criteria known by all.. It is a pool of Information.Everything we need,any information regarding anything we can find on the internet. So, people are using and depending on it more and more. As internet practice is increasing, it makes the world small; people are coming closer. Swift technological growth and advances have provided massive areas of new opportunity and efficient sources for organizations of all standards.It has become now a national asset, the whole national security is also depending on it.Due to these new technologies unparalleled threats are resulted with them as a cyber crime.**Cyber crimes** are any crimes that involve a computer and a network. In some cases, the computer may have been used in order to commit the crime, and in other cases, the computer may have been the target of the crime.Cyber crime mainly consists of illegal access to computer systems i.e data modification, data destruction, and theft of intellectual applications. Cyber crime in the frameworkof national security may involve hacking, traditional espionage, or information warfare and related activities.Crimes committed usually are hacking, spamming, phishing etc.

II. CATEGORIESOF CYBER CRIME

Cyber crime can be divided into two categories namely,
1. Cybercrime in a narrow sense (computer crime): Any illegal behavior engaged with respect to electronic operations results in threat to the security of computer systems and the data processedby them.
2. Cybercrime in a broader sense (computer-related crime): Any illegal behavior committedby means of, or in relation to, a computer system or network,including such crimes asillegal ownership and contribution or distributing information by means of a computer system or computer network.
Pornography, intimidatingemail, assuming someone's identity, sexual harassment, defamation, SPAM and Phishing are some examples where computers are used to commit crime, whereas viruses, worms and industrial espionage, software piracy and hacking are examples where computers become victim of cyber crimes.
Convention on Cyber Crime distinguishes between four different types of offences:
1.offences such as such as illegal access, illegalinterception,datainterference,system interference and misuse of devoice are Offences against the confidentiality, integrity and availability of computer data andsystems,
2.offences such as computer-related forgery and computer-related Fraud are Computer-related offences.
3. Content-related offences, such as offences related to child pornography; and
4. Copyright-related offences, such as offences related to copyright infringements andrelated rights.

III. TYPES OF CYBER CRIME

I. Unauthorized Access:
Also known as Hacking.ItIncludes gaining access illegally to a computer system or computer network and in some cases making illegal use of data access. Hacking is also the method by which other procedures of cyber-crime (e.g., fraud, terrorism) are committed.

II. Theft :
Theft of any information contained in electronic form such as hard disks, removable storage media etc. Theft may be

IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

NCAIT 2017

JSS Academy of Technical Education

Vol. 4, Special Issue 8, May 2017

either by seizing the data physically or by altering them through the virtual medium.

III. Email bombing-
This refers to sending a large number of emails to the victim resulting in the victim's email account (in case of an individual) or mail servers (in case of a company or an email service provider) crashing.

IV. Data diddling-
This kind of an attack involves altering raw data just before a computer processes it and then changing it back after the processing is completed. The electricity board faced a same problem of data diddling while the computerization of department.

V. Salami attacks-
This type of crime is normally dominant in the financial institutions or for the persistence of committing financial crimes. An important feature of this type of offence is that the alteration is so small that it would normally go unnoticed. E.g. a bank employee inserts a program, into the bank's servers, that deducts a small amount of money (say 5 cents a month) from the account of every customer. This unlicensed debt is likely to go unnoticed by an account holder.

VI. Denial of Service attack-
The victimised computer is swamped with more requests than it can handle which results in crash.Distributed Denial of Service (DDoS) attack is also a type of denial of service attack wherein the perpetrators are many and are geographically widespread,E.g. Amazon, Yahoo.

VII. Virus / worm attacks-
Viruses are modules that assign themselves to a computer or a file and then itterates themselves to other files and to other computers on a network. They typically affect the data present on a computer, this can be done by altering or deleting it. Worms distinguish themselves from viruses with no involment of the host and cycles itself. They simply make functional copies of themselves and do this iteratively till they eat up all the available space on a computer's memory.

VIII. Logic bombs-
These are event dependent programs. This implies that these programs are created to do something only when a certain event (known as a trigger event) occurs. E.g. many viruses are termed logic bombs because they lie inactive all through the year and become active only on a particular date (like the Chernobyl virus).

IX. Trojan attacks-
This term has its origin in the word 'Trojan horse'. In software field this means an unauthorized programme, which passively gains control over another's system by representing itself as an authorizedprogramme. E-mail is the most communalway for trojan to multiple itself.

X. Internet time thefts-
Normally in these kinds of thefts the Internet surfing hours of the victim are used up by another person. This is done by gaining access to the login ID and the password. E.g. Colonel Bajwa's case- the Internet hours were used up by any other person. This was possibly one of the first reported cases related to cyber crime in India. However this case made the police ill-reputed as to their lack of understanding of cyber crime.

XI. Web jacking-
In these kinds of offences the hacker gains access and control over the web site of another. He may even mutilate or change the information on the site.

XII. Cyber-Terrorism
Hacking designed to cause terror. Like conventional terrorism, `e-terrorism' is utilizes hacking to cause violence against persons or property, or at least cause enough harm to generate fear.

IV. CYBER SECURITY

It is the method for safeguarding of networks, computers, programs and data from attack, harm full or illegal access by using technologies, processes and practices designed. It involves the protection of hardware, software or the data on the system, as well as from interruption or misleading of the services provided by systems from the robbery or damages or unlawful accesses.

i. Goals of Cyber security

->safeguard of computer ,systems and computer networks.
->secure the confidentiality of information , data, database.
->securing devices, products and promote reliability of applications.

ii.Need for security

Most initial computer applications had no or best or very less security. This was continued till the importance of data was realized. Until then data was something which is use full but not protected. Computer security is important because it can provide the opportunity for users to protect their important information present on the network and also in the systemsCybermischeif, hacking, unlawful accesses have reached the level of complexity and in many cases go beyond the capability of most organization to defend against. The requirement of information security

IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

NCAIT 2017

JSS Academy of Technical Education

Vol. 4, Special Issue 8, May 2017

within the organization has undergone major changes. Before the prevalent use of data processing equipment, the safekeeping of information felt to be of great importance to an organization,this was provided primarily by physical and administrative means. The need for automated tools for protecting files and other information stored on computer become evident. The basic name for the collection of tools designed to protect data and thwart hackers is cyber security or computer security.

Joseph Kizza defines computer security in terms of

I.Confidentiality-

The principle of confidentiality agrees that only the sender and the future recipients should be able to access the contents(information) of message. Confidentiality get compromised if an unauthorized person is able to access a message

II. Integrity-

when the content of a message are changed after the sender sends it, but before it reaches the intended recipient, then the integrity of message is lost**.**

III.Availability-

the principle of availability states that resources should be available to authorized parties at all times.

IV.Access control-

the principles of access control determines who should be able to access what.

V**.**Authentication-

the mechanism help to establish proof of identities .The process ensures that the origin of document or message is correctly identified.

V. TYPES OF CYBER SECURITY

i.Network Security:

Network access fortification involves network division, and encrypted communication to guard automation networks against unauthorized or unlawful access.

Network security refers to any activity planned to guard the usability and integrity of your network and data or information. Shielding a network from unauthorized access is critical when it comes to avoiding immeasurable risks:

I. Increase and maintenance of plant availability.

II. Protection of confidential data**.**

III. Protection against manipulation.

ii.System Security.

As computing systems become more necessary to our daily life, it becomes ever more important that the services provided by the system are obtainable whenever we need them. We must also be able to depend on the integrity of the systems, and thus the information that they can hold on to and provide when needed our society and our economy depend more upon certain pieces of information that is confidential.

iii.Data Security:

Another important form of the computer security is the data security. It is defined as the type of security that is used to protect the important data present on different drives of the computerfrom different types of threats through different types of software/hardware solutions

VI. CYBER PREVENTION

it is the act of limiting, overwhelming, governing , eliminating, or preventing the incidence of cyber attacks, in computer systems both hardware and software systems, networks and data, or any other electronic devices .

i.Cyber Detection systems

it detects an asymmetric and abnormal activities of the system. It can scan a network for people that are on the current network and check who should not be there or are doing things that they should not be doing, for example trying a lot of passwords to gain access to the network.

ii.Prevention of cyber crime

Prevention is always better than cure. It is always better to take certain precautions while working on the internet. One should make them a part of his cyber life.

1. Identification of exposures through education will promote responsible companies and industries to meet these challenges.
2. Avoid exposure of any personal information to foreigners, via e-mail or any social networking site.
3. Assign multiple and different password and username combinations for different accounts and resist the temptation to write them down.
4. An update Anti-virus software to guard against virus attacks should be used and should also keep back up so that one may not suffer data loss in case of virus infection.
5. Never reveal the credit or debit cards detalis to unauthorised sites to guard against hacks.
6. Defend your data by using encryption for your most sensitive files such financial records and tax returns.
7. Web site owners should watch traffic and check any irregularity on the site. It is the responsibility of the web site owners to implement some policy for preventing cyber crimes as number of internet users are growing day by day.
8. Strict legal laws need to be passed by the Legislatures keeping in mind the interest of citizens.
9. Use of firewalls proves advantageous.
10. Avoid opening attachments or e-mails which were not expecting and have come from unknown source or person.

VII.ELECTRONIC CRIME DETECTION

Naturally electronic crimes are detected by one or more types of intrusion detection techniques. Such techniques include • Tripwires• Honey pots• Anomaly detection systems • Operating system commands.

Tripwire is detection software and data veracity tool useful for managing and notifying on specific file changes on a range of systems. In this case, tripwires provide the

IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

NCAIT 2017

JSS Academy of Technical Education

Vol. 4, Special Issue 8, May 2017

required lead of electronic crimes because most of the obtrusive hackers make modifications when they install entry points or alter file system and directory features unknowingly while interfering.

Honey pots: Honey pot lures are employed to trap and keep an electronic criminal busy enough to allow for identification of culprit. These lures can be bogus system administration accounts, invented product or client information, or a myriad of created files that appear to contain sensitive information. In addition to facilitating offender identification, honey pots also store the evidence of the electronic crime itself.

Anomaly detection systems: Anomaly detection system emphasis on unusual outlines of activity. Significantly, anomaly detection systems advances and analyze user profiles, host and network activity, or system programs in anticipations of discovering deviations from expected action. Unusual intervals, abnormal commands, and unconventional program activities can provide evidence regarding the existence can provide evidence regarding the existence of an electronic crime.

Operating system commands: Intrusion detection is also possible through the use of certain operating system commands, for example checking log files and linking outputs of similar programs are among the numerous manual techniques involving operating system commands. Typically these commands are used on daily bases by system administrators to search for evidence suggesting the possibility of electronic crimes.

CONCLUSION

By conclusion, computer crime is having a major effect on the world we live,it usually attacks every human being irrespective of from where he is,many hackers around us view internet as public data generation centre and do not see their actions as criminal, hackers are there from the point where internet was evolved, they are influential in making the internet what it is today, it can also be said that hacking and computer crime will be with us for as long as we have the Internet. so it is our responsibility and conscious to keep the balance between what is a crime and what is done for pure enjoyment. even though government is making an effort to control the Internet, but true control over the Internet is impossible, because the reasons the Internet was created was for the noble cause, here comes the real role of families and the institution of education, parents and teachers need to guide their children what it is okay to do on the computer and what is not, and to educate them on the consequences of their actions. but we are not able to predict the true nature of computer crime in the future, because what was called as crime today may not be called as a crime the next day due to advancement in technology, more encryption techniques can be used to secure the passwords in future, recorded computer crimes cases in many organization involve more than individual and virtually all computer crime cases known till today are committed by employer of the organization, criminals are also using the advancement in technology to further their own illegal activities, many cyber laws should also be enforced to avoid computer-related crimes and the techno-criminals who commit them. this article is meant to suggest us to expose us to the the computer-related crime and provides ways to prevent them.

REFERENCES

1).cryptography and network security by williamstallings(4th and 2nd edition)
2). Cyber security everything an executiveneeds to know by philipferora.
3). Cyber security and unserstandingcyber crimes by Nina Godbole and Sunithbelapure
4).http://business.cch.com/franlaw/cybercrime_whitepaper.pdf
5).http://www.nalsarpro.org/CL/Modules/Module4/Chapter-1.pdf
6). http://cyberlaws.net/cyberindia/articl es.htm
7). http://www.cyberlawsindia.net/
8).http://satheeshgnair.blogspot.com/2009/06/selected-case-studies-oncyber- crime.html
9). Kumar Vinod – Winning the Battle against Cyber Crime