RISK FACTORS IN CYBER CRIME & IT'S CHALLENGES.

MANASA BOLLAVARAPU
CSE, ALIET,VIJAYAWADA

Abstract:

A cybercrime is an illegal behaviour that is performed by means of electronic operations and it tries to harm the security of computer and it tries to harm the security of computer and it tries to harm the security of computer systems as well as the data processed by them. This involves a computer and network using the computer as the tool. As this became the most problematic element in the present world we use the term cyber security – it is the body of technologies, processes and practices designed to protect networks, computers and data from damage or unauthorized access.

Keywords: cybercrime, illegal behaviour, computer and network, cyber security, unauthorized access.

INTRODUCTION

Today we are living in a computer age. Computer is a mastermind gift of the science to the humankind. We can't imagine our day without it as it made our life very comfortable and easy. We store lots and lots of data in our computers but nowadays there is no security for that data as it being stolen by different types of cyber crimes like as hacking, phishing, identical theft, cyber stalking etc.Steps are in place to protect against cyber crimes.So,cyber security is very important as the world's growing dependency on technology is leading to the world's vulnerability.

Cybercrime:

Everybody is using computer right from teenagers to adults and from white collars to terrorists.So, conventional crimes like forgery, kidnapping etc.

The first recorded cyber crime took place in 1820. The fact abacus, which is thought to be the earliest form of a computer, has been around since 3500 B.C is not surprising. In India, Japan and China, the modern era of computers began with the analytical engine of Charles Babbage. The first spam email took place in 1976 when it was sent out over the ARPANT. The first virus was installed on an Apple computer in 1982.

Objectives:

- To provide general awareness of cyber law and cyber crime.
- To understand cyber crime methods.
- To identify internet scams.
- To learn how to keep from being a victim.

Categories of cyber crime:

We can categorise cyber crimes into two ways:

The computer as a target: using it to attack another computer.

Example: Hacking, virus attacks, Dos attack etc.

The computer as a weapon: using a computer to commit the real-world crime.

Example: cyber terrorism, credit card fraud and pornography etc.

TYPES OF CYBER CRIME:

Hacking:

Hacking is termed as an illegal obtrusion into a computer system and/or network. It is also known as cracking. Government websites are the hot target of the hackers due to the press coverage, it receives. Hackers enjoy the media coverage. The motive behind the crime called hackers. Motive behind the crime called hacking

greed power, publicity, revenge, adventure desire to access forbidden information destructive mindset wants to sell n/w security services.

Hackers are classified according to their actions. Some of them are :

Ethical Hacker: A hacker who gains access to systems with a view to fix the identified weaknesses is considered as an ethical hacker.

Cracker: A hacker who try to gain unauthorized access to computer systems for personal gain is considered to be cracker. They usually steal corporate data, violate privacy rights, transfer funds from bank accounts etc.

Grey hat: He/she breaks into computer systems without authority with a view to identify weaknesses and reveal them to the system owner.

Script kiddies: An unskilled person who wants to access the computer systems using already made tools.

Hacktivist: A hacker who send social, religious, and political, etc. Messages is called an Hacktivist. This is done by hijacking websites..

Phreaker: A hacker who identifies and exploits weaknesses in telephones instead of computers.

Child pornography :

The Internet is being highly used by its abusers to abuse children sexually. As more homes have access to the internet, more children would be using the internet and more are undergoing this problem.

How do they operate?

Paedophiles trap the children by using the false identity and interact with them .

Denial of service attacks:

This is an act by the criminals they fill their E-mail box with spam email stripping the services that they are entitled to access or provide. Many DOS attacks, such as the ping of death and Teardrop attacks.

Virus dissemination: Malicious software that attaches itself to other software.

Examples: virus, worms, Trojan horse, web jacking, e-mail bombing etc.

Viruses are categorized according to their infection technique, as follows:

Polymorphic Viruses :

Some viruses encrypt the code in a different way with each infection and change it to different forms to try to avoid detection.

Stealth Viruses :

These viruses hide characteristics the normal virus, like changing the original time and date stamp of the file to prevent the virus from being noticed as a new file on the system.

Fast and Slow Infectors:

These viruses can avoid detection by infecting quickly or slowly. This can sometimes allow the program to infect a system without detection by an antivirus program.

Sparse Infectors :

These viruses infect only a few systems or applications.

Armored Viruses :

These viruses are encrypted to prevent detection.

Multipartite Viruses :

These advanced viruses create multiple infections.

Cavity Viruses :

These viruses attach to empty areas of files.

Tunnelling Viruses:

These viruses are sent through different protocols or encrypted to prevent detection.

Camouflage Viruses:

These viruses appear to be another program.

NTFS and Active Directory Viruses:

These viruses specifically attack the NT file system or Active Directory on Windows systems.

Computer vandalism :

Damaging or destroying data rather than stealing or misusing them is called cyber vandalism. These are programs that replicate itself and then circulate.

Cyber terrorism:

Terrorist attacks on the Internet are a distributed denial of service attacks, hate websites and hate E-mails, attacks on service network etc.

One of the cyber crimes was online credit card fraud on e-bay.

Place: Bhubaneswar

Rourkela police busted a racket involving an online fraud worth Rs 12.5 lakhs. The modus operandi of the accused was to hack into the eBay India website and make purchases in the names of credit cardholders. A Mastermind Debases Pandit and a BCA student were under arrest and presented before the divisional magistrate at Rourkela.The other arrested person is Rabi Narayan Sahu. Superintendent of police D.S. Kutty said that the duo was later remanded in judicial custody but four persons supposedly involved in the commotion were imperceptible. A case is registered against the accuse under Sections 420 and 34 of the IPC.While Pandit, son of a retired employee of Rourkela Steel Plant, was arrested from his Sector VII residence last night, Sahu, his associate and a constable, was nabbed at his house in uditnagar. Pandit purportedly hacked into the eBay India site and collected the particulars of around 700 credit cardholders. He subsequently made purchases by means of their passwords.

The fraud came to the notice of eBay officials when it was detected that several purchases were made from Rourkela while the customers were based in cities such as Bangalore, Baroda and Jaipur and even London, said V. Naini, deputy manager of eBay. When the customer lodged a complaint, the company refereed the matter to the pursuance of Rourkela police. Pandit furnished the address of Sahu for delivery of the purchased goods, according to police source. The gang was involved in train, flight and hotel reservations.

The hand of one Satya Samal was recently arrested in Bangalore, is suspected in the crime. Samal had sheltered in one of a Bangalore hotels for three months where he the hotel and transport bills surprisingly to Rs 5 lakhs, which he did not pay. The he was arrested for default of bills, subsequently which Pandit hurried to Bangalore and stood guarantor for his release on bail, police sources say.

Crimes threaten social security

The Union home minister Shivraj Patel viewed that the increasing point of cybercrime is an sign of massive hazard to national safety. On Google's social networking site Orkut, Facebook, have been perplexing authorities. There is huge potential for damage to national security through cyber attacks. The internet became a means for money making and funding terrorist attacks in an organized manner.

Cyber Security:

Cyber Security involves protection our personal information through prevention, detection and response to different online attacks. Cyber security actually prevents the attacks, cyber security. We can keep our data secured by following mentioned points :

Privacy Policy:

When you are logging your name, e-mail, address, on a website look for the sites privacy policy.

Keep Software Up to Date:

If the seller reduces patches for the software operating system to your device, install it as soon as possible. Installing them will prevent attackers from being able to take advantage. Use strong passwords to protect from theft. Do not choose an option that allows your computer to remember your passwords.

Disable remote connectivity:

All our PDA's and phones are accomplished with wireless technologies, such as Bluetooth, that can be used to connect to other devices or computers.

Objectives of cyber security :

- Creating a Secure Cyber Ecosystem
- Creating an Assurance Framework
- Encouraging Open Standards
- Strengthening the Regulatory Framework
- Creating Mechanisms for IT Security
- Securing E-governance Services
- Protecting Critical Information Infrastructure.

Advantages of cyber security:

The cyber security will defend us from critical attacks. Internet Security process all the incoming and outgoing data on your computer. It protects our devices and accounts from hacks and virus. Application of cyber security used in our PC needs to update every week

Cyber law of India :

Cybercrime involves criminal activities that are traditional in nature, such as theft, fraud etc all of which are subjected to the India Penal code. In a simple way, we can say that cybercrime is an unlawful act where the computer is used as a tool or as a platform to do illicit acts.

Some of them are:

1. Cyber crimes against persons (cyber stalking, hacking, email-spoofying,child pornography, carding etc.)
2. Crimes against person's property (cyber vandalism, transmitting virus, intellectual property crimes)
3. Cyber crimes against government (cyber terrorism, cyber warfare)
4. Crimes against society at large (online gambling, forgery, financial crimes)

Conclusion:

Since, use of computer systems and internet is increasing world wide it became very easy to access our information from anywhere within seconds.So,certain precautionary methods and safety tips should be followed by the netizens so that we can challenge this threat. Indian laws are well drafted and are capable of handling all kinds of challenges as posed by cyber criminals. Technology is destructive only in the hands of people who do not realize that they are one and the same process as the universe.

"Technology is like a fish .The longer it stays on the shelf, the less desirable it becomes."

References :

1. Moore, R. (2005) "Cyber crime: Investigating High-Technology Computer Crime," Cleveland, Mississippi: Anderson Publishing.
2. Susan W. Brenner, Cybercrime: Criminal Threats from Cyberspace, ABC-CLIO, 2010.
3. Federal Bureau of Investigation for tips to avoid Internet fraud..www.fbi.gov/scams-safety/fraud/Internet_frau

BIOGRAPHY

BOLLAVARAPU MANASA at present has been pursuing B.Tech in CSE at ALIET, Vijayawada. She has participated in several national conferences and published a paper on "Machine learning the prospect of future technology!!:An elucidation" in Institute of Research And Journal (IRAJ).