1 BASICS OF CYBER SECURITY

Cyber crime can be defined as any crime with the help of computer and telecommunication technology with the purpose of influencing the functioning of computer or computer system. It is estimated that there are over 600 million users connected to the internet and e-mail today. With the boom in e-commerce and e-governance, the cyber crimes pose a serious threat to progress the information age.

Computer crimes are different from conventional crimes, as they can be easily committed from distant places, difficult to detect and even harder to prove them. It is a very low risk and high reward venture. As is evident, computer crimes do not involve violence but rather greed, pride or pay on some character weakness of the victims. It is very difficult to identify the culprit, as the net can be accessed from any part of the globe. The field is wide open for hackers. That is why cyber crimes are also called white collar crimes.

Cyber crime can take the form of simple snooping into a computer system for which we have no authorization. It can be the freeing of a computer virus into the wild. It may be malicious vandalism by a disgruntled employee. Or it may be theft of data, money or sensitive information using a computer system. The cyberpunk who explores a computer system without authorization is performing a criminal act. We might find ourselves faced with theft of sensitive marketing data by one of our competitors. A virus may bring down our system or one of its components.

Cyber crime can be of three categories, namely, against person, property and government.

i) ***Against persons:*** These crimes include various crimes such as harassing anyone with the use of a computer that could be via e-mail, cyber-stalking and transmission of child-pornography. One of the most important cyber crimes known today includes dissemination of obscene material including pornography, trafficking, distribution, posting, and indecent exposure, and child pornography.

ii) ***Against property:*** These crimes include, computer vandalism, transmission of harmful programmes and unauthorized possession of computerized information and unauthorized computer trespassing through cyberspace.

iii) ***Against government:*** a distinct kind of crime in this category is cyber terrorism. This crime manifests itself into terrorism when an individual or a group of people cracks into a government or military-maintained website.

The following are some of the more common computer-related crimes:

i) ***Data diddling:*** It is a simple and common computer-related crime which involves changing data prior to or during input to a computer. Data can be changed by anyone involved in the process of creating, recording, encoding, examining, checking, converting, or transporting computer data. This crime can be minimized by applying internal security controls.

ii) ***Trojan Horse attacks:*** Trojan horse involves the placement of unwanted computer instruction in a programme so that the host computer will perform some undesired/unauthorized function. The instructions enter the target system hidden in some other message or programme, thus the name Trojan horse attacks. This crime can be minimized by implementing security control measures for all incoming data containing hidden content.

Notes

iii) ***Logic bomb:*** Logic bomb is a computer programme executed at a specific time to cause damage to computer programmes or data. Logic bombs often enter a computer system using the Trojan Horse method, but differ because their presence is detected only after the bomb blows up. For example, a disgruntled employee may write a computer programme to cause the company's computer system to crash on a particular date. At the specified date and time, the system crashes costing hundreds of hours and thousands of dollars to restore. This crime can be minimized by using security methods that verify the system for inappropriate content.

iv) ***Impersonation:*** When access to a computer system is controlled by passwords and user identifiers, the most common method to gain access to the system is to impersonate an authorized user. Impersonation in the workplace may be accomplished as easily as taking an authorized user's place at an unattended terminal which has not been logged off. However, impersonation usually requires that the intruder has-access to two or three pieces of information:

a) User ID or account number;

b) Password of the authorized user; and

c) A dial port number, if access is attempted from a remote location.

Minimize the risk of unauthorized access by implementing security measures and password maintenance. Passwords should be of adequate length to maximize security and maintenance systems should force a change of passwords at regular intervals.

v) ***Internet and bulletin boards:*** Internet and bulletin boards can be used by hackers to exchange information necessary to commit criminal acts on computer systems. Both the Internet and bulletin boards allow users to communicate and exchange information on a wide range of topics. Therefore, a system access password obtained by a hacker in one city could be provided to any number of like-minded individuals around the world. Once this information is shared, hundreds of hackers may attempt to gain unauthorized access to the computer system. In a similar manner, payment card information or telecommunications calling card information can be shared with interested individuals around the world in a moment.

vi) ***Computer virus:*** A computer virus is programme code which can attach itself to other programmes and corrupt data and damage hardware. In addition to infecting other programmes, the virus may damage data by way of data diddling, Trojan horses or logic bombs. A virus may do nothing more than temporarily interrupt the computer service to display a message on the screen, or it may bring down the infected computer system. Software or hardware containing a virus can come from many sources such as public domain software, bulletin boards, the internet, computer club software, a friend or colleague's diskette, or commercial packages that have been tampered with. This crime can be minimized by incorporating virus scanning into the start -up of the computer system and scan any new software prior to use.

vii) ***Trap doors:*** A quick way into a programme by passing security.

viii) ***Spamming:*** Mass mailing of unsolicited e-mail messages.

ix) ***Piggibacking:*** Following an authorized person through a locked door, either a physical one or a computer's security firewall.

x) ***Dumpster diving:*** Scavenging through materials that have been thrown away.

Notes

xi) ***IP spoofing:*** Unauthorized access to computers where hacker sends messages to a computer with an IP (Internet Protocol) address indicating the message is coming from trusted sources.

xii) ***Data dawdling:*** False data entry, changing data before or during their input into a system.

xiii) ***Masquerading:*** Where one person uses the identity of another to gain access to a computer.

xiv) ***Password suiting:*** Automated guessing of phone numbers, user ID's and passwords.

xv) ***Worms:*** A stand alone programme that replicates itself on one computer and tries to infect other computers.

xvi) ***Cyber-loafing:*** Spreading excessive time on the internet gambling, pornography, checking stock travels, sports sources, etc.

xvii) ***Salami techniques:*** An unauthorized programme that causes the unnoticed debiting of small amounts of assets from large number of sources/accounts.

xviii) ***E-mail abuse:*** Sending unwanted e-mails, e.g., "I love You", "Love Bug", etc.

xix) ***Cyber harassment:*** It is a distinct cyber crime. Such harassment can be sexual, racial, religious, etc. Persons perpetuating such harassment are also guilty of cyber crimes. Cyber harassment could also lead to violation of privacy of citizens. Violation of privacy of online citizens is a cyber crime of a grave nature.

xx) ***Information warfare (IW):*** IW by foreign nations against critical infrastructures are the greatest potential threat to national security.

The cyber crime preparators could be students, amateurs or members of an organized group. The cyber criminals are bright, eager and highly motivated and willing to accept technological challenges. The cyber threats are from:

i) ***Insiders:*** The insiders are main sources of cyber crimes for many companies.

ii) ***Hackers:*** They crack into networks simply for the challenge of it.

iii) ***Crackers:*** Persons who break security on a system.

iv) ***Phreaker:*** One who breaks into telephone companies networks and uses them.

v) ***Virus writers:*** Virus writers pose serious threats to networks and systems worldwide.

vi) ***Foreign intelligent services:*** FIS uses cyber tools as part of their espionage activities.

vii) ***Terrorist:*** Terrorist groups are using cyber networks to formulate plans, raise funds, spread propaganda, etc.

Hacking and cracking are considered amongst the gravest cyber crimes. This happens when a stranger has broken into your computer system without your knowledge and consent and has subsequently tampered with your confidential data and information. This happens since no computer system in the world is hacking proof. Software piracy is also a distinct kind of cyber crime that is to distribute illegal and unauthorized pirated copies of software online. Further to use one's own programming abilities with malicious intent to gain unauthorized access to a computer or network can also be considered very serious crimes. Similarly, creation and dissemination of harmful computer programmes or virus which could do irreparable damage to computer systems also amounts to cyber crime.

It is the data and not the computer system per se that is the target of cyber crime. Theft of a computer printout may also be construed as cyber crime. The planting of a computer virus causes destruction of data, not the

Notes

computer itself. From this perspective, the computer system is the means not the end. However, investigating crimes against data means investigate the crime scene: the computer system itself.

The computer criminal is motivated by several things. He/she is in the hacking game for financial gain, revenge, or political motivation. There are other aspects of the modern hacker that are disturbing. Most proficient hackers are accomplished code writers. They not only understand the systems they attack, most write their own tools. Many hacking tools are readily available on the internet, the really effective ones are in the private tool kits of professional intruders.

Even though today's cyber crook has a specific goal in mind-to steal or destroy your data-he or she still has an inviting playing field. Today's intruder already has that understanding. He or she wants your data. Today's cyber crook will either make money off your or get revenge against you. He or she will not simply learn about your system.

Many organizations are not equipped to investigate computer crime. Although they may have the resources to get the process started, an in-depth technical investigation is usually beyond their scope. It means these organizations have two alternatives. They can call in law enforcement or they can employ consultants from the private sector. Many organizations prefer to do the latter. Calling in consultants is not a step to take lightly, however. The world is full of self-styled security consultants reformed hackers and other questionable individuals who are riding the computer security wave.

Private investigators traditionally involved with physical crime and civil matters, are looking at the world of virtual crime as a growth area for their businesses. If you use one of these firms be sure that they have the requisite experience in cyber crime investigation.

The best general source for investigative consultants is within the computer security community. However, you must use care in your selection, because not all consultants are created equal. The best requirement for your request for proposal then is likely to be references. References can be hard to get in some cases, of course, since most clients are understandably reluctant to discuss their problems with the outside world. Consultants can fill a number of roles on your investigative team. The most common is the role of technical specialist. Most consultants are more familiar with the security technologies involved than they are with the legal and investigative issues.

If social engineering is the emerging threat of the 1990s, the ability to interview, interrogate, and develop leads is about as old school investigation style as can be. In this instance good, old-fashioned police legwork pays big dividends, if it is performed by an investigative professional with experience. Many computer crimes involve fraud and money. An experienced information systems auditor with fraud investigation experience is worth whatever you pay in cases of large-scale computer fraud.

Present information systems are susceptible to cyber crime, because, it is inexpensive, quick and easy for anyone to launch attacks against the critical information infrastructures. The high density of information, high proceeding power and open connectivity of the system provide an attractive target for infiltrators for attacking information.

The computer system security should ensure that automated systems, data, and services receive appropriate protection from accidental and deliberate threats to confidentiality, integrity and availability. Absolute security is an unrealistic goal. A natural disaster or an adversary with sufficient resources and ingenuity is enough to compromise even the most secure systems. The optimum security system balances the cost of implementing protective mechanisms with the reduction in risk achieved.

Notes

The steps to establish and maintain an adequate computer security programme are:

i) Identify the computer system assets that require protection.

ii) Determine the value of each asset.

iii) Identify potential threats associated with each asset.

iv) Identify the vulnerability of the computer/EDP system to each of these threats.

v) Assess the risk exposure for each asset.

vi) Select and implement security measures.

vii) Audit and refine the security programme on a regular basis.

A computer system security should include the following components:

i) Administrative and organizational security

ii) Personnel security

iii) Physical security

iv) Electronic security

v) Hardware security

vi) Software security

vii) Operation security

The new technologies for preventing crimes are:

i) Firewall: Firewall implemented with secure standards will not allow any intruder into the system.

ii) Encrypted tunneling: An encrypted tunnel allows secure communications across internet. In this the data packets on internet are encrypted and then wrapped in IP at the initiation point of the tunnel. The encrypted packets can then be transmitted over the internet. When the packets arrive at the other end of the internet. When the packets arrive at the other end of the tunnel, they are unwrapped and decrypted.

iii) Secure Sockets Layer (SSL) and Secure HTTP (SHTTP) provide an encrypted TCP/IP. Pathways between two hosts on the internet (they require that both the browser and server be SSL-enabled). SSL can be used to encrypt any TCP/IP protocol (HTTP, FTP, TEL:NET), SHTTP, can only encrypt HTTP.

iv) Secure Electric Transform (SET) is the new technology for credit on internet. This involves cryptographic algorithms to encrypt the credit card numbers, so it cannot be seen on the internet.

v) Digital signature: Cryptographic technique is used so that only authorized and authenticated person can enter in the system.

vi) Employee training

vii) Cash account security.

Cyber crime is becoming one of the net's growth businesses. The recent spate of attacks that gummed up websites for hours-known as denial of service-is only one type. Today, criminals are doing everything from

Notes

stealing intellectual property and committing fraud to unleashing viruses and committing acts of cyber terrorism in which political-groups or unfriendly governments nab crucial information. Indeed, the tactic used to create mayhem in the past few days is actually one of the more innocuous ones. Cyber thieves have at their fingertips a dozen dangerous tools, from scans that ferret out weaknesses in website software programmes to snuffers that snatch passwords.

Net security is becoming an expensive necessity. As big as those numbers sound, no one really knows how pervasive cyber crime is. Almost all attacks go undetected-as many as 60 per cent, according to security experts. Most companies that have been electronically attacked will not talk to the press. A big concern is loss of public trust and image-not to mention the fear of encouraging copycat hackers.

Since cyber crime is a newly specialized field, growing in cyber laws, there is absolutely no comprehensive law on cyber crime anywhere in the world. This is precisely the reason why investigating agencies like FBI are finding cyberspace to be an extremely difficult terrain to handle. These various cyber crimes fall within the ambit of internet law that is neither fully nor partially covered by the existing laws and most importantly that too in some countries.

Notes