Cyber Security and Cyber Crime

Author: Sayyed Muhammed

M.E. – Digital Communication and Networking, Bangalore, India.

Abstract: *The world has become more advanced in communication, especially with the invention of the Internet. The main problem in today's society is cybercrime or e-crime (electronic crime), another term for cybercrime. Thus, e-crime is dangerous for nations, organizations and individuals around the world. It is widespread in many parts of the world and millions of people are victims of e-crime. Given the serious nature of e-crime, its global nature and its consequences, it is clear that a general understanding is needed to deal effectively with such crimes at the international level. This research includes the definition, type and intrusion of e-crimes. It also focuses on e-crime laws in different countries. Cyber security and search methods to be safe are also part of the study.*

Keywords: Cyber-Crime, Cyber-Security, Operational Security, Internet, Computer

Introduction:

Cyber-Security:

Cyber-security can be described as a combination of methods, technologies and processes to protect the privacy, integrity and availability of computer systems, networks and data from cyber-attacks or unauthorized access. The main purpose of cyber security is to protect all institutional assets from both external and internal threats as well as barriers caused by natural disasters. Since organizational assets are made up of multiple different systems, effective and efficient cyber security consolidation requires coordinated efforts across all of its information systems.

Cyber security is a major part of technology, processes and networks, computer systems, various programs and methods designed to protect data from cyber-attacks, all of which are harmful or have unauthorized access. In computer terms, security includes both cyber security and physical security. Security standards that enable organizations to study secure security techniques to reduce the number of successful cyber security attacks and restrict their data or systems. However, cyber security is important for network security, data security, communication security, operational security and application security.

Cyber security is the tools, strategies, security concepts, security guards, guidelines, risk management approaches, actions, training, best practices, assurances and technologies that can be used to protect the cyber environment and the organization and user's assets. The assets of the organization and the user include the integrity of the connected computer devices, staff, infrastructure, applications, services, telecommunications systems and / or information stored in the cyber environment. Cyber Security seeks to ensure the availability and maintenance of the security features of the organization and to protect the user's property against related security threats in the cyber environment. Following are the sub-domains of cyber security…..

1. **Application Security:** Application security involves the implementation of various immunizations against a variety of threats to all software and services used in an organization. Design of secure application architectures, secure code writing, robust data input authentication, threat modelling, etc. to minimize the possibility of any unauthorized access or alteration of resources in the application.
2. **Identity Management and Data Security:** Identity management includes frameworks, processes, and activities that enable the authentication and authorization of legal entities for information systems within an organization. Data security involves the implementation of a robust information collection system that ensures the security of the data at rest and in transition.
3. **Network Security:** Network security involves the implementation of both hardware and software systems to protect networks and infrastructure from unauthorized access, disruption, and misuse. Effective network security helps protect organizational assets from multiple external and internal threats.
4. **Mobile Security:** Mobile security means protecting both organizational and personal information stored on mobile devices such as cell phones, laptops, tablets, etc. from various threats such as unauthorized access, device destruction or theft, malware, etc.
5. **Cloud Security:** Cloud Security is concerned with building applications for the organization using protected cloud architectures and various cloud service providers such as AWS, Google, Azure, Rackspace, etc. Effective architecture and environmental structure ensure protection from various hazards.

6. **Disaster recovery and business continuity planning:** DR&BC deals with processes, monitoring, vigilance and planning that help organizations to keep critical business systems online during and after any disaster, as well as operations and systems resumed after an incident.

The significance and challenges of cyber security:

With the rapidly evolving adoption of technological landscapes and software in many areas, including the economy, government, military, retail, hospitals, education, to name a few, more and more information has become accessible through digital and wireless wired digital communication networks and ubiquitous. All of this highly sensitive information is invaluable to criminals and perpetrators, so it is important to protect it using robust cyber security measures and procedures. Recent high-profile security breaches by organizations such as Equifax, Yahoo and the US Securities and Exchange Commission (SEC) highlight the importance of good cyber security strategies, which resulted in the loss of highly sensitive user information that caused irreparable damage to both their finances and prestige. And with the trend, the number of cyber-attacks is showing no signs of abating. Both large and small companies are targeted daily by attackers to obtain sensitive information or disrupt services. The landscape of similarly evolving technologies also poses challenges in implementing effective cyber security strategies. The software is constantly changing as it is updated and improved which introduces new problems and insecurities and opens it up to various cyber-attacks. In addition, as IT infrastructure develops, many companies have already moved their on-premise systems into the cloud, leading to a whole new set of design and implementation issues that lead to new insecurities. Companies are unaware of the various risks in their IT infrastructure and therefore fail to place any cyber security countermeasures in place until it is too late.

Problematic Elements of Cyber Security:

One of the most problematic elements of cyber security is security risk. The traditional approach focuses on many resource components and protects against hazards, leaving some less important system components unchanged and some less dangerous risks, i.e. not protected. Such an approach is inadequate in the current environment. Following are challenging features of cyber security:

1. **Virus:** Runs against knowledge and your will, these are computer programs that attach or infect themselves to systems or files and transmit them to other mail on the network, by mail, by clicking on external devices, etc., disrupting computer operation and affecting data. Archived either by modifying it or by removing it completely.
2. **Warms:** Insects that are not like viruses do not need a host to stick to. They only make replicas without consuming all the available memory in the system. The term larvae are sometimes used as self-replicating malware (malice software). It occupies some free memory of drives or external devices.
3. **Hackers:** A hacker is usually a computer that usually breaks into a computer by gaining administrative control. Types of hackers:
    a. **White Hat Hackers:** A white hat hacker is a computer security expert who breaks into protected systems and networks and monitors their security. White hat hackers use malicious hackers (known as black hat hackers) to increase their security skills before detecting and exploiting them. Although these methods are not the same as those employed by malicious hackers, white hat hackers are allowed to hire them against an organization that hires them.
    b. **Grey Hat Hacker:** The term "grey hat" or "grey hat" refers to a computer hacker or computer security expert who may occasionally violate laws or specific ethical standards but is not the malicious intent of a black hat hacker.
    c. **Black Hat Hacker:** A black hat hacker is a person with extensive computer knowledge intended to breach or bypass Internet security. Black hat hackers are also known as crackers or dark-sided hackers. The general opinion is that when hackers make things, firecrackers break things.
    d. **Malware:** The word "malware" comes from the word "malice software". Malware is any software that infects and damages a computer system without the owner's knowledge or permission. (1) Viruses, (2) Worms, (3) Root Kits, (4) Trojans, (5) Spyware, (6) Crime, (7) Adware
    e. **Trojan:** Trojan horses are email viruses that can duplicate themselves, steal information, or harm computer systems. These viruses are the most serious threat to computers.
    f. **Password Cracking:** Which are able to determine passwords or find passwords on different protected electronic areas and social network sites.

Management of Cyber Security:

The risk associated with any attack depends on three factors: threats (who is attacking), insecurity (the attacks they are attacking) and the consequences (what the attack does). Information technology risk management is considered fundamental to effective cyber security. Following are the best practices of cyber security…..

1. **Risk Assessment Performance:** Organizations should conduct a formal risk assessment to identify all valuable assets and prioritize them based on the consequences of the compromise. This will help organizations decide how to best use their resources to secure each valuable asset.
2. **Confirm Protected Password Storage and Guidelines:** Organizations should implement the use of strong passwords that comply with industry recommended standards for all employees. They should be forced to make regular changes to avoid compromised passwords. In addition, industry best practices for using salt and robust hashing algorithms in password storage should be followed.
3. **Conduct Cyber Safety Training and Cognizance:** If employees are not educated on cyber security, company policies and incident reporting, a strong cyber security policy will not succeed. Expensive security breaches result when employees commit malicious acts for no reason or intent. Educating employees through seminars, classes, online courses and raising awareness about the company's policies and best practices for safety is a great way to reduce the likelihood of neglect and safety breaches.
4. **Execute Periodic Safety Evaluations:** Going through the occasional security reviews of all software and networks helps to quickly and securely identify security issues in a secure environment. Security reviews include application and network access testing, source code reviews, architecture design reviews, red team evaluations, and more. Once security insecurities are identified, organizations should prioritize them as soon as possible and reduce them.
5. **Backup Data:** Backing up all data from time to time increases redundancy and ensures that all sensitive data is not lost or created when security is breached. Attacks, such as injections and ransom ware, compromise the integrity and availability of data. Backup can help protect in such situations.
6. **Use encryption for data at rest and in transition:** All sensitive information should be stored and transferred using robust encryption algorithms. Encrypting data ensures privacy. Effective key management and rotation strategies must also be maintained. All web applications / software must use SSL / TLS.
7. **Design Software and Networks with Security in Mind:** When creating applications, write software, architectural networks, always design with security in place. Keep in mind that the cost of refactoring software and then incorporating safety measures is much higher than increasing safety from the start. Security Designed applications help reduce threats and help them fail securely if software / network fails.
8. **Implement strong input authentication and industry standards in secure coding:** Strong input authentication is often the first line of protection against a variety of injection attacks. Software and user applications are designed to accept user input as they open up to attacks, and this is where strong input validation helps filter out malicious input payloads processed by the application. Furthermore, secure coding standards should be used when writing software as it helps to avoid the much prevalent insecurity described in OWASP and CVE.

Cyber Crime:

Cybercrime is a crime that involves a computer, networking device or network. Most cybercrimes are committed by cybercriminals to make a profit, some cybercrimes are used to directly damage or disable computers or equipment, while others use computers or networks to spread malware, illegal information, images or other content. Some cybercrimes target both computers, i.e., infecting computer viruses, which then spread to other machines and sometimes to entire networks. The primary consequence of cybercrime is financial; Cybercrime involves a variety of for-profit criminal activities, including ransom-ware attacks, email and internet fraud and identity scams, as well as attempts to steal financial account, credit card or other payment card information. Cybercriminals can target one's personal information as well as corporate data for theft and resale. Following are the some different types of cyber-crimes...

1. Hacking: Simply put, hacking is the permission of an intruder. Hackers are basically computer programmers, who have advanced knowledge about computers and usually misuse this knowledge for wrong reasons. They are usually technologists who have expert level skills in a particular software program or language. As intended, there may be many, but the most common are very simple and can be explained by human instincts such as greed, fame, power, etc. Some people do it entirely to show off their skills through relatively harmless activities. Such as improving software and even hardware to carry out tasks beyond the manufacturer's purpose, others seem to be destroyed. Due to greed and sometimes voluntary tendencies, a hacker can break into the system to steal personal banking information, corporation financial data, etc…
2. **Virus Diffusion:** Viruses are computer programs that attach themselves to systems or files and infect them, and tend to spread to other computers on the network. They disrupt computer operations and affect stored data either by modification or deletion altogether. Unlike viruses, "worms" do not require a host to stick to. They only make replicas without consuming all the available memory in the system. The word "worm" is sometimes used for the selfish purpose of "malware". The term is frequently changed in reference to hybrid viruses / worms that

dominate the current viral situation. Trojan horses differ from viruses in their mode of transmission. They masquerade as legal files, such as email attachments from a friend with a trusted name and do not spread you.

3. **Logic Bomb:** A logic bomb, also known as a "slag code", is a piece of malicious code that is intentionally inserted into software to perform malicious actions when triggered by a specific event. It is not a virus, although it usually behaves the same. This program is inserted precisely into the program where it is dormant until a specific program is completed. Malicious software, such as viruses and worms, often contain logic bombs that run on a specific payload or at a predetermined time. Payload of logic bombs to the user of the software and it performs unwanted functions. Codes programmed to execute at a particular time are known as "time-bombs." For example, the infamous “Friday the 13th” virus attacked the host system only on certain dates; Every Friday it "exploded" (duplicated itself) which was the thirteenth of the month, so the system slows down. Logic bombs are usually assigned by disgruntled employees working in the IT sector. You may have heard of "Dissatisfied Employees Syndrome" in which employers of fired angry employees use logic bombs to delete databases, temporarily stabilize networks, or even trade internally. The trigger associated with the execution of a logic bomb could be a specific date and time, an entry not received from the database, or a failure to place commands at the usual time, meaning that the person no longer works there. Many logic bombs only stay in the network in which they work. So often they are an internal affair. This makes them easier to design and operate than viruses. No need to duplicate it; which is a more complex task. To protect your network from logic bombs, you need constant monitoring of data on every computer on the network and efficient anti-virus software.
4. **Phishing:** This is a technique to extract confidential information, such as credit card numbers and username passwords, under the guise of a legitimate enterprise. Phishing is usually carried out through email spoofing. You may have received emails with links to legitimate websites. You may have been suspicious and have not clicked on the link. The malware may have installed itself on your computer and stolen private information. Cybercriminals use social engineering to trick you into downloading malware from the Internet or filling out your personal information under false pretences. There are a few things to keep in mind when it comes to phishing scams in email.
5. **Email Spamming and Bombing:** Email bombing is characterized by a victim's email account or mail server crashing as a result of a large number of emails being sent to the target address by a prohibited user. Message is useless and too long to use resources. If multiple accounts on the mail server are targeted, denial of service may result. Frequent mail in your mail can be easily detected by the spam filter. Email bombing is usually carried out using botnets (private Internet connected computers whose security is compromised by malware and under the control of attackers) as a DDOS attack.
6. **Web Jacking:** Web jacking is called "hijacking". Here, the hacker fraudulently takes control of the website. It may change the content of the original site or redirect its controlled user to another fake similar page. The owner of the website no longer has control and the attackers may use the website for their own benefit. Cases of ransom have been reported by the attackers, as well as pornographic material posted on the site. The attack of the web jacking method can be used to create a clone of the website and to present the victim with a new link stating that the site has been moved. Unlike the usual phishing methods, when you hover your cursor over the provided link, the URL presented will be original, not the attacker's site. But when you click on a new link, it opens and is quickly replaced with a malicious web server. The name on the address bar will be slightly different from the original website which will make the user think that it is a legal site.
7. **Cyber Stalking:** Cyber stalking is a new form of internet crime in our society when a person is being pursued or followed online. A cyber stalker does not physically follow your victim; He literally does this through his online actions to gather information about the pastor and to harass and verbally threaten him. This is an attack on someone's online privacy. Cyber stacking uses the Internet or any other electronic means and is different than offline stacking, but usually with it. The most common victims of this crime are women who are victimized by men and children by adult predators and paedophiles. Cyber stalkers thrive on inexperienced web users who are unaware of the rules of native and internet safety. A cyber stalker may be a stranger, but a person you know can easily become a stranger.
8. **Data Diddling:** Data dissection is the process of unauthorized exchange of data before or during access to a computer and back after the process is complete. Using this technique, the attacker can improve the expected output and is difficult to track. In other words, the information that will be entered is altered, the virus programmed to alter the data, the programmer or creator of the database or of application, anyone else involved in the recording process, encoding, checking, investigating, converting or transmitting data is the easiest computer related crime. There is a method, because even a computer amateur can do it. Although this is an easy task, it can have detrimental effects. For example, a person in charge of accounting indicates that the data may change, either for himself or for a friend or relative. They are able to steal from the enterprise if the information changes or fails. Other examples include forging or forging documents and exchanging valid computer tapes or cards with ready-made replacements. Electrical circles in India have fallen victim to data diddling by computer criminals when private parties were computerizing their systems.

Conclusion:

Any smart device that can send data to one or more other devices is within the scope of cyber security which covers the entire foundation of modern society. Everyone needs to be aware of cyber security as well as cybercrimes and the reasons behind them. There is little seriousness about safety regarding online, social and other activities that would increase the risk. This has led to data loss, data modification, removal of useful information such as personal information, mail account passwords, social accounts or bank accounts. People can know about cybercrime laws or cyber laws and what action will be taken and how to fight crime.

References:

1. Bhanu Sahu, Neeraj Sahu, Swatantra Kumar sahu, and Priya Sahu (2013), 'Identify Uncertainty of Cyber Crime and Cyber Laws', International Conference on Communication Systems and Network Technologies Gwalior : IEEE, pp. 450 – 452.
2. Fawn T. & Paternoster R. (2011), 'Cybercrime Victimization: An examination of Individual and Situational level factors', International Journal of Cyber Criminology, Vol-5, pp. 773-793.
3. Moon B., Mccluskey J., Mccluskey C. (2010), 'A general theory of crime and computer crime: An empirical test', Journal of Criminal Justice, Vol-38, Issue-4, pp. 767-772.
4. Reith, M., Carr, C., & Gunsch, G. (2002), 'An examination of digital forensic models, International Journal of Digital Evidence', Vol-1, Issue-3, pp. 1-12.
5. Rachna Buch, Dhatri Ganda, Pooja Kalola et al. (2017), 'World of Cyber Security and Cybercrime', Recent Trends in Programming Languages, Vol-4, Issue-2, pp. 18–23.
6. Alansari, M. M., Aljazzaf, Z. M., & Sarfraz, M. (2019), 'On Cyber Crimes and Cyber Security', In M. Sarfraz (Ed.), Developments in Information Security and Cybernetic Wars, pp. 1-41. IGI Global, Hershey, PA, USA.
7. Hewett R., Rudrapattana S., and Kijsanayoth P. (2014), 'Cyber-security analysis of smart SCADA systems with game models', Proceedings of the 9th annual cyber and information security research conference, ACM, 2014, pp. 109–11

Biographies:

Author: Sayyed Muhammed has Master of Engineering in Digital communication and Networking and Two M.B.A Degrees and a Post Graduate Diploma in Cyber Security. He is working in IT industry in the area of cloud computing and Cyber Security as a Technology Leader.