CYBER SECURITY

[1]DEVENDRA SINGH CHAUHAN

[2]KRISHNA MAHOR]

[3]RANDEEP KUMAR SAHU

[1]MCA, CCSIT, TMU, MORADABAD
[2]MCA, CCSIT, TMU, MORADABAD
[3]ASSIT.PROF, CCSIT, TMU, MORADABAD
[1] deveshchauhan170@gmail.com
[2]krishnarajpoot97@gmail.com
[3]randeep.computers@tmu.ac.in

Abstract

Cyber security, also referred to as information technology security, focuses on protecting computers, networks, programs and data from unintended or unauthorized access, change or destruction.The state of being protected against the criminal or unauthorized use of electronic data, or the measures taken to achieve this.

INTRODUCTION

CYBER SECUIRITY

Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk
management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment.

1. INTERNET

Internet is among the most important inventions of the 21st century which have affected our life. Today internet have crosses every barrier and have changed the way we use to talk, play games, work, shop, make friends, listen music, see movies, order food, pay bill etc.The technology have reached to an extent that we don‟t even require a computer for using internet. Now we have internet enabled smartphone, palmtops, etc. through which we can remain connected to our friends, family and office 24x7.

2.CYBER CRIME

The internet was born around 1960‟s where its access was limited to few scientist, researchers and the defence only. The term cyber crime is used to describe a unlawful activity in which computer or computing devices such as smartphones, tablets, Personal Digital Assistants (PDAs), etc. which are stand alone or a part of a network are used as a tool or/and target of criminal acitivity .

Classification of Cyber Crimes

The cyber criminal could be internal or external to the organization facing the cyber attack. Based on this fact, the cyber crime could be categorized into two types:

1.Insider Attack:

An attack to the network or the computer system by some person with authorized system access is known as insider attack. It is generally performed by dissatisfied or unhappy inside employees or contractors. The insider attack could be prevented by planning and

installing an Internal intrusion detection systems (IDS) in the organization.

2. External Attack:

When the attacker is either hired by an insider or an external entity to the organization, it is known as external attack. An expreicend network/security administrator keeps regual eye on the log generated by the firewalls as extertnal attacks can be traced out by carefully analysinig these firewall logs. Also, Intrusion Detection Systems are installed to keep an eye on external attacks.

TYPES OF MALWARE

1.Adware
2.Spyware
3.Browser hijacking software
3.Virus
4.Worms
5.Trojan horse
6.Scareware

TYPES OF CYBER CRIME

1.Cyber Stalking
2.Cyber Terrorism
3.Phishing
4.Computer Hacking
5.Spamming
6.Cross Site Scripting
7.Online Auction Fraud
8.Cyber Squatting
9.Web Jacking

10.Internet Time Thefts
11.Denial of Service Attack
12.Data Diddling
13.Email Spoofing

CYBER SECURITY TECHNIQUES

1. AUTHENTICATION

It is a process of identifying an individual and ensuring that the individual is the same who he/she claims to be. A typical method for authentication over internet is via username and password. With the increase in the reported cases of cyber crime by identity theft over internet, the organizations have made some additional arrangements for authentication like One Time Password(OTP), as the name suggest it is a password which can be used one time only and is sent to the user as an SMS or an email at the mobile number/email address that he have specified during the registration process. It is known as two-factor authentication method and requires two type of evidence to authentication an individual to provide an extra layer of security for authentication. Some other popular techniques for two-way authentication are: biometric data, physical token, etc. which are used in asconjunction with username and password.

2. ANTIVIRUS

There are verities of malicious programs like virus, worms, trojan horse, etc that are spread over internet to compromise the security of computer either to destroy data stored into the computer.

To prevent these malicious codes to enter to your system, a special program called an anti-virus is used which is designed to protect the system against virus.

There are many cyber security techniques to combat the cyber security attacks.The next section discusses some of the popular techniques to counter the cyber attacks.

Fig .1- Antivirus cyber security

3. ENCRYPTION

It is a technique to convert the data in unreadable form before transmitting it over the internet. Only the person who have the access to the key and convert it in the readable form and read it. Formally encryption can be defined as a technique to lock the data by converting it to complex codes using mathematical algorithms. The code is so complex that it even the most powerful computer will take several years to break the code. This secure code can safely be transmitted over internet to the destination. The receiver, after receiving the data can decode it using the key. The decoding of the complex code to original text using key is known as decryption. If the same key is used to lock and unlock the data, it is known as symmetric key encryption.

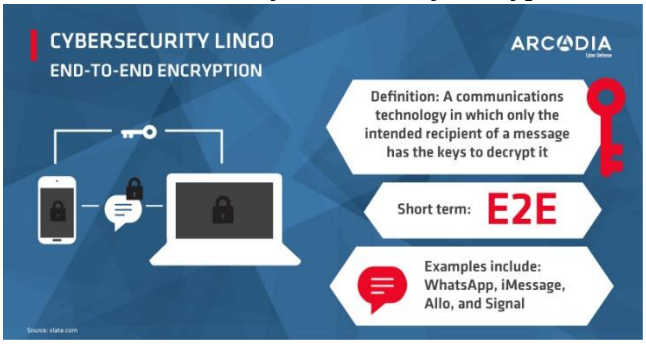

Fig.2- Encryption cyber security

4. DIGITAL SIGNATURES

It is a technique for validation of data. Validation is a process of certifying the content of a document. The digital signatures not only validate the data but also used for authentication. The digital signature is created by encrypting the data with the private key of the sender. The encrypted data is attached along with the original message and sent over the internet to the destination. The receiver can decrypt the signature with the public key of the sender. Now the decrypted message is compared with the original message. If both are same, it signifies that the data is not tempered and also the authenticity of the sender is verified as someone with the private key(which is known to the owner only) can encrypt the data which was then decrypted by his public key. If the data is tempered while transmission, it is easily detected by the receiver as the data will not be verified. Moreover, the massage cannot be re-encrypted after tempering as the private key, which is posses only by the original sender, is required for this purpose.

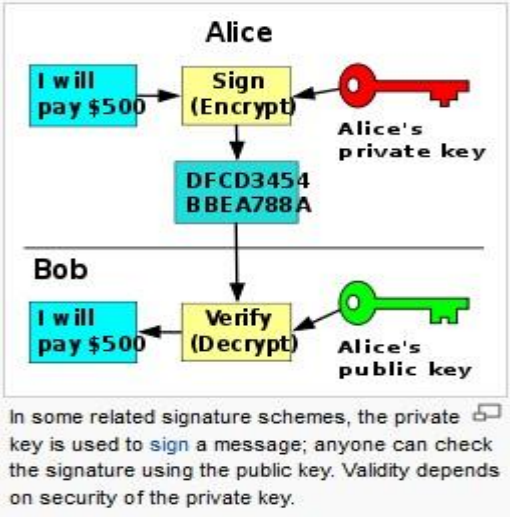

Fig.3- Digital singnatures security

5. FIREWALL

It is a hardware/software which acts as a shield between an organization's network and the internet and protects it from the threats like virus, malware, hackers, etc. It can be used to limit the persons who can have access to your network and

send information to you. There are two type of traffic in an organization viz. inbound traffic and outbound traffic.

Using firewall, it is possible to configure and monitor the traffic of the ports. Only the packets from trusted source address can enter the organization's network and the sources which are blacklisted and unauthorized address are denied access to the network. It is important to have firewalls to prevent the network from unauthorized access, but firewall does not guarantee this until and unless it is configured correctly. A firewall can be implemented using hardware as well as software or the combination of both.

Fig.4.Firewall Internet security

COUNTER CYBER SECURITY INTIATIVES IN INDIA :

To counter cyber security attacks, Government of India have taken some initiatives which are listed below:

1. **National Counter Terrorism Center (NCTC):** After 26/11 attack in 2008, suddenly the Indian government realized the importance of Counter terrorism initiatives and proposed National Counter Terrorism Center (NCTC) to provide intelligence inputs to the decision makers to plan for counter terrorist activities. The NCTC is supposed to coordinate between various State and Central govt. agencies and serve as a single and effective point of control and coordination of all counter terrorism measures. It is modeled on the American NCTC and Britain‟s Joint Terrorism Analysis Centre and will derive its powers from the Unlawful Activities Prevention Act, 1967 (Mrunal, 2012).

2. National Information Security Assurance Programme (NISAP): To create the awareness among the people in the government and critical sector organization, CERT-In has taken an initiative called National Information Security Assurance Programme (NISAP), to develop and implement information security policy and information security best practices based on ISO/IEC 27001 for protection of their infrastructure. CERT-in has established the facility for Computer Forensics for investigation of cyber crimes and to provide hands on training to the law enforcement agencies and judiciary. This infrastructure is being augmented to include network
forensics and mobile forensics investigation facility. CERT-In is cooperating with defence, banks, judiciary and law enforcement agencies in training their officials as well as extending the support in investigation of cyber crimes (Srinath, 2006).

3. Computer Emergency Response Team-India(CERT-In): The Indian Computer Emergency Response Team was created in 2004 by Department of Information Technology. The purpose of creating CERT-In was to respond to computer security
incidents, report on vulnerabilities and promote effective IT security practices
throughout the country and is also responsible for overseeing administration of the IT act (CERT-In, 2014).

4. Indo US Cyber Security Forum (IUSCSF): The India-US Cyber Security Forum was established in 2001 and is dedicated to protecting the critical infrastructure of the knowledge-based economy. The members of the forum are various government and
private sector organizations, both from India and the United States, working under the Forum‟s auspices, have identified risks and common

concerns in cyber security and crafted an action-oriented work plan on securing networked information systems. The Forum focuses on cyber-security, cyber-forensics and related research and works towards enhancing co-operation among law enforcement agencies on both sides in dealing with cyber crime.

5. National Critical Information Infrastructure Protection Centre (NCIPC) of India: It is declared as a nodal agency for the protection of critical information infrastructure of India and is responsible for all measures including R&D for protection of critical information infrastructure.

6. National Intelligence Grid (Natgrid) project of India: It is the integrated intelligence grid developed by C-DAC-Pune connecting databases of core security agencies of the Government of India (C-DAC, 2014). It is a counter terrorism measure that collects and collates a host of information from government databases including tax and bank account details, credit card transactions, visa and immigration records and itineraries of rail and air travel (Yasmeen, 2013).

This combined data will be made available to 11 central agencies.

7. Crime and Criminal Tracking Networks and Systems (CCTNS) project of India: The goals of the CCTNS are to facilitate collection, storage, retrieval, analysis, transfer and sharing of data and information at the police station and between the police station and the State Headquarters and the Central Police

Organizations. CCTNS would provide a comprehensive database for crimes and criminals, and it would be easier for the law enforcement agencies to track down a criminal moving from one place to another.

ACKNOWLEDGEMENT:

Cybersecurity is also sometimes conflated inappropriately in public discussion with other concepts such as privacy, information sharing, intelligence gathering, and surveillance. Privacy is associated with the ability of an individual person to control access by others to information about that person.

CONCLUSIONS:

Computer security is a vast topic that is becoming more important because the world is

becoming highly interconnected, with networks

being used to carry out critical transactions. Cyber crime continues to diverge down different

paths with each New Year that passes and so does the security of the information. Privacy and security of the data will always be top security measures that any organization takes care.

REFERENCES:

[1] Barry M. Leiner, V. G. (s.j.). Brief History of the Internet. Onttrek Dec. 20, 2015 uit http://www.internetsociety.org/internet/what-internet/history-internet/brief-history-internet available under Creative Commons Attribution-NonCommercial-ShareAlike 3.0 Unported License.

[2] CERT-In. (2014). Indian Computer Emergency Response Team.

[3] Chander, M. (2013). National Critical Information Infrastructure Protection Centre (NCIIPC): Role, Charter & Responsibilities.

[4] Cyber Crime Investigation Cell, Mumbai. (s.j.). Onttrek Dec. 20, 2015 uit http://cybercellmumbai.gov.in/

[5] CYBER SECURITY MANIFESTO 2.0. (2012, Oct. 01). Onttrek Sep. 26, 2015 uit cyber security manifesto: http://cybersecuritymanifesto.com/