VOLUME - 9, ISSUE - 10, October - 2020 • PRINT ISSN No. 2277 - 8160 • DOI : 10.36106/gjra

Original Research Paper

Commerce

CYBER SECURITY: CRYING NEED OF THE DAY

Dr. Md. Shahnawaz*

Guest Faculty, LNMU, Darbhanga, Bihar-846004. *Corresponding Author

ABSTRACT

Cyber Security includes application of all the methods to protect the confidentiality, Integrity, availability of cyber information and safety of the data, programs and even entire computer networks from unauthorized access. It plays a vital role in the area of information technology (IT). The Government are taking so many measures to prevent cyber crimes. The present paper attempts to find out components and challenges faced by cyber security regarding information technology. Illegal use of application has transmitted data in wrong way.

KEYWORDS : Introduction, Cyber Security, Security Attacks, Cyber Techniques.

• INTRODUCTION

Cyber Security means infrastructure of technologies, process and practices designed to protect the programs, devices, server, network, and business information from malicious attacks, damage or unauthorized access. It is also called as information technology (IT) security. The main objective of cyber Security is to protect the computers, networks, software from cyber attacks. The Security objectives may include integrity, confidentiality and availability of business information. The objective such cyber attack is to access, alter, and delete the sensitive information form computer. It is also made to interrupt normal business activity and extort money from victims. The Cyber Security is also needed to provide safeguard against the cyber crime which is one of the major crime done by the computer expert. The cyber crime includes illegal access, interception system, interference data and interference misuses of data.

Today, a person can be able receive and send sensitive business information either through e-mail, audio or video messages safely without any risk of its leakage and able to perform on line transaction through Electronic Commerce Operator (ECO). It could be possible only due to Cyber Security. Now-a-days there are so many new technologies; a person is not able to safeguard their sensitive information effectively. Hence cyber crimes are increasing day-by-day. In such a situation, the importance of cyber security is increased. The Cyber Security Techniques may include authentication, encryption, digital signature, anti-virus and firewall etc.

• OBJECTIVE

The main objectives are given below.

To understand the components of Cyber Security.

To identify the challenges faced by cyber security regarding information technology.

To understand the types of Security Attacks and Cyber Security Techniques.

• Elements Of Cyber Security

The components of cyber security may include Application Security, Communication Security, Network Security, and Operational Security etc. The components are discussed as unde

Application Security

The software used to perform business operations by the user must be protected irrespective of the way of acquiring such software. Such software may contain vulnerabilities through which attackers may enter into the system. Basically, this type of security is the use of software, hardware and guidelines adopted the system from external threats. The application security may provide counter measures to the threats which may arise during the phases of System Development Life Cycle (SDLC). These security measures may inbuilt into the system.

Information Security

It is a set of practices required to manage the tools, procedures and policies to protect the digital or non-digital information. It is necessary to maintain the confidentially, integrity and availability of IT systems and business information is only disclosed to authorize person, the integrity refers to prevent unauthorized modification of data and the availability refers to the business information must be accessed by authorize user whenever required by them.

Mobile Security

Today, the cyber criminals are attacking mobile devices and certain apps. In such a situation, the user must try to configure their connections to keep network traffic private. Hence the user of mobile device should control which device can access their network. The security of such devices is more important in the present scenario because now-a-days the user of such device perform many work e.g. financial or non-financial through these devices.

E-mail Security And Network Security

The E-mail security ensures the blocking of incoming mail message from cyber attackers. This type of security protects the loss of sensitive business information. The network security denies access to malicious websites. It also refers to steps to be taken to protect the web site and sensitive business information in the cloud.

• Types Of Cyber Attack

The security attack refers to any action adopted by organization to ensure the security of information held by such organization. There are so many types of attack some of them are given as under.

• DOS Attach

The Denial of Service (DOS) attack is a type of cyber attack which refers to render a computer and other device unavailable to its users by interrupting the normal function of such devices. In this situation, the resource cannot process the requests by intended users or slows or crashes such resources. Generally, there are two methods of DoS attack i.e. flooding services or crashing services. The flood attacks occur when the system receives too much traffic for the server to buffer and causing them to slow down and sometimes completely stop.

• BF Attacks

The Brute Force Attack refers to a situation when an attacker submitting many passwords with the hope of guessing it correctly. In this situation, the cyber attacker systematically enters all possible passwords until the correct one is found. On the other hand, the attacker try to attempt guess the key which

is typically created from the password using a key derivation function. It is also called as trial and error attempt to guess password.

- **Web Browser Attacks**

The web browser means a software application that allows users to view and interact with content on a web page e.g. text, graphics, video, music, games etc. It is a very popular method by which users access the Internet. The web browser attacks focuses on end users who are browsing the internet. These attacks used fake software update or application. Websites are also force to download malwares. To avoid such attacks a user has to update web browsers regularly.

- **SSL Attack**

The SSL is the standard in online security. It is used to encrypt data sent over the Internet between a client (own computer) and a server (web site). This attack automatically prevents many types of attacks: if a hacker intercepts encrypted data then such hacker can't read it or use it without the private decryption key. So, the SSL makes many websites more secure. It provides data in case of theft and modification.

- **Botnet Attacks**

The Botnet owners can have access to several thousand of computers at a time and can command them to carry out malicious activities. First of all, the cyber criminals enter into these devices by using special Trojan viruses to attack the security systems of computer. These attackers are also called as hijackers.

- **Backdoor Attacks**

The backdoor attack is a type of malware that provides cyber criminals unauthorized access to a website. The cyber criminals install the malware through unsecured points of entry. If cyber criminals enter through the back door the access to all sensitive information including customer database. The backdoor attacks added in the programs or created by altering an existing program formulated by its users.

- **Cyber Challenges**

All organizations such as small, large, government sector or private sector organizations prone to cyber attacks from across the globe. Hence, challenges of cyber security should keep on top priority basic for all organizations which are as under.

Advance Persistent Threats (APT)

Advance Persistent threats stays around the server for longer period without getting detected by any person. These threats are designed particularly to highly sensitive information and today the organizations fail to protect it from Advance Persistent threat attacks.

Evolution Or Ransomware

In this situation, a malware penetrates inside the system. Gradually, it starts to encrypt all files on the system and at last, all the files on system get locked and a ransom is being demanded in the form of bit coin. When the payment is made, then a decryption key is being provided by hackers. Then, all data can be decrypted and access is returned back to its user. Thus, the ransomware is the bane of cyber security, IT professionals, and executives.

Internet Of Things (IOT) Threats

The IOT is a system of interrelated computing, digital devices that can transmit data over a network without the need of any human to human/computer intervention. The IOT devices have unique identifier through which it identifies the device. Thus, it leads to increased risk of attacks and gap in securities.

Cloud Security

The organization would not like to put its data on the cloud because the organization would like to be reserved until it is ensured that the cloud is highly secured. However, the cloud attack issues are open for attackers due to its misconfig urat ion, Insecure APIs, human error, data loss due to natural disaster.

- **Steps To Prevent Cyber Crime**

During the process of digitalization, the cyber crime has been major problem in each sector. It cannot be ignored. Hence, the Government has undertaken certain measures for the resolutions of issues related with cyber security. These measures are as under.

Under Cyber Crime Prevention For Women And Children (CCPWC) Scheme.

The Government of India has released grants to states/union territories to set up a Cyber Forensic Cum Training Laboratory and to organize capacity building programme on awareness of cyber security and investigation programme related to cyber crime.

National Cyber Security Coordinator (NCSC)

The NCSC is under National Security Council Secretariat (NSCS) coordinates with different agencies at the national level for matters related to cyber security.

Information Technology (IT) Act, 2000

The Information Technology Act, 2000 has enacted to provide different provisions to deal with cyber crime and cyber attacks. Basically, it provides legal recognition for electronic communication, e-commerce and cyber crime etc.

Cyber Swachhta Kendra And National Critical Information Infrastructure Protection Centre (NCIIPC)

The Government has recently launched Cyber Swachhta Kendra for detection of malicious programs and it provides free tools for their removal. The Government has also established NCIIPC for protection of critical information infrastructure in the country.

National Cyber Security Policy (2013) Framework And Computer Emergency Response Team (CERT –IN)

The Government has formulated National Cyber Security Policy (2013) to ensure a secure cyber space for people to avoid cyber crime and latest cyber threats. The main objective of establishing CERT-In is to issues alerts and advisories regarding cyber threats and counter measure on regular basis.

- **CONCLUSION**

It has been found that the benefits of cyber security includes improved security of cyberspace, increase in cyber defence, increase in cyber speed, protecting data of company and its information, protects system & computers against virus, worms, malware and spyware, protects networks and resources, fight against computer hackers and identity theft and gives privacy to users. However the cyber security has certain short comings such as costly for average users; Need to keep updating the new software in order to keep security up to date and make system slower than before etc.

The cyber security can be beneficial when certain safety measures are maintained such as use antivirus software, pop-up blocker, uninstall unnecessary software, maintain proper backup, check security settings properly, use secure connectivity, open all attachment carefully, use strong password for negating www crime.

The Government has undertaken certain measures to solve the matters related to cyber security and cyber crime. These counter measures may include establishment of National Cyber Coordination Centre, Under Cyber Crime Prevention for Women and Children (CCPWC) Scheme, National Cyber Security Coordinator (NCSC), Information Technology (IT)

Act, 2000, Cyber Swachhta Kendra and National Critical Information Infrastructure Protection Centre (NCIIPC), National Cyber Security Policy (2013) framework and Computer Emergency Response Team (CERT –In), in order to turn negative into positive.

• REFERENCES

1- Anjana Mishra, Cyber security: A practical strategy against cyber threats, Risks with real world usages, Das-Nhuong Le et al. (eds.), Cyber Security in Parallel and Distributed Computing.
2- Jitendra Jain & Dr. Parashu Ram Pal, A Recent Study over Cyber Security and its Elements
3- Data Warehousing and Data Mining Techniques for Cyber Security by Anoop Singhal.
4- Rachna Buch, Dhatri Ganda, Pooja Kalola, Nirali Board; World of Cyber Security and Cybercrime, Recent Trends in Programming Languages, ISSN 2455-1821, volume 4, Issue 2; stmjournals.com
5- https://www.educba.com/cyber-security-challenges
6- https://www.hackmageddon.com/2020/01/23/2019/-cyber-attacks-statistics/
7- https://www.dsci.in/content/cyber-security-challenges
8- https://www.research gate.net/publication/32 1528686_A_Recent_Stud y_ove r_Cyber_Security_and_its_Elements.