International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 04 Issue: 04 | April -2020 ISSN: 2582-3930

CYBER CRIME AND CYBER SECURITY*

*Author 1: YASH SHARMA
*Author 2: ANANYA SHARMA

*Department of Computer Science Engineering
Dr. Akhilesh Das Gupta Institute of Technology and Management, New Delhi,
India Affiliated to Guru Gobind Singh Indraprastha University

***Abstract*—** Cyber security plays one of the most important part in Information Technology. Basically, it can be termed as a leg on which Information Technology stands on. Storing information has become one the biggest challenge as of today's need, and to prevent that data from intrusion and theft, We need Cyber Security. Cyber Crime is increasing immensely day by day. Recently there have been many Data Breaches which affected billion's of people throughout the globe. Moreover has cost the Companies their reputation and a huge amount of financial loss. To prevent such data breaches and malicious attacks on the data stored we need Cyber Security. This paper basically focuses on various types challenges faced by IT and how to change the face of cyber security and the need to bring advancement in Cyber Security.

Keywords:* C*yber Security, Cyber Crime, Data Breach, Trojans, Malware, Cyber Ethics, Hacking

I. INTRODUCTION

Today we people can send any form of data by just one tap on our computer or mobile screens. Be it an e-mail, audio file, Video file, or be it a document file for that matter. But the data we share with people, is it actually reaching to them specifically? Maybe or Maybe Not. Internet is Rapid growing infrastructure and sharing our private data over t he internet should not be accessed by everyone. For this, Cyber Security comes into play. Cyber Security or Information Technology Security is the protection of computer systems and networks from any kind of data theft or damage to their software or hardware or e-data, as well as misdirection of the services they provide.

But in today's technical environment we cant protect our data just like that, because we don't acquire the complete understanding of these cyber attacks. It seems really easy to send data over just one tap but it can be stolen from the internet just like that too. Today more than 65 percent of money transactions are done online, so this requires high level of security for transaction to get through without getting Bypassed by any sort of Internet Viruses. Since these sort of transaction holds a great value and information, We need to enhance the Cyber security which is essential for every nation's Security and Economic well being.

Technical measures alone cannot prevent these crimes from happening, it is important on the part of law enforcement agencies to investigate such cyber crime and prosecute them. Nations and governments are imposing really strict laws regarding cyber security in order to prevent loss of any sort of sensitive information. Also, on our end we must train ourselves to protect us from these increasing cyber crimes. Hence Cyber Security has become one of the latest issue bothering people across the world. The scope of cyber security is not just limited to Information technology but to various other fields as well.

II. CYBER CRIME

Cybercrime, or computer-oriented crime, is any sort of illegal activity related to crime that involves a computer and a network as its primary means of commission, theft, trafficking in child pornography, stealing identities or violating privacy. The list of Cyber Crime goes on and includes crimes at a major level like terrorism. Technology plays a vital role in our lives and it is getting updated day by dad so is the crime related to it. Cyber crime is likely to hit $6 trillion annually by 2021.These data exploitations are done by people who have core knowledge of hacking -' HACKERS'.

There are 3 types of Hackers;

1) BLACK HAT
2) GREY HAT
3) WHITE HAT

Black Hat - They are also knows as ' CRACKERS'. These are the hackers who hack in order to gain unauthorised access to a system and harm its operations or steal sensitive information by exploitation of system. Black Hat hackers are always considered illegal because they intent to steal the corporate data, damaging the systems, manipulating networks and communications.

Grey Hat - Grey Hackers are a mixture of both Black Hat as well as White Hat. They act without malicious intention, they exploit security weaknesses in a computer system and network without the permission of the owner.

White Hat 'ETHICAL HACKERS' are known to be the White Hat Hackers. They never intent to harm any system or network instead they work opposite of Black hats. They look for the vulnerabilities and fix them to avoid data leakage of any sort. They are usually hires by large companies to avoid system or network break ins.

III. CYBER SECURITY

The world relies on technology now more than before, because of which digital data creation has surged. Businesses and Government store a great amount of data on computers and transmit it across networks to other computers. Every 39 seconds, a cyber crime happens. A major data breach can have a devastating consequences on any company or Government. It can unravel the reputation the company holds through loss of consumer and partner trust. Its estimated that a major data breach can cost a company $3.6millions High-profile data breaches make the top headlines of the media so its important that organisations adopt Cyber Security Experts to assist them if there is even a minor data leak.

Types of Cyber Securities;

1) Antivirus/anti-malware
2) Cloud Security
3) Intrusion Détection System(IDS)
4) Data Loss Prevention(DLP)
5) Identity and Access Management(IAM)
6) Internet of Things Security(IoTS)

Antivirus - These are softwares which scan the computers for any know threats, and can also detect previous unknown threats based on their behaviour.

Cloud Security - It protects the data which is stored in cloud-based services and applications.

Intrusion Detection System - It works to protect computers from any threats by identifying potentially hostile cyber activity.

Data Loss Prevention - It helps in protecting the data by focusing on location, classification and monitoring of information at rest, in use and in motion.

Identity Access Management - It authenticates services to limit and track employee access to protect internal systems from malicious entities.

Internet of Thing Security - IoT refers to a wide variety of critical and non-critical physical systems, like sensors, televisions,Wifi routers etc.

IV. MALWARES AND RANSOMWARE

Malware refer to all types of malicious programs including virus, worms, bugs, bots, root-kits, spyware, Trojans etc. Malware is a short note for Malicious Software, which are used to get the control over a victim's computer by planting the malicious file inside the victim's computer. Trojans are scripts which creates a backdoor for a hacker to enter the victim's network or computer and gain its full control. These Malware can be tricked into mails or any other web-based messaging application to fool the victim and enter the system.

Trojans like TheFatRat, Beast, have their source code available on the internet and makes it easy even for an immature to hack into a computer.

Ransomware is advanced and more dangerous malware which are particularly used to commit financial frauds and extort money from computer users. They are designed to target a particular company or an individual. It's a type of malware that allows the attacker to gain complete gain complete control of the system and restricts access to personal files. It either locks out the victim of the computer screen or encrypts the entire data until the ransom is paid. The two main types of ransomware are 'Crypto' and 'Locker'.

How to Prevent these Malware and Ransomware ?

Malware can be prevented by installing anti-malware softwares which can kill these malware, but for a ransomware, best option is to pay the ransom, because there is no coming out of it using softwares as it is designed to hit a particular target.

There are various other methods which are used to create backdoors to a computer, these script are available on internet to learn and to prevent your computers from such attacks.

V. CYBER SECURITY TECHNIQUES

1) Anti-Virus software

Antivirus softwares are computer programs designed to detect any unusual activity with any sort of file that a computer has, and to disarm or remove it. These softwares have auto-updates which keeps them updated even for the latest viruses. Its a basic necessity for every system to have it.

2) Malware Scanners

These are like anti-viruses too, they sniff if there is any malware or any suspicious code or any harmful file present in the system. Viruses, worms, and Trojan horses are examples of malicious softwares that are grouped together knows as malware.

3) Firewalls

A firewall can be a software as well as hardware too. It doesn't allow hackers to reach out the system through internet. Every data packet receiving or releasing goes through the firewall, that is, everything is examined . The data packets those do not meet the criteria cant be passed through a firewall, Thus is play an important role in detecting trojans and viruses.

4) Password Security for access

Secured access to a computer or a network is the primary step for cyber security. Every system should be password protected with a unique password so that it cant be easily decrypted.

5) Authentication of Data

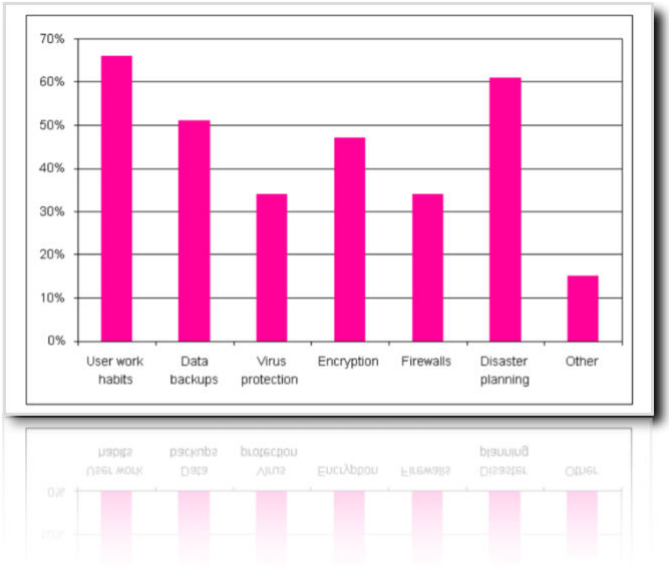
Everything that we download from the internet must be authenticated properly. The documents that we receive must be reviewed before downloading if they are from genuine source and haven't been altered. This thing is usually done by anti-virus, that is why a good anti-virus is always recommended.

6) Data Backups

The data should be stored online in the forms of backup, so that if system goes through any harm via malware, it can be restored easily.

7) Encryption of Data

This is one of the best method to secure data from an attacker. Converting the entire data, can be done by using bit locker (built-in function in window (**"Go to Control Panel > BitLocker Drive Encryptions"**))If the data is encrypted its hard to decrypt and steal.



VI. CYBER ETHICS

Cyber Ethics is the study of ethics related to computers, it covers behaviour of the users and computers, and how it affects an individual as well as society. Internet is considered as world's largest library with information on every topic in the world, so using information in correct way is always essential. Cyber Ethics if followed can lead to better and safer usage of internet. The Government has taken a huge role in making resources for parents and children to learn about cyber Ethics. Few of them are;

Copyright/Downloading;

This has become a major problem due to programs like 'Napster', 'LimeWire' which allows user to download music, programs for free. Many people, especially children do not realise that this behaviour has major consequences. Always adhere to copyrighted information and do download games or videos only if they are permissible.

Hacking;

Hacking or attacking is an intentional damage that a person inflicts onto another computer network. This usually considers stealing classified information from companies or an individual, stealing passwords to get into a site and also changing a website source code without permission. Using any sort of hacking tools to get into a network or into a system without authorisation is considered illegal and can lead to serious consequences.

Cyber Bullying:

Bullying does not only happen in real life anymore. Cyber bullying is growing and people are becoming aware of its effect on children, 'The Megan Meirer' case shed light on this issue that was thought of by many people as harmless bullying, This cyber bullying made the poor girl suicide.

Sharing sensitive information;

Never share your passwords or personal information with anyone as there is a good chance of others misusing it and you could lend yourself in a trouble.

Creating Fake Identity;

Never pretend to be other person on internet and never try to crate fake accounts on someone as it can lend you behind the bars too.

VII. CONCLUSION

Computer, Internet and their security is a vast topic seeking our attention more and more day by day. Due to development of new technology everyday, Cyber crimes are increasing too. Every 39 seconds a cyber crime is reported, that is the reason why we are in such a need of advanced Cyber Security. Hacking knowledge is freely available on resources like'Youtube'. Now it's all dependent on us whether we use it to prevent ourselves from attack or we use it to attack others.Reports say, Cyber crime is gonna cost companies in trillions. This study identified the seven factors that enhances the cyber security in the Computer Sector.

REFERENCES

1. Cyber Security: Understanding Cyber Crimes - Sunit Belapure Nina Godbole
2. Computer Security Practices in Non Profit Organisations - A NetAction Report by Audrie Krause
3. IEEE Security and Privacy magazine - IEEECS "Safety Critical Systems - Next Generation" July/ Aug 2018.
4. https://www.clearias.com/malware-types/
5. https://www.britannica.com/topic/cybercrime
6. https://www.malwarebytes.com
7. https://www.cshub.com/case-studies/whitepapers/case-studies-cyber-security-protects-sensitive
8. https://www.securityaffairs.co/wordpress/category/reports