Cyber Security

AUTHOR: Hemalatha.S
Department of commerce, Sri Krishna Adithya College of Arts and Science
Affiliated to BharathiarUniversity
Coimbatore, India

CO-AUTHOR: I. ANGEL ISHWARYA
Department Of Commerce,
Sri Krishna Adithya Collage Of Arts And Science
Affiated To Barathiyar University
Coimbatore, India

Abstract:
The word Cyber is a combining form relating to information technology, the internet, and virtual reality. Cyber Security or information technology security are the techniques of protecting computers and data from unauthorized access or attacks that are aimed for exploitation. A man named Ray Tomlinson saw the idea of cyber security and made it self-replicating the first computer worm. The first computer virus is created in the early 1970's. Cyber Security is important because government, corporate, financial and medical organizations collect and store huge amount of data on computers and other devices. It is dedicated to protecting that information and the systems where the information are stored. Hacker is a person who breaks into computers, by gaining access to administrative controls. The major security problems are Virus, Hackers, Malware, Trojan horses, Password cracking. From these threats cyber security protects the data and integrity of computing assets belonging to an organizations network.

Keywords: Technology, security,protection, information, attacks, hackers, threats, cyber breaches, cracking, recognition.

I. INTRODUCTION:

Cyber Security is primarily about process, and technologies working together to encompass the full range of threat reduction, vulnerability reduction, incident response, and recovery policies and activities, including computer network operations, information assurance, law enforcement. It enables organizations to practice safe security techniques to minimize the number of successful cyber security attacks caused by the hackers.

II. OBJECTIVE OF THE STUDY:

- To understand what is cyber security?
- To explain the importance of cyber security.
- To know the cyber threats and how to protect the system and the data contained in it.

What is cyber security?

Cyber Security is the protection of internet connected systems, including hardware, software, and data from cyberattacks, damage or unauthorized access. The word cyber is related to the technology which contains systems, network and program or data. The word security is related to the protection which includes systems security, network security, application and information security. With an increasing amount of people getting connected to internet, the security threats that causes massive harm are also increasing.

III. IMPORTANCE OF CYBER SECURITY

Cyber security has become a major concern over the last few years as hackers have penetrated the IT (Information Technology) infrastructure of government and enterprises with increasing frequency and sophistication. Cyber security is important because government, military, corporate, financial and medical organizations collect, process, and store unprecedented amounts of data on computers and other devices. A significant portion of that data can be sensitive information, whether that can be financial data or other type of data from which unauthorized access could have negative consequences.

Organizations transmit sensitive data across networks and to other devices in the course of doing businesses, and cyber security is dedicated to protecting that information and the systems used to process or store it. Cyber security ensures safer data processing and facilitates secure and reliable collaboration that protects the privacy of individuals. It prevents companies from hacking, phishing and attacks. It ensures safety of online transactions and personal information exchanged over the internet.Having the right level of preparation and specialist assistance is vital to minimize and control damage, and recover from a cyber breaches and its consequences.

IV. FEATURES OF CYBER SECURITY

Recent statistics show that 60% of businesses are forced to suspend operations after a cyberattack are never able to reopen for business. This is largely due to revenue lost due to downtime as well as damage to the company’s reputation. These threats can be mitigated with reliable cyber security.

Data Breach Prevention- data breaches happen when cyber criminals successfully attack systems that hold sensitive information. Business can employ standard security software such as antivirus and intrusion detection systems to defend against data leakages by monitoring sensitive files and data transfers.

Phishing Prevention- phishing involving the use of digital messages by cyber criminals to steal credit card information, user logins and other types of sensitive data. Installation of security systems and updating of all software are essential methods to greatly reduce phishing attacks.

Ransomware Prevention and Detection- the average ransomware attack costs a company a whopping $133000. Cyber criminals make use of malicious software to encrypt a victim’s data and then demand ransoms in order to decrypt the data. One of the measures is to use updated security software, have a good backup and restore plan and also to train employees on how to avoid emails that may carry ransomware.

V. BENEFITS OF CYBER SECURITY:

A. Benefits for the business:

- ❖ Protection for your business- cyber security provide digital protection to your business that will ensure your employees aren’t at risk from potential threats such as Adware and Ransomware.

- Increased productivity- viruses can slow down computers to a crawl, and making work practically impossible. Effective cyber security eliminates this possibility, maximizing your business potential output.
- Inspires customer confidence- if you can prove that your business is effectively protected against all kinds of cyber breaches, you can inspire trust in your customers that their personal data will not be compromised.
- Stops your websites from going down- if your business that hosts your own websites, a potential cyber breach could be disastrous. If your system becomes infected, it's possible that your website could be forced to close meaning you will lose money as a result from lost transactions.

B. Benefits for the government:

- e-Government- full secure and cost effective delivery of online services to both citizens and businesses, such as taxes and customers, social welfare, civil and land registries, passports and driving licenses.
- e-Defense- early warning, alerts and defenses against cyberattacks through national CIRT (Computer Emergency Response Centre).

VI. CYBER CRIME IN INDIA

Artifice (fraud) from mobile apps has increased by 680% between 2015 and 2018, with frauds originating in mobile channels growing by 70% in 2018.

Steps taken by Government:

- Government has undertaken number of legislative, technical and institutional measures for addressing cyber security issues and strengthening cyber security system in country.
- National Cyber Security Coordination (NCSC).
- Information Technology (IT) Act 2000.
- National Critical Information Infrastructure Protection Center (NCIIPC).
- Cyber Crime Prevention for Women and Children (CCPWC) scheme.

VII. TYPES OF HACKERS:

Hacker:

A hacker is a person who is intensely interested in the mysterious working of any computer operating system. Hackers are most often programmers. They gather advanced knowledge of operating systems and programming languages and discover loopholes within systems and the reasons for such loopholes.

- **Black Hat Hackers:**

Black Hat Hackers are called Crackers. They can gain the unauthorized access of your system and destroy your vital data. They find banks or other companies with weak security and steal money or credit card information. The truth about their methods of attack is that they often use common hacking practices they have learned earlier. They are considered to be as criminals and can be easily identified because pf their malicious actions.

- **White Hat Hackers:**

White Hat Hackers are also known as Ethical hackers are the one who is authorized or the certified hackers who work for the government and organizations by performing penetration testing and identifying loopholes in their cyber security. They also ensure the protection from the malicious cybercrimes. They work under the rules and regulations provided by the government, that's why they are called Ethical hackers or Cyber Security experts.

- **Grey Hat Hackers:**

Grey Hat Hackers fall somewhere in the category between white hat or black hat hackers. They are not legally authorized hackers. They work with both good and badintensions; they can use their skills for personal gain. Since grey hat hackers don't have permission to access the system by its owner, their actions are ultimately considered illegal, despite any alarming finding they might reveal.

- **Hacktivists:**

Hacktivists is a hacker who gain unauthorized access to government files and network for further social or political ends.

VIII. CYBER SECURITY THREATS

- **Malware:**

Malware refers to various forms of harmful software, such as viruses and ransomware. Once malware is in your computer, it can wreak all sorts of havoc, from taking control of your machine, to monitoring your actions and keystrokes, to silently sending all sorts of confidential data from your computer or network to the attacker's home base.

- **Phishing:**

It is a kind of fraudulent attempt that is made through email, to capture personal and financial information. Perpetrator sends e-mail that seems to come from well known and trustworthy address ask for your financial information, such as bank name, credit card number, social security number, account number or password.

- **Ransomware:**

An attack that involves encrypting data on the target system and demanding a ransom in exchange for letting the user have access to the data again.

- **Trojan Horse:**

It is named after the Trojan horse of ancient Greek history, Trojan is a type of malware that enters a target system looking like one thing, example: a standard piece of software, but then lets out the malicious code once inside the host system.

IX. CONCLUSION

Significant statistics show that India stands on third position in the usage of internet and also experiencing the problem of cyber security. Technology is destructive only in the hands of people who do not realize that they are one and the same process as the universe.Cybercrime is indeed getting the recognition it deserves. However, it is not going to restricted that easily. In fact, it is highly likely that cybercrime and its hackers will continue developing and upgrading to stay ahead of the law. An increased investment in research that could help address cybersecurity vulnerabilities while also meeting socio-economic needs and national security requirements is necessary. So, to make us a safer we must need cyber security.

REFERENCES:

- https://www.csis.org/news/cybersecurity
- http://cybersecurityventures.com/cybersecurity-education/
- http://cset.nsu.edu/programs/k20cybersecurity
- https://searchsecurity.techtarget.com
- http://digitalguardian.com
- http://economictimes.indiatimes.com