International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 4 Issue 6, September-October 2020 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

Cyber Security

P. H. Gopi Kannan, A. Karthik, M. Karthikeyan

Student, Sri Krishna Adithya College of Arts and Science, Bharathiar University, Coimbatore, Tamil Nadu, India

ABSTRACT

As more business activities are being automated and an increasing number of computers are being used to store sensitive information, the need for secure computer systems becomes more apparent. This need is even more apparent as systems and applications are being distributed and accessed via an insecure network, such as the internet. The internet itself has become critical for governments, companies, financial institutions, and millions of everyday users. Networks of computers support a multitude of activities whose loss would all cripple these organizations. As a consequences Cyber Security issues have become national security issues. Protecting the internet is a very difficult task. Cyber Security can be obtained only through systematic development.

KEYWORDS: *Cyber-security, Cyber-crime, Hacking and Phishing*

How to cite this paper: P. H. Gopi Kannan | A. Karthik | M. Karthikeyan "Cyber Security" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-4 | Issue-6, October 2020, pp.658-662, URL: www.ijtsrd.com/papers/ijtsrd33483.pdf

IJTSRD33483

Copyright © 2020 by author(s) and International Journal of Trend in Scientific Research and Development Journal. This is an Open Access article distributed under the terms of the Creative Commons Attribution License (CC BY 4.0) (http://creativecommons.org/licenses/by/4.0)

1. INTRODUCTION

Cyber Security refers to a set of techniques used to protect the integrity of networks, programs and data from attack, damage or unauthorized access. The use of Cyber Security can help prevent from cyber attacks, data breaches, and identity theft and can aid in risk management. A very wide - ranging term with no standard definition. It covers all aspects of ensuring the protection of citizens, businesses and critical infrastructures from threats that arise from their use of their computers and the internet. With an increasing amount of people getting connected to the internet, the security threats that cause massive harm are increasing also. It means securing information related to the internet. Cyber Security can therefore be considered as a subset of information security.

2. Types of Cyber Security:

The 5 main types of Cyber Security are

- **Critical Infrastructure Security:**

Critical infrastructure security consists of the cyber – physical systems that modern societies rely on. Some common examples of critical infrastructure:

- Electricity grid
- Water purification
- Traffic lights
- Shopping centers
- Hospitals

Having the infrastructure of an electricity grid on the internet makes it vulnerable to cyber – attacks. It's the area of concern surrounding the protection of systems, networks and assests whose continuous operation is deemed necessary to ensure the security of a given nation, its economy, and public's health and/or safety.

- **Application security:**

Application security refers as the one of the several must have security measures adopted to protect your systems. It uses the software and hardware methods to tackles the external threats that can arise in the development stage of an application. Types of application security:

- Antivirus programs
- Firewalls
- Encryption programs

Application security focuses on keeping software and devices from free threats. A compromised application could provide access to the data its designed to the product. It help to prevent data or code within the app from being stolen or hijacked. The application security procedures is to identify or minimize security vulnerabilities.

- **Network Security:**

As Cyber Security is concerned with outside threats, network security guards against unauthorized intrusion of your internal networks due to malicious intent. Network security ensures that internal networks are secure by protecting the infrastructure and inhibiting access to it. It is a board terms that covers a multitude of technologies, devices and processes. In its simplest form it is a set of rules and configuration designed to protect the integrity, confidentially and accessibility of computer networks and data using both software and hardware technologies. Some common examples of network security implementation:

- Extra logins
- New passwords
- Application security
- Antivirus programs
- Anti spy software

- Encryption
- Firewalls
- Monitored internet access

- **Cloud Security:**

Improved Cyber Security is one of the main reasons why the cloud is taking over. Cloud security is the software-based security tool that protects and monitors the data in your cloud resources. Cloud providers are constantly creating and implementing new security tools to helps the enterprise users better secure their data. It's the protection of data stored online via cloud computing platforms from theft, leakage and deletion. Several methods of providing cloud security include firewalls, penetration testing, obfuscation, tokenization, virtual private networks (VPN), and avoiding public internet connections. The report further finds that

- On -premise environment users experience an average of 61.4 attacks.
- Service provider environment customers experienced an average of 27.8 attacks.

Without the time and cost of high maintaining huge data facilities and the risk of security breaches is minimal.

- **Internet Of Things Security (IOT)**

IOT refers to a wide variety of critical and non-critical cyber physical systems, like appliances, sensors, televisions, wifi - routers, printers, and security cameras. IOT data center, analytics, consumer devices, networks, legacy embedded systems and connectors are the core technology of the IOT market. IOT devices are frequently sent in a vulnerable state and offer little to no security patching. This poses unique security challenges for all users. It focuses on protecting your internet enabled devices that connect each other on wireless networks. IOT security is the safest components tied to the internet of things, and it strives to protect IOT devices and networks against cybercrime. Overall Cyber Security is essential to govern the conducts and manners of interacting with computer systems from suspicious behavior. As hackers continue to adapt to progressing technology, so will the it security experts whose main focus is to keep our data secure.

3. Principles Of Cyber Security:

When implementing Cyber Security, there are two specific goals to be attained first, confidential information must be kept out of reach of potential cyber attackers and other unauthorized individuals. Second, Cyber Security measures must not hinder authorized users access to the information. The following are the three main principles of Cyber Security.

- **Confidentiality:**

Cyber Security should ensured that the information should be secured is only accessible to the authorized users and prevents the disclosure of the information to unauthorized parties. Access to information must be restricted only to those who are authorized to view the required data. Data can be categorized according to the type and severity of damage that could happen to it should fall into unauthorized hands. Once the secrets has been revealed there is no way to un-reveal it. Most systems also implement confidentiality through data encryption, which is an additional layer of the security. The failure of confidentiality commonly known as breach. Decryption of the data requires an individual or system to attempt access using the requisite key. So in summary a breach of confidentiality means that someone gain access to the information who shouldn't have access to it.

- **Integrity:**

Cyber Security efforts should ensure information remains accurate, consistent and subject not to unauthorized modification. Consistency, accuracy and trustworthiness of data should be maintained over its lifecycle. Sensitive data should not be altered in transit, and security measures, such as file permissions and user access controls, should be taken to make sure that it cannot be modified by unauthorized users. The failure of integrity is when you try to connect to your website and a malicious attacker between you and the website redirects your traffic to the different website. In that case, the site you are directed to is not genuine. In addition, backups or redundancy plans should be planned and implemented to restore any affected data in case of integrity failure or security breach in order to restore data back to its correct state.

- **Availability:**

Efforts to secure information in cyberspace should not hinder its access by an authorized party. Additionally Cyber Security implementation has to provide redundancy access in case of any outage. It is best guaranteed by properly maintaining all hardware and software necessary to ensure the availability of sensitive data. It is also important to keep up with the system upgrades. A routine backup job is advised in order to prevent or minimize total data loss from such occurences. To prevent data loss, backup should be located in a geographically separate location, and in a fireproof, waterproof vault. Dedicated hardwares can be used to guard against downtime and unreachable data due to malicious actions such as distributed denial of service (DDOS) attacks.

4. Types Of Cyber threats:

The threats countered by Cyber Security are three - folds:

- **Cybercrime:**

It includes single actors or groups targeting systems for financial gain or to cause disruption.

- **Cyber-attack:**

It often involves politically motivated information gathering.

- **Cyber terrorism:**

It is intended to undermine electronic systems to cause panic or fear.

The types of cyber attacks are:

- **Malware:**

Malware means malicious software. One of the most common cyber threats, malware is software that a cybercriminal or hacker has created to disrupt or damage a legitimate's user computer. Malware is the general term that covering all the different types of threats to your computer safety. It can attach itself to legitimate code and propagate; it can lurk in useful applications or replicate itself across from the internet.

The types of malware are

- **Virus:**

A self - replicating program that attaches itself to clean file and spreads throughout a computer system, infecting files with malicious code. Many viruses are harmful and can destroy data, slow down systems resources, and log keystrokes.

- **Trojans:**

A Trojan or Trojan horse is a program that hides in a useful program and usually has a malicious function. A major difference between viruses and Trojans is that Trojans do not self – replicate. Cybercriminals trick users into uploading Trojans onto their computer where they cause damage or collect data.

- **Spyware:**

A program that secretly records what a user does, so that cybercriminals can make use of this information.

- **Adware:**

Advertising software which can be used to spread malware.

- **SQL Injection:**

An SQL (Structured Query Language) injection is a type of cyber attack used to take control of and steal data from a database. SQL injection attack has become a common issue with database-driven websites. It occurs when a malefactor excuses a SQL query to the database via the input data from client to server. This gives them access to the sensitive information contained in the database.

- **Phishing:**

Phishing attack is that the practice of sending emails that appear to be from trusted sources with the goal of gaining personal information or influencing users to do something. It could involve an attachment to an email that loads malware onto your computer. Cybercriminals target victims with emails that appear to be form a legitimate company asking for sensitive information. Phishing attacks are often used to dupe people into handing over credit card data and other personal information.

- **Denial-Of-Service Attack(DOS):**

A denial-of-service-attack overwhelms a system's resources so that it cannot respond to service requests. A DDoS attack is also attack on system's resources, but it is launched from a large number of other host machines that are infected by malicious software controlled by the attacker. This renders the system unusable, preventing an organization from carrying out vital functions.

- **Man-In-The-Middle-Attack(MITM):**

A man-in-the-middle attack is a type of cybercriminal threat where a cybercriminal intercepts communication between two individuals in order to steal data.

Here some common types of man-in-the-middle attacks:

- **Session Hijacking:**

In this type of MITM attack, an attacker hijacks a session between a trusted client and a network server. The attacking computer substitutes its IP address for the trusted client while the server continues the session, believing its communicating with the client. The attack relies on the attacker's knowledge of your session cookie, so it is called cookie hijacking.

- **IP Spoofing:**

IP spoofing is used by an attacker to convince a system that is communicating with a known trusted entity and provide the attacker with the access to the system. The data transmitted over the internet is first broken into multiple packets, and those packets transmitted independently and reassembled at the end.

- **Replay:**

A replay attack occurs when an attacker intercepts and saves old messages and then tries to send them later, impersonating one of the participants. This type can be easily countered with session timestamps or a random number of strings that changes with time. The added danger of replay attacks is that a hacker doesn't even need advanced skills to decrypt a message after capturing it from the network. The attack could be successful simply by resending the whole thing.

5. Advantages Of Cyber Security:

Cyber Security refers to arrange of concepts including the practice protecting an organization's information, networks, computers, and resources against the attacks from security and computer attacks. It also saving the users from possible cyber attacks it also warn it from potential risks. Cyber Security plays an important role to guarantee and protect people who use internet usage purposes.

The advantages of Cyber Security are:

- Protects the system from the viruses, worms, spyware and other unwanted programs.
- Protection against data from theft.
- Protection from the malicious attack on your computer.
- Risk mitigation.
- Evade loss of crucial data.
- Valuable information protection.
- It helps us to browse the safe website.
- The application of Cyber Security used in our PC needs updated every week.
- Improved security of cyberspace.
- Gives privacy to users.

6. Disadvantages Of Cyber Security:

So as to give a powerful digital security component inside of an association, it is required to adjust all the endeavours through its information system. It protects individual private information for businesses. It protects individual private information. It protects network and resources, and tackles computers hackers and theft of identity.

The disadvantages of Cyber Security are:

- Firewalls can be difficult to configure correctly.
- Makes the system slower than before.
- Need to keep updating software in order to keep security up to date.

- It will be costly for average users.
- Improved hacker speed and ability.
- Cyber Security can be a costly affair; as highly trained professionals are required.
- Latest security patches must be updated regularly.
- Incorrectly configured firewalls may block users from performing certain actions on the internet, until the firewall configured correctly.

7. Safety tips for Cyber Security:

The internet has become a space riddled with malicious links, Trojans, and viruses. Data breaches are becoming more frequent, and unsuspecting users are more vulnerable than even before. Here's a deeper dive into the 10 Cyber Security safety tips that everyone should know and follow.

- **Keep Software Up To Date:**

Software patches can be issued when the security flaws are discovered. One of the most important Cyber Security tips to mitigate Ransomware is patching outdated software, both operating system and applications. Always install the latest security updates for your devices:

- Turn on automatic updates for your operating system.
- Use web browsers such as chrome or firefox that receive frequent, automatic security updates.
- Keep your web browser plugins like flash, java, etc. updated.

- **Clicking Without Thinking Is Reckless:**

Just because you can click, doesn't mean you should. Remember it can cause you a hefty sum. Malicious link can do damage in several different ways. Avoid visiting unknown websites or downloading software from untrusted sources. These sites often host malware that will automatically install and compromises your computer. If attachments or links in the email are unexpected or suspicious for any reason, don't click on it.

- **Use Two-Factor Authentication:**

It's important to have strong password but it's even more imperative to have two-factor, or multi-factor, authentication. Without two-factor authentication, you would normally enter a username and password. A password management program helps you to maintain strong and unique passwords for all of your accounts. The truth is passwords are important in keeping hackers out of your data.

- Don't use the same password twice.
- Choose something that is easy to remember and never leave a password hint in open or make publicity available for the hackers to see.
- Reset your password when you forget it.

- **Lookout For Phishing Scams:**

Phishing attacks are some of the greatest Cyber Security threats as they are very easy to fall for. In a phishing attack, a hacker will pose as someone that the recipient may be familiar with to trick them into opening a malicious link. Phishing scams are a constant threat using various social engineering ploys, cyber-criminals with attempt to trick you into divulging personal information such as your login ID and password, banking or credit card information. This often leads to a Ransomware attack.

- **Use Anti-Virus Protection & Firewall:**

Anti-Virus protection software has been the most prevalent solution to fight malicious attacks. AV software blocks malware and other malicious viruses from entering your device and compromising your data. Use AV software from the trusted vendors and only run one AV tool on your device. Firewalls prevent unauthorized users from accessing your websites, mail services, and other sources of information that can be accessed from the web. Your router should also have a firewall built in to prevent attacks on your network.

- **Connect Securely:**

You might be tempted to connect to your own device to an unsecured connection, but when you weigh the consequences its not worth it. Don't use public Wi-Fi without using a virtual private network (VPN). By using a VPN the traffic between your device and the VPN server is encrypted. Its easy for a cybercriminal to access your device. Only connect to the private networks when possible especially when handling sensitive information.

- **Secure Your Mobile Device:**

Security doesn't end at your desktop. It's important to get into the habit of securing your presence through your mobile device as well. Always use strong passwords to protect your devices. Don't auto updates using public Wi-Fi .You'll want to make sure that you are protected

- Lock your device with a PIN or password – and never leave it unprotected in public.
- Only install apps from the trusted sources (Apple App store, Google play)
- Keep the device operating system up to date.
- Don't click on links or attachments from unsolicited emails or texts.

- **Never Leave Devices Unattended:**

The physical security of your devices is just as importance as their technical security.

- If you need to leave your laptop, tablet, or I-PAD for any length of time – lock it up so no else can use it.
- You must lock your screen for desktop computers or shut down the system when not in use.
- The data that you keep protected on a flash drive or external hard drive make sure their encrypted and locked up as well.
- Always protect the devices with passwords or PIN numbers to keep your files safe.

- **Protect Your Sensitive Personal Identifiable Information(PII):**

Personal identifiable information (PII) is any information that can be used by a cybercriminal to identify or locate an individual. It includes information such as name, address, phone numbers, date of birth, social security number and IP address. You can review your privacy settings and change all the required information. If it is visible to others it will dramatically increase your risk of a security breach. Hackers use this information to their advantage. So protect your information with high security levels.

- **Back-Up Your Data:**

These days storage doesn't cost much. There's no excuse not to have a backup of important data. Back it up on the physical location and on the cloud. If you are a victim of a security incident, the only guaranteed way to repair your computer is to erase and re-install the system. Back it up to have an ultimate recovery tool.

8. Cyber Security challenges:

Cyber Security is continually challenged by hackers, data loss, privacy, risk management, and changing Cyber Security strategies. With the increase of the cyber attacks, every organization needs a security analyst who makes sure that their system is secured. As new technology emerge and technology is used in new or different ways, new avenue of attacks are developed as well. In our quest to deal with newly emerging threats, we often face challenges that one must deal with to secure their territory. The few main Cyber Security challenges are explained in detail:

➢ Ransomware:

Ransomware is a type of malware in which the data on a victim's computer is locked, and payment is demanded before the ransomed data is unlocked. Ransomware is the bane of Cyber Security, data professionals, IT and executives. Once the payment is made, a decryption key is being provided by hackers, using which all the data can be decrypted back and the access is returned. Data disappears and the business can't revive it. That is unless they pay the cybercriminals. Ransomware is the bane of Cyber Security, data professionals, IT and executives.

➢ Blockchain:

Blockchain technology is the most important invention in computing era. It is the first time in the human history that we have a genuinely native digital medium for peer-to-peer value exchange. The blockchain is a technology that enables a crypto currencies like bitcoin. Many companies adopting crypto currencies technology don't implement appropriate security controls. As a result they will only continue to experience financial losses, predicts, bill weber, principal security. So it is being advised, to understand the security controls before implementing these technologies. Some of the attacks made are Eclipse attack, Sybil attack, and DDOS attack.

➢ IOT Threats:

IOT stands for internet of things. It is a system of interrelated physical devices which can be accessible through internet. The connected physical devices have a unique identifier (UID) and have the ability to transfer data over a network. In today's world, every digital device that we use can be connected with a network and yes it is happening in almost all parts of the globe. The problem is that all of that interconnectedness makes consumers highly susceptible to cyber attacks. In other words, if you access one device, you've accessed them all and this leads to increased risks of attacks and gap in securities.

➢ AI expansion:

AI is short form is Artificial intelligence. It is an area of computer science which is the creation of intelligence machines that do work and react like humans. AI take immediate actions against the malicious attacks at a moment when a threats impact a business. Biometric login is one of the example of artificial intelligence. While this is a good side of it there is a bad side as well. Robots might be able to defend against incoming cyber-attacks. Hackers can also use AI and machine learning to design innovative solutions for performing out more sophisticated attacks. Timing is everything with malware and other vicious data manipulations.

9. Conclusion:

To conclude in this about I have explained all the types, challenges, and safety methods about Cyber Security. Cyber Security is a never-ending battle. The future of Cyber Security will in one sense be like the present hard to define and potentially unbounded as digital technologies interact with human beings across virtually all aspect of politics, society, the economy, and the beyond. Since the attackers have being using an attack life cycle, organizations have also been forced to come up with a vulnerability management lifecycle. Also an increased investment in research that could help address Cyber Security vulnerabilities while also meeting socio-economic needs and national security requirement is necessary. So, only way to be safe is pay attention and act smart.

10. Reference Links:

[1] https://www.kaspersky.co.in/resource-center/definitions/what-is-cyber-security#:~:text=Cyber%20security%20is%20the%20practice,security%20or%20electronic%20information%20security.

[2] https://mind-core.com/blogs/Cyber Security/5-types-of-cyber-security/

[3] https://www.secureworks.com/blog/cyber-threat-basics

[4] https://security.berkeley.edu/resources/best-practices-how-to-articles/top-10-secure-computing-tips

[5] https://sites.google.com/site/xinyicyber/the-disadvantages-and-advantages-of-cyber-security

[6] https://www.javatpoint.com/cyber-security-challenges