Emerging Cyber Security Threats

Rushikesh Patil[1], Pratik Awari[2], Sunny Mhatre[3], Himanshu Ghatole[4]

[1] *Student, Computer Engineering, Pillai HOC College of Engineering and Technology, Maharashtra, India*

[2] *Student, Computer Engineering, Pillai HOC College of Engineering and Technology, Maharashtra, India*

[3] *Student, Computer Engineering, Pillai HOC College of Engineering and Technology, Maharashtra, India*

[4] *Student, Computer Engineering, Pillai HOC College of Engineering and Technology, Maharashtra, India*

ABSTRACT

Cyber security or IT security helps to keep computer systems and networks protected from different kinds of thefts and hackers who basically tries to steal one's personal information/data or even try to hijack networks in an organization. In the year 1971, The world's first virus named creeper was discovered it was created by Bob Thomas a programmer at BBN Technology which is located in Cambridge, Massachusetts. In the year 1983, US was the first country to create a patent for cyber security. The patent introduced an algorithm called RSA (River-Shamir-Adleman) it was the first public key cryptosystems. Now a day's Cyber security is getting important day by day as there is growth in usage of computer systems, Internet and different kinds of smart devices such as smartphones, TVs, smartwatches, smart locks, voice controllers, financial systems, automobile and many more which are equipped with wireless network standard that are Bluetooth and WIFI. All these devices are vulnerable to cyber-attacks as this is the only way an attacker can get access to the system. For cyber-attack, first attacker needs to find security loophole in the network, once he finds out the loophole the attacker can inject malicious file or software in the system. There are various kinds of cyber-attacks such as eavesdropping, Phishing, DoS (Denial of Service) attack, Backdoor attacks, Malware attacks and many more by which hackers can use it to tamper the security of an organization so they can get access to their confidential and private data and misuse it.

Keyword: - *Security, Threat, Malware, Hacker, Network.*

1.Introduction

Cyber security helps to protect system devices such as hardware and software which are connect over a network from cyber threats. It is used by individual and organization to protect against different kinds of cyber-attacks and unauthorized access to their systems. As in year 1971, world's first virus creeper was created by Bob Thomas was a programmer at BBN Technology. The creeper was a worm virus which replicated itself and used to spread to other systems over a network. Bob Thomas was working on an experiment to illustrate self-duplicating program, the creeper was able to gain access to ARPANET (Advanced Research Projects Agency Network) and replicated itself on remote systems where a message saying "I'm the creeper, catch me if can!" was displayed on the systems [1]. Reaper was the first antivirus to remove the virus creeper from infected systems. It was created by Ray Tomlinson, Reaper deleted self-replicating virus creeper by moving across ARPANET [8]. The goal of cyber security is to provide security for devices such as computer system, networks, servers and data stored in these devices from attackers. There are few common categories in cyber security –

1.1 Network Security

Network security helps to protect the network traffic by preventing any suspicious connection entering or spreading into the network. Network security makes sure that networks are secured by using firewalls, monitor network access, packet encryption these implementations help protect the infrastructure and inhibiting access to the network [7].

1.2 Application Security

Application security helps to improve the security of an application program by finding and fixing the vulnerabilities in application code. As applications are being developed it goes under different stages to surface security vulnerabilities. The different stages an application need to go are design, development, deployment, upgrade, and maintenance [7].

1.3 Information Security

Information security is known as data security it helps to protect the integrity and privacy of data to secure it from unauthorized users. The information can be in any form such as physical, electronic, tangible (paperwork), or intangible (knowledge) [5].

1.4 Cloud Security

Cloud security involves the technology that is used to secure cloud computing against cyber-threat these can be either insider or either external. As cloud computing delivers different services to store data on internet such as databases and software the demand for cloud security is increasing. Cloud security is managed and designed to protect your data and application from unauthorized access [7].

1.5 Operational Security

Operational security is a process used to determine friendly actions which could be used by the attacker to reveal sensitive information. The Operational security uses a counter measure to eliminate the exploitation of critical information. It is a strategic as well as analytical process use to identify whether the information can be exploited by the attacker and use it to collect sensitive information that could damage an organization [5].

2. Literature survey

In this paper Margaret Rouse described about kinds of cybersecurity and cyber threats. As cybersecurity is used to protect network devices like hardware and software from cyber threats. The cybersecurity is basically used by an organization as well as an individual person to protect against unauthorized access to computer systems which connected over a network [2].

Cybersecurity's goal is to ensure that everyone's privacy is maintained and devices like servers, mobiles, computers are securely protected from attackers. As cyberattacks are increasing day by day the need of cybersecurity is continuously changing with new technologies evolving [2].

Cybersecurity should be implemented to help protect the organization and individuals from cyber-attacks. In cybersecurity risk management training is the approach and is continually updated as new technologies change and evolve [2].

3. Cyber Threats

Cyber threat is used to describe the statistics related to security matters. As in today's world the digital signals travelling around across wires can represented as an attack. The cyber-attack is a type of attack that is used to expose, destroy, steal or gain unauthorized access to an individual's system or to an organization's private data. The aim of the attacker is dependent as many cyber-attacks are just threats, some of them are quite serious, while some of them can be potentially threatening to human lives [3].

There are various reasons why we need to protect ourselves from cyber-attack as it can cause breaches of security data, electrical blackouts and failure in systems it can also result into stealing of valuable and private data. Cyber-attack can also disturb computer and phone networks, making the unavailable to the user. From last few years the cyber threats are growing rapidly [3]. There are different types of cybersecurity threats they are –

3.1 Malware

Malware is a piece of software that is used to perform malicious task on a system or a network. The malware includes spyware, trojan, RATs, Rootkits, viruses, worms and ransomwares. The malicious software is developed and designed by the cyber-attacker to cause extensive amount of damage to the systems and gain unauthorized access to the network. The Malware can be in the form of a link or an executable file of even a document which requires user to click and open it to execute the malware [3].

Fig -1: Malware

3.2 Phishing

The phishing is an email borne attack that is used to trick the receiver by obtaining sensitive information such as credit/debit card details, usernames, passwords and even bank account details through a message. Social engineering is an example of phishing it is used swindle the user. Cyber attackers lure users by impersonating as they are from trusted sources such as banks, colleagues, or IT administrators [3].

Fig -2: Phishing

3.3 Man in the Middle (MITM) attack

A man in the middle (MITM) attack is an attack where attacker alters the communications between sender and receiver both the party i.e. sender and receiver. believe they are communicating with each other. MITM attack is mostly used to eavesdrop between a connection were attacker can see their text messages and can alter them without knowing. The MITM is also used in military to confuse there enemy [3].

Fig -3: Man in the Middle attack

3.4 Distributed Denial of Service attack (DDoS)

In Distributed Denial of Service attack (DDoS) the attack where the hacker tries to make a network or machine unavailable temporarily or disrupt the network where many hosts are connected to the internet. As the DDoS attack floods the victim from different origins is becomes very difficult or even impossible to stop the attacker by just blocking a single origin. The DDoS mostly target the web sites or web servers such as online banking or payment gateways [3].

Fig -4: DDoS attack

3.5 Backdoors

Backdoor is the method to bypass the normal authentication or an encrypted system or device without users understanding. Backdoors are mostly used to obtain access to cryptographic systems so attacker can gain access to data stored on a disk, user's passwords and he can transfer or delete this information unknowingly. A backdoor is hidden and it can be in a program code or a part of operating systems and even it can be inside of virus such as trojan horse which can create vulnerabilities in a system or device and can install a backdoor [9].

Fig -5: Backdoor attack

4. How to protect against cyber attacks

Nowadays, high-profile cyber-attacks on business companies have raised the importance of cyber security. As per the result of recent surveys conducted by Small Business
Authority, National Cybersecurity Alliance, Kaspersky Lab and Symantec said there are many small businesses that are still operating under false cyber security mechanisms. [10]

When we talk about Cyber Attacks, it may come in many ways that you cannot expect. While using the internet the most important step is to not open the emails that look suspicious. If sometimes a mail containing offers and contests looks good it is very crucial for one to avoid this high-risk area on the internet to protect yourself [11]. The following sections introduces you about different measures to prevent yourself from cyber-attacks.

4.1. Install Antivirus

While your common sense can protect you from cyber-attacks many times, but it is very important for one to install antivirus on system to protect yourself from malware and virus that may enter through internet on your computer that you cannot expect. An antivirus software is a software application developed by world class security firms to protect their consumers and businesses from most of the cyber-attacks. Currently antivirus is one of the easiest ways to secure yourself from cyber-attacks [11].

Fig -6: Antivirus Software

4.2. Use Strong Passwords

Your password should always be unbreakable. If you have so much money in your bank account and your password is like ‘william132’, then you must be ready for the surprise transaction. It is very important for one to keep the

passwords unguessable so that no one including your closed ones will be able guess your passwords right. You should not be fully reliable on the password limitations provided by the different websites. A strong password always contains 12+ characters (combination of uppercase & lowercase characters), at least 1 special character & numbers [6].

Fig -7: Password

4.3. Keep Your Software Up-To-Date.

Despite of developer's best intention to develop the secure software by considering all the security mechanisms, still sometimes hacker finds some way to break the security of the software. To overcome this situation, developers are always intended to release frequent updates for the software. Thereafter it's our (software users) responsibility to keep the software up to date to prevent it from cyber-attacks [6].

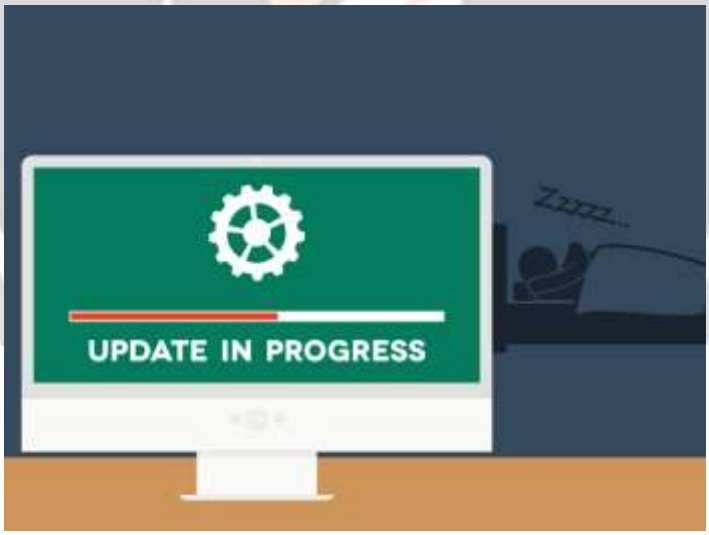

Fig -8: Software updates

4.4. Avoid Identity Theft

Identity thefts occurs when someone uses your personal information to gain access to all the features you had on any particular website using your name. Attacker gets all the benefits but the bills are addressed to your account. This is just an example; Identity theft can be more crucial than financial losses [6]. There are some security measures to be taken while dealing with your personal identifiable information:

- Do not share your Aadhaar/Pan no with anyone whom you don't trust/know.
- Never post sensitive information of yours on any social media platform.

- Never share your OTP with anyone.
- Never fill your personal information on the websites that claim to offer benefits in return.

Fig -9: Identity Theft

4.5. Always Take Appropriate Actions If You Have Been an Attacked/Victim

These are some important security measures you must take into consideration as soon as you realize that you have been hacked:

- File a complaint about your situation to the police and related authorities.
- Try regaining the access to the hacked accounts by using secondary/recovery contacts.
- Reset the password for the accounts that were using same password as of hacked account.
- Stay aware of the data breach in cyber world so that this will not happen again with you and prevent yourself from cyber-attack for the next time [6].

5. Future Scope

5.1. Shortage of Cyber Security Professionals

Since there are so many types of cyber-attacks, cybersecurity professions are facing the problem of not being prepared to overcome the cyber-attacks. According to the Worldwide Information Security Workforce Study (GISWS) around 19641 cybersecurity professionals are not able to address the difficulties [4].

5.2. Partially Skilled Professionals

As per research in 2019, data security professionals have hardly any expertise in facing dangers. Therefore, professionals must do certification and increase skills so that they will be competent enough to face any problem coming to their way [4].

5.3. Global Demand

Due to increase in cyber-attacks, there is a demand for operations and security management professionals. According to a survey Incident and Threat management positions are most popular in LATAM (63%) and Middle East and Africa (65%) than some other positions [4].

5.4. High Pay

Job seekers and Professionals who are looking for a job and grow up their career, for them cyber security is a great option. It will provide top pay, and respected position in any organization across the globe [4].

6. Conclusion

The demand for cyber security is continuously increasing, it is becoming difficult to predict the number of workers required with skills and knowledge of cyber security. Cyber security is surrounded with a variety of roles and occupations and is too wide and it has various single occupation or profession.

As cyber threats are increasing, the global demand for cyber security is increasing too. Each and every day the world faces many cyber-attacks which causes data breaches, as of report of 2018 there is increase in data breach by 11% as a result the demand is rapidly increasing for cyber security. Due security threats the demand for cloud computing has increased the experts predicted that in coming years there will be more cloud attacks.

7. References

[1]. Norman Jeremy. (2020). "The Creeper Worm, the First Computer Virus found in Cambridge, Massachusetts, United States". https://www.historyofinformation.com/detail.php?id=2465.
[2]. Rouse Margaret, Alexander Gillis and Casey Clark (2020). "What is cybersecurity? Everything you need to know". https://searchsecurity.techtarget.com/definition/cybersecurity
[3]. Taylor Hugh. (2020). "Cyber Security What Are Cyber Threats and What to Do About Them". https://preyproject.com/blog/en/what-are-cyber-threats-how-they-affect-you-what-to-do-about-them/
[4]. admin. (2020). Scope of Cyber Security in 2020 | Future of Cyber Security. https://www.imedita.com/blog/scope-of-cyber-security/
[5]. Fruhlinger Josh. (2019). "What is cyber security? Types, careers, salary and certification". https://www.csoonline.com/article/3482001/what-is-cyber-security-types-careers-salary-and-certification.html
[6]. awasthi7xenextt. (2019). "How to Protect Yourself From Cyber Attacks?" https://www.geeksforgeeks.org/how-to-protect-yourself-from-cyber-attacks/
[7]. Mindcore (2018). "5 types of cyber security". https://mind-core.com/blogs/cybersecurity/5-types-of-cyber-security/
[8]. Metcalf J. (2014). Core War: Creeper & Reaper. https://corewar.co.uk/creeper.htm
[9]. Kim Zetter. (2013). "How a Crypto 'Backdoor' Pitted the Tech World Against the NSA". https://www.wired.com/2013/09/nsa-backdoor/
[10]. The capacity group. (n.d.). "10 Ways to Prevent Cyber Attacks". https://capcoverage.com/index.php/10-ways-to-prevent-cyber-attacks/
[11]. Kaspersky. (n.d.). "Avoid Most Types of Cybercrime With These Simple Tips". https://www.kaspersky.co.in/resource-center/preemptive-safety/types-of-cybercrime-tips