ISSN No:-2456-2165

Cyber-Attacks and Cybersecurity

The pressing need for the latter

Subhabrata Chakraborty
B.Tech., CSE
Maulana Abul Kalam Azad University of Technology
Kolkata, West Bengal, India

Abstract:- The importance of cybersecurity is rapidly increasing with the enormous growth in the number and types of cyber-attacks. This article explores some of the most common types of cyber-attacks plaguing cyberspace today and stresses the need for cybersecurity. It then goes on to explain cybersecurity and its features. With the help of cybercrime statistics from India and a unique Man-In-The-Middle attack case from Kolkata, it further strengthens the case for a robust cybersecurity. Finally, the criteria for a strong future cybersecurity framework is provided.

Keywords:- *Cybersecurity; Cyber-Attacks; Need; Robust; Framework*

I. INTRODUCTION – THE CYBER-ATTACK THREATS WE FACE

With the growing use of the internet, the threat for transactions and activities has increased manifold. The increase in such threats has necessitated the rapid growth in cybersecurity. One has to understand the nature of cyber-attacks to provide robust security. This section defines and explains the different kinds of cyber threats. Such cyber-attacks mainly affect data by corrupting confidentiality, integrity, and availability – the three qualities that are so integral to data. Such attacks may severely affect the reputation of a financial organization and jeopardize its Information Technology systems.

Now, how do these attacks take place? A simple answer would be that hackers use malicious code and software to alter computer code, logic, and data. Such disruption results in data compromise. That, in turn, leads to dangerous consequences like financial information theft or system infiltration. Not all cyber-attacks are similar. They can be of various types based on the method used. Some of the common cyber-attack types are:

Viruses: Viruses are lines of code hidden in malware or phishing mails that, upon execution, replicate themselves by modifying computer programs.

Malware: Malware(Malicious Software) can be spyware, ransomware, or adware. It installs like software and takes control of the computer. It then sends all the confidential data to the attacker silently.

Ransomware: Ransomware is a type of malware that takes control of files and encrypts them. The attacker then demands money (ransom) from the victim for the decryption key. If the victim does not pay, he destroys the decryption key, rendering the files useless. [1]

SQL Injection Attack: It involves the injection of malicious code into a website. It can result in stealing or removal of customer information from the website.

Cross-Site Scripting: The attacker silently includes malicious scripts in the web browser of the victim. Generally, a legitimate web page or web application contains such scripts. The attack occurs when the victim visits the web page or web application. It delivers the malicious script to the browser.

Cross-Site Request Forgery: This forces the user to execute unwanted actions. The help of social engineering is taken to trick the users into executing unwarranted actions. A CSRF attack can force the user to change his email address, transfer funds, etc.

Distributed Denial-of-Service: This involves flooding the network system with packets of data, messages, etc. These packets are sent by several infected machines together. The flood slows down or crashes the entire networking system.
Botnets: Botnets are the millions of systems infected with malware to carry out Distributed Denial-of-Service attacks. These bots or zombie systems carry out attacks against the target systems, often overwhelming their bandwidth and processing capabilities. These attacks are difficult to trace because botnets remain in different geographic locations.

Drive-by Attack: This attack involves hackers looking for insecure websites and planting malicious code on one of the pages. It might install malware directly onto the computer of a site visitor. It might re-direct the victim to a website controlled by hackers. Unlike the other cyber security attacks, a drive-by does not rely on a user to do anything. One does not have to click a download button or open a malicious email attachment to become infected. With the help of an operating system, an app, or web browser containing security flaws due to unsuccessful updates or lack of updates the attack is channelized.

Eavesdropping Attack: Eavesdropping, also known as sniffing or snooping, is a network security attack where individual attempts to overhear the information that smartphones or computers send. This hack capitalizes on accessing the data

transmitted in an unsecured network. It is difficult to detect since it does not cause abnormal data transmissions.
Man-in-the-middle Attack: In this attack, a hacker puts himself between the communications of a client and a server. The hacker then gains access to the data being sent or received.

Social Engineering: Social engineering techniques manipulate human trust and extract information. An email or a phone call to reveal sensitive data might spell doom for the victim.

Malicious Emails: It tricks users into sharing personal details or credentials. In Spear Phishing, carefully crafted emails are sent to a small list of people. A cybercriminal may impersonate as an executive and attempt to get an employee, customer, or vendor to transfer funds or sensitive information to the phisher.

Smishing and Vishing: In these, telephones replace emails as the method of communication. Smishing involves the sending of text messages by criminals, while vishing involves telephone conversations.

Angler Phishing: A new type of attack, social media offers a myriad of ways for criminals to trick people. Cloned websites, tweets, posts, fake URLs and instant messaging can be used to make people download malware.

Password Attack: Passwords are the usual mechanism to authenticate users to an information system. So, obtaining passwords is a common and effective ploy. Such can be obtained by looking around a person's desk, ''sniffing'' the connection to get unencrypted passwords, using social engineering, gaining access to a password database. Outright guessing can also be used with Brute-force or Dictionary attack.

AI-Powered Attack: Artificial intelligence is present in everyday applications through an algorithmic process referred to as machine learning. Machine learning software trains a computer to perform particular tasks on its own. AI can hack into many systems like autonomous vehicles and drones, converting them into potential weapons. It makes cyber-attacks more powerful and efficient. It can kill or injure people, steal money, or cause emotional harm. Large attacks can even affect national security.

Threats associated with outsourcing: Sophisticated cyber activity against Third-Party Managed Service providers, vendors that provide services to Banks.

Insider Threats: one of the biggest threats, and often one of the hardest to detect, is that of malicious, careless, and compromised employees, contractors, and partners who are already inside the secure perimeter and have legitimate access to its sensitive data and IT networks.

Advanced Persistent Threats: These are long, directed cyber-attacks that are often state-sponsored. An organization or individual accesses another organization's LAN or internal internet through a gateway or a vulnerability and extracts information or implements other malicious measures.

II. CYBERSECURITY – A FORMIDABLE COUNTER AGAINST CYBER-ATTACKS

Cyber security is the method of protecting networks, systems, and programs from cyber-attacks. These are usually aimed at changing, accessing, or destroying sensitive information, extorting money from users, or interrupting normal business processes by deliberate exploitation of computers, networks, and technology-dependent enterprises. It protects information from malicious threats that affect confidentially, integrity, and availability - the three qualities integral to information [2].

The key elements of cyber security are:
i) Network security
ii) Application security
iii) Endpoint security
iv) Data security
v) Database and infrastructure security
vi) Mobile security
vii) Identity management
viii) Cloud security
ix) End-user education
x) Disaster recovery/business continuity planning

Network Security

It covers numerous technologies, devices, and processes. It is the crafted set of rules and configurations implemented for the protection of the confidentiality, integrity, and accessibility of networks and data. It protects internal networks from attackers by securing the infrastructure. Strong passwords and two-factor authentication (2FA) are examples of network security.

Application Security

It uses software and hardware for the protection and security against threats during the development stage of an application. Firewalls, antivirus programs, and encryption are the different types of application security.

Endpoint Security

It is the protection of computer networks remotely bridged to client devices. The connection of endpoint devices like tablets, mobile phones, laptops, Internet-of-things devices to corporate networks results in attack paths. A definite level of compliance with standards is ensured by endpoint security.

Data Security

It means protecting digital data (a database, etc.) from unwanted actions of unauthorized users and destructive forces.

Database and Infrastructure Security

Securing physical devices and databases is vital in a network. Database and infrastructure security provides security for these cyber-physical systems.

Mobile Security

Also known as wireless security, it is the protection that is in place for laptops, smartphones, tablets, other devices, and the networks they are connected to from the risks and threats in wireless computing.

Identity Management

Identity management and access control can be components crucial to security architecture. It involves the management of access to enterprise resources. It can ensure the security of systems and data. It helps in the identity verification of users before granting them access to the systems or sharing information.

Cloud Security

It refers to the services, technologies, controls, and policies to protect cloud data, applications, and infrastructure from cyber-attacks. It helps to manage risks associated with on-premises attacks by constantly monitoring and protecting the data in the cloud.

End-user Education

It is the process of training and educating users about the security practices and safety measures (e.g., not to click unknown links, not to download suspicious attachments, etc.) to avoid entry of malware or other malicious software. A good end-user security training program can enhance the security of an organization. It should be in a language and at a technical level that can be followed by everyone.

Disaster Recovery or Business Continuity Planning

It is the process of resuming business after a disruptive event. Business continuity planning ensures that enterprises can keep running the business not only after small disruptions but also in case of bigger disasters. The two terms are mentioned under the acronym BC/DR. These are mapped out to help employees communicate and go about doing their jobs in the unlikely event of an attack. The details may vary depending on the size, scope, and workings of the company.

III. THE CURRENT BOOM IN CYBER ATTACKS

After explaining the various cyber threats and then emphasizing the different kinds of cybersecurity, it is pertinent to produce a picture of cyber threats presently plaguing the world. In this case, we use the example of India although the situation and severity of cyber-threats remain a cause for concern all over the world.

The cyber situation of India is important as India ranks 3rd in the total number of internet users all over the world. According to a report published by NITI Aayog, India's internet use has a CAGR growth rate of 44%.[3] It also ranks in the top 10 when it comes to spam-sending. Of the countries affected by cyber-crime, India ranks among the top 5.

Most of these cyber-attacks belong to the categories of Denial of Services, Web Attacks, and Payment cards skimming. Also, the majority of the attacks included the use of malware and stolen passwords. About 75% of Indian CXOs are said to lack confidence in their company's cybersecurity infrastructure. Some reports suggest that cybercrime damages will cost the world six trillion dollars in damages annually by 2021.

The case of hackers hacking into the system of the Union Bank of India in 2016 is a glaring example of how cyber-attacks take place. Through a phishing mail sent to an employee, the hackers were able to access his credentials. Funds worth 171 million dollars were swindled and transferred. However, the prompt action of the bank helped it recover most of its money.

In 2017, the Wannacry ransomware affected India and several thousands of computers were locked down by ransom-seeking hackers. The systems belonging to the Andhra Pradesh Police and the state utilities of West Bengal were also affected in the process.

These statistics highlight how the challenges are mounting and stress the need for a robust cybersecurity solution for the future.

IV. THE KOLKATA MITM ATTACK AND HOW FOLLOWING BASIC CYBERSECURITY RULES COULD HAVE AVERTED IT

In June 2021 Kolkata's ATMs were attacked by MITM (Man in the middle) based attacks.[4] These focused on the communication between the host and the ATM PC. The attacks faked the host response for the transactions without debiting the money from the account.

The hackers used a BlackBox device. The device was connected between the ATM's PC and the dispenser. This allowed the attacker to send cash dispensing commands directly to the ATM without any validation from the bank side.

Now, this could have been prevented as most of the ATMs under attack were not upgraded software which is a clear breach of cybersecurity norms. Secondly, there was a need to employ a virtual private network (VPN) before sending the data. This would have ensured that the data got encrypted and could not be read by the hacker.

V. THE ESSENTIAL FEATURES OF FUTURE CYBERSECURITY

While the need for cybersecurity is of utmost urgency, one must clearly outline what qualities the future cybersecurity should have. Besides the extant features, future cybersecurity must have:

1. *Prediction* – Predict the most likely targets, attacks, and methods. Take proactive measures to identify attackers, their methods, and objectives before the materialization of attacks.
2. *Prevention* – Deter or prevent attacks so that no loss is experienced. Secure the computing environment with current patches, tools, updates, and best-known methods in an efficient and timely manner. Reinforcing and educating good user behaviors is critical too.
3. *Detection* – Identify attacks that are not prevented by the system to allow for a thorough and rapid response. Efficient management of efforts to repair, contain and recover, as needed returning the environment to normal operations.
4. *Response* – Rapidly address incidents for minimal losses and quick return to a normal state. Monitor key areas and

activities for the attack which evade prevention. Identify breaches, issues, and attacks.

5. *Driven by AI & ML*: As artificial intelligence and machine learning gather speed, and start to impact more and more industries, it is poised to play a greater role in cybersecurity. Machine learning models that can accurately identify and predict attacks could be a real boon. These models need to be honed and trained. However, there is a risk that AI and machine learning may be exploited by attackers.

6. *Layered security*: A layered cybersecurity approach is a gradual process. [5] One needs to take stock of inventory to ascertain the number of devices used. Then, security can be added wherever necessary in the different layers. Yes, the world of work has changed. The opportunity for attackers to get their hands on data has increased manifold. To protect business regular tests are required to ensure that security controls are effective and that they work properly.

VI. CONCLUSION

Here I have tried to analyze and define the different kinds of cyber-threats and how cybersecurity might find use as a formidable defense against them. Cybersecurity has to meet future standards. So, after making a case for cybersecurity, I have mentioned the features that cybersecurity needs to develop to become future-ready.

REFERENCES

[1]. “17 Types Of Cyber Attacks To Secure Your Company From”, Bojana Dobran, February 21, 2019, Unpublished.
[2]. University Of North Dakota, Blog Article On Cybersecurity, Unpublished.
[3]. Paper on Cyber Security by Dr. V. K. Saraswat, Member, NITI Aayog, India at Cyber Security Conclave, Vigyan Bhawan, New Delhi, India,2017.
[4]. Times of India, online portal, 31st May 2021.
[5]. 7 Types Of Layering Techniques – Microage(Online), Unpublished.