Cyber-Attacks Identification and Measures for Prevention

Shubham CHOPRA[1], Hitesh MARWAHA[2], Anurag SHARMA[3]
Faculty of Computational Science, GNA University, Phagwara, Punjab, India
[1] shubham.chopra@gnauniversity.edu.in
[2] hitesh_marwaha@gnauniversity.edu.in
[3] anurag.sharma@gnauniversity.edu.in

Abstract

In the present digitization era, almost everything is available online, at just one click away from us, which offer a lot of opportunities, like saving a lot of time, but also many challenges, due to the existence of many cyber-attacks, more complex and difficult to be detected. The cyber-attacks effects can be data theft, modification, or alteration. In recent time, cybersecurity is very important also in the academic field, because schools and universities systems are connected online. To protect our data from various attacks, cybersecurity plays the most important key role. Cybersecurity helps in ensuring the safety of data, personally identifiable information, and intellectual property. Cybersecurity is not only for individuals, a specific group or organization, but it is for all the people and for the government to keep data integrity, confidentiality, and availability. This paper presents the cybersecurity concept, analyzing different cyber-attacks and the specific preventions measures.

Index terms: cyber-attacks, cyber-threats, cybersecurity, prevention measures

1. Introduction

The whole world is leading towards IoT (Internet of Things). Everything becomes digital from maintaining a student academic records to paying online to life saving equipment and everything which is on the Internet is not secured from the cyber criminals. They use different tricks to get access in our systems to steal personal and financial details of users without getting into the knowledge of the victim.

Cybersecurity comes into play because we need to protect the systems, networks, devices, and data from the cyber-attacks. Everyone which is connected to the internet needs cyber security because all records of information is stored digitally and the cyber-attacks aim to exploit common vulnerabilities, in order to compromise the computer systems. The cyber criminals have ample motivation - there's a lucrative market for the sale and exploitation of the data.

Cybersecurity refers to the protection of data from the external resources present in the network or internet. In other words, cybersecurity is the practice to defend the critical systems, servers, networks, data from malicious attacks carried out by some unauthorized persons such as cybercriminals, hackers, spammers.

The cybersecurity concerns with the 3 basic concepts:

- **Confidentiality** - It refers to when data or information is read or copied by someone who is not authorized to do so that leads to "loss of Confidentiality". Example: military secrets.

- **Integrity** - It refers to when data or information has been changed or being modified by someone who is not authorized to do so that leads to “loss of Integrity”. Example: a user entering incorrect data into the database.
- **Availability** - It refers to when data or information is not been available to the authorized person to access it or the data or information is destroyed by unauthorized person so that the authorized person can not access it that leads to “loss of Availability”.

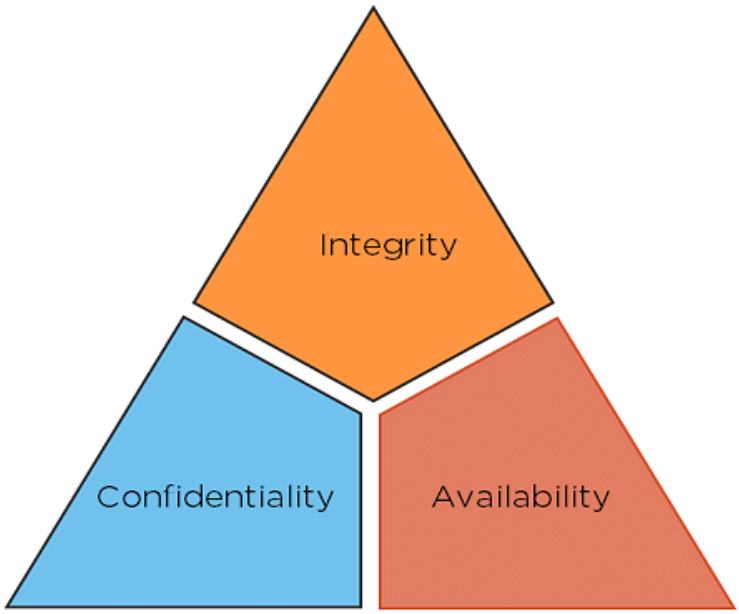

Fig. 1. C-I-A triad [1]

Increase in the cyber-attacks and data breaches no one is remain untouched with this problem as of now it's the era of digitalization everything is known available online and especially due to pandemic also, we have to shift physical to digital or virtual. Individuals, governments, for-profit companies, not-for-profit organizations, and educational institutions are all at risk of cyberattacks and data breaches and In the near future, the number of attacks will grow as digital technologies evolve so as to protects all categories of data from theft and damage which includes sensitive data, personally identifiable information (PII), protected health information (PHI), personal information, intellectual property, data, and governmental and industry information systems. It is no longer a question that "when a cyber-attack will occur" and with the advancement in the techniques of cyber-attacks antivirus software or firewalls are not much the efficient to protect us from these attacks. This is why cyber security is much needed and is of such great importance.

2. Cybersecurity threats and their prevention

Malware refers to a variety of forms of malicious software’s or malicious code that include viruses, trojans, spyware, adware, botnet, ransomware or can be in any executable form or in an active web content such as animated GIF’s, embedded object. So that they are used to disrupt or damage or hijack the resources or assets or system of a authenticated user. In other terms these are inserted into a system which used to compromise the so-called C-I-A triad. Malware can be distributed by various ways such as [2]:

- Email attachment.
- Fake internet ads.
- Infected application software’s or websites.

2.1. Phishing

Phishing refers to cyber-attack that uses disguised email as a weapon. It pretends to be the entity, person or company you often used to deal with it generally. The goal of this is to forcefully believe the recipient into believing that the information or message is needed or wanted by the recipient and by clicking it leads to download malware which helps the attacker to get an access into the infected person systems information.

Phishing is a form of fraudulent activity with the motive to steal personal and financial details of a user, which is usually done through email which seems to be from a legitimate or reputable source. The attacker tries to be the part of that organization or provides you a cloned website of a Company or organization from which the user wants to communicate or for getting services or something else. Usually, it is difficult for the user to distinguish between the genuine one and the cloned one which is going to be used by the attacker to trap the target user. There are some steps used for phishing attacks which is used by the attacker to obtain information from the target user [3]:

- Planning.
- Compose Fraudulent email.
- Attack the target.
- Gather Credentials.
- The End Game.

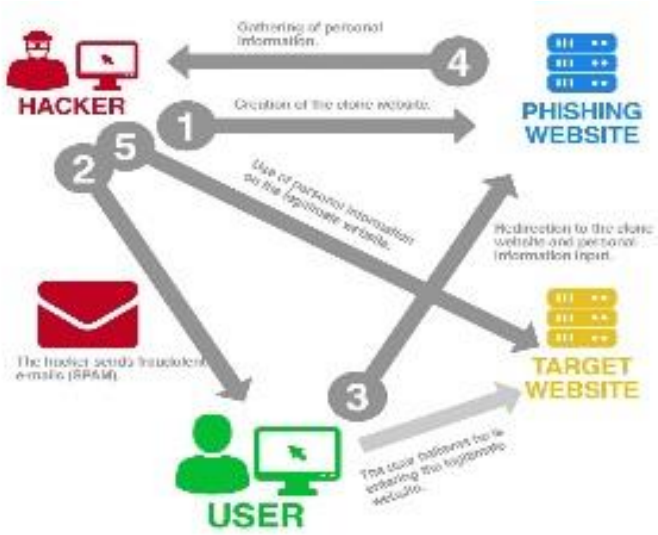

Fig. 2. Phishing attack mechanism [4]

Planning - The attacker starts with the Planning game here "game" refers to make a spoof of a legitimate or reputable website from where the attacker gathered the user's or target's credentials or information. It becomes difficult for the target to distinguish between the spoof and legitimate and genuine website and here the target gets trapped first.

Compose fraudulent email - As shown above in the figure 2, the attacker (Phisher) then composes a fraudulent email with the help of spoof website used for phishing. The Email is composed in such a way that it seems legitimate to the target.

Attack the target - The next step is to attack the user, as we mentioned earlier that it becomes difficult for the target to distinguish between the spoof and legitimate and genuine website the target tends to open the email which contains the link of the phisher phishing website.

Gather credentials - After being redirected to the phishers phishing website. The target user enters the login credentials on that website which automatically provides the same credentials to the

phisher (attacker) also. Unknowingly the target user takes the bait and just gone through the data theft.

Accessing information - In this last step the phisher (attacker) using the data obtained from the phishing website logins to the official target website and now can access all the information of the victim or targeted user. The attacker can also sell the login credentials or the obtained information of the target user or victim on the Dark web.

Anti-Phishing Techniques

Anti-phishing is a service or technique that helps to prevent unauthorized access to secure information of a specific individual, Organization or Business. In other words, it is the efforts of blocking the Phishing attacks. Various Anti phishing applications are available to check whether the website is safe or legit on behalf of user. It can be integrated into the Web browser also. In general, anti-phishing techniques can be classified into following four categories [5].

- Content Filtering- In this methodology content/email are filtered as it enters in the victim's mailbox using machine learning methods, such as Bayesian additive Regression Trees or Support Vector Machines.
- Blacklisting- Blacklist is collection of known phishing Web sites/addresses published by trusted entities like Google's and Microsoft's blacklist. It requires both a client & a server component. The client component is implemented as either an email or browser plug-in that interacts with a server component, which in this case is a public Web site that provides a list of known phishing sites.
- Symptom-Based Prevention- Symptom-based prevention analyses the content of each Web page the user visits and generates phishing alerts according to the type and number of symptoms detected.
- Domain Binding- It is a client's browser-based techniques where sensitive information is bind to a particular domain. It warns the user when he visits a domain to which user credential is not bind.

2.2. SQL Injection

A SQL injection is a cyber-attack which usually deals in stealing or damaging the data present in the database by using malicious Structured Query Language (SQL) statement which can used to retrieve the content of entire database or can also be used to add, modify or delete records in the database.

The attacker finds that whether the webpage or web application uses SQL databases such as MySQL, Oracle, SQL server and after that exploit the vulnerabilities by injecting malicious SQL statements. After that the attacker searchers for the vulnerable user inputs within a web application or webpage of which the attacker uses such inputs and can also create input content which is known as malicious payload which plays a significant role in the overall attack performed which is then the content or so-called malicious payload executed in the database. There are several types of SQL injection attacks such as [6]:

- In-band SQLi.
- Blind SQLi.
- Out-of-band SQLi.

```
# Define POST variables
uname = request.POST['username']
passwd = request.POST['password']

# SQL query vulnerable to SQLi
sql = "SELECT id FROM users WHERE username='" + uname + "' AND password='" + passwd + "'"

# Execute the SQL statement
database.execute(sql)
```

Fig. 3. SQL Injection statement [6]

Prevention of SQL Injection attack

The only sure way to prevent SQL Injection attacks is input validation and parametrized queries including prepared statements. The developer must sanitize all input, not only web form inputs such as login forms. Turning off the visibility of database errors on your production sites can also be a good idea.

If you discover an SQL Injection vulnerability you can use a web application firewall to sanitize your input temporarily. There are certain Primary defenses options available that should be followed to prevent SQL Injection [7]:

- Option 1: Use of Prepared Statements (with Parameterized Queries).
- Option 2: Use of Properly Constructed Stored Procedures.
- Option 3: Allow-list Input Validation.
- Option 4: Escaping All User Supplied Input.

2.3. Man in the middle (MITM)

Man in the middle cyber threat refers to intercept the communication of the two authenticated user or while the user communicating or requesting resource or information from server so that to steal data or information also the attacker may filter the data. As the attacker is present unknowingly in the middle of the communication.

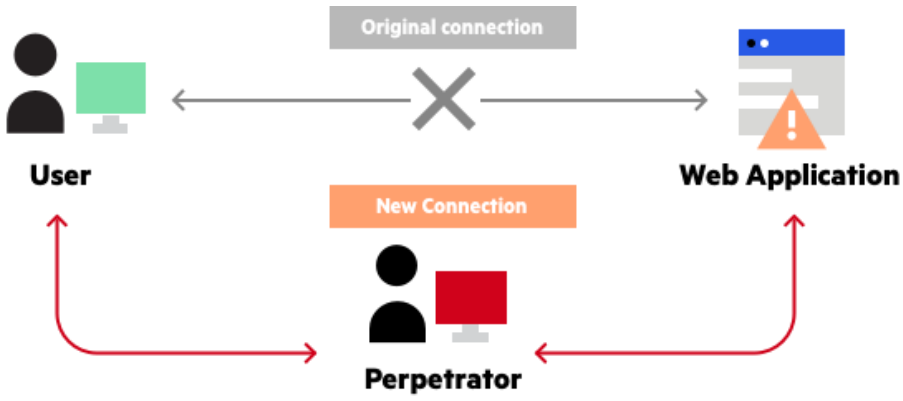

Fig. 4. Man-in-the-middle attack mechanism [8]

A successful MITM attack involves two specific phases: Interception and Decryption [9].

Interception phase

This phase deals with that how the attacker inserts themselves as the "man-in-the-middle". As the attacker intercepts the users original or legitimate network traffic with the fake network traffic before it reaches to its intended destination. It is frequently done by creating a fake open Wi-Fi network or when a user connects to an open public Wi-Fi.

Once the attacker inserts themselves successfully then may choose a technique from a variety to get further with the attack:

- IP spoofing involves an attacker altering the IP packets by disguising himself.
- ARP spoofing involves use of forged ARP message to link attackers MAC address with the target's legitimate IP address.
- DNS spoofing also known as DNS cache poisoning involves an attacker altering or infiltrating a DNS server so that the target web traffic gets redirected to the attacker's fake website.

Decryption phase

After the Interception the decryption phase comes in to play as a MITM attack doesn't stop here, as in this phase the attacker which has the target's encrypted data after gaining the access now need to be decrypted so that the attacker is able to read it and use it. For decrypting the data any method can be adopted by the attacker:

- HTTPS Spoofing is a method which makes the target to believe that the certain website is safe and authenticated when it's not by sending the fake certificate to their browser.
- SSL Hijacking involves the attacker passing a forged authentication keys to both the user and application during TCP handshake and pretending to be a secure connection which is not and the entire session is in control of the so called "man-in-the-middle (attacker).
- SSL Stripping involves the attacker downgrading a user secure HTTPS connection to unsecure HTTP version of the website while the secure connection to the secure website is maintained by the attacker.

Prevention of MITM

Some measures aimed to prevent MITM attacks are [10]:

- Avoid Wi-Fi networks that aren't password protected and never use a public Wi-Fi network when dealing with some sensitive personal information.
- Use a Virtual Private Network (VPN).
- Log out of sensitive websites such as banking websites.
- Use multifactor authentication.
- Use a firewall to for a secure connection.
- Use antivirus software to protect your devices.

3. Cyber Security Tips and Best practices

Ensuring cybersecurity and remain protected from cyberattacks is challenging, however. It's difficult to keep up when cybercriminals are persistently looking for new ways to expose security risks. Still, there are a number of ways to ensure cybersecurity are as follows [11]:

Keep software up-to-date

Software companies typically provide software updates for 3 reasons: to add new features, fix known bugs, and upgrade security. Always update to the latest version of your software to protect yourself from new or existing security vulnerabilities.

Avoid opening suspicious emails

If an email looks suspicious, don't open it because it might be a phishing scam.

Someone might be impersonating another individual or company to gain access to your personal information. Sometimes the emails may also include attachments or links that can infect your devices.

Keep hardware up-to-date

Outdated computer hardware may not support the most recent software security upgrades. Additionally, old hardware makes it slower to respond to cyber-attacks if they happen. Make sure to use computer hardware that's more up-to-date.

Use a secure file sharing solution

The files you share are only as secure as the tools you use to share them with. Adopt a secure file sharing solution to encrypt your files while they're in transit and at rest to prevent unauthorized access and keep your files safe.

Use anti-virus and anti-malware

As long as you're connected to the web, it's impossible to have complete and total protection from malware. However, you can significantly reduce your vulnerability by ensuring you have an anti-virus and at least one anti-malware installed on your computers.

Use VPN for a secure connection

For a more secure and privatized network, use a virtual private network (VPN). It'll encrypt your connection and protect your private information, even from your internet service provider.

Creating strong passwords and change it frequently

Put more effort into creating your passwords. You can use a tool like howsecureismypassword.net to find out how secure your passwords are.

Enable 2-Factor Authentication

Many platforms now allow you to enable 2-factor authentication to keep your accounts more secure. It's another layer of protection that helps verify that it's actually you who is accessing your account and not someone who's unauthorized. Enable this security feature when you can.

Remove adware

Adware collects information about you to serve you more targeted ads. It's best to rid your computer of all forms of adware to maintain your privacy. Use adware cleaner tools to clean adware and unwanted programs from your computer.

Double check for HTTPS on websites

When you're on a website that isn't using HTTPS, there's no guarantee that the transfer of information between you and the site's server is secure. Double-check that a site's using HTTPS before you give away personal or private information.

Avoid using public networks or Wi-Fi

When you connect to a public network, you're sharing the network with everyone who is also connected. Any information you send or retrieve on the network is vulnerable. Stay away from public networks or use a VPN when you're connected to one.

Maintain Back up of important data

Important data can be lost as a result of a security breach. To make sure you're prepared to restore data once it's lost, you should ensure your important information is backed up frequently on the cloud or a local storage device.

Train employees

The key to making cybersecurity work is to make sure your employees well trained, in sync, and consistently exercising security practices. Sometimes, one mistake from an improperly trained employee can cause an entire security system to crumble.

Hire a "White Hat" hacker

Not all hackers are bad. Some hackers expose security risks for the sake of helping others improve their cybersecurity by keeping them aware of security flaws and patching them. These hackers are known as "white hat" hackers. It might benefit you to hire one to help you find risks you never knew you had.

4. Conclusion

As of now everything is somehow connected to the internet cyberattacks are increasing at an alarming rate which is a serious matter of discussion and specific prevention steps should be taken from individual as well as from the government side also by implementing or making new laws for ensuring the safety of public as well as government sensitive information. One of the most important reasons for the occurrence of these attacks are lack of adequate knowledge about the cyber security. No one wants to accept that they are the victim of these attacks or breaches not even government or any other industry as it will present a bad image in front of public which raises a question in their mind that even they are not protected so how they will protect us, protect our sensitive information.

This study shows the steps for identifying a cyber-attack, techniques used by cyber criminals to get access in systems and how we can prevent or protect our computer systems. The motive of this paper is to provide an idea and create awareness, for whom security of their network or information is the key aspect.

References

[1]. https://www.simplilearn.com/ice9/free_resources_article_thumb/cia_triad.png.
[2]. https://blog.netwrix.com/2020/06/12/malware-prevention/.
[3]. Shankar, A., Shetty, R., & Nath, B. (2019). A review on phishing attacks. International Journal of Applied Engineering Research, 14(9), 2171-2175.
[4]. https://www.swascan.com/swascan-phishing-simulation-attack/.
[5]. Gaurav, Madhuresh Mishra, Anurag Jain, "Anti-Phishing Techniques: A Review", International Journal of Engineering Research and Applications ISSN: 2248-9622, Vol. 2, Issue 2, Mar-Apr 2012, pp. 350- 355.
[6]. https://www.acunetix.com/websitesecurity/sql-injection/.
[7]. https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html.
[8]. https://www.imperva.com/learn/wp-content/uploads/sites/13/2017/09/man-in-the-middle-mitm-attack.png.
[9]. https://www.imperva.com/learn/application-security/man-in-the-middle-attack-mitm/.
[10]. https://www.pandasecurity.com/en/mediacenter/security/man-in-the-middle-attack/.
[11]. https://www.titanfile.com/blog/cyber-security-tips-best-practices/.