International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 06 | June 2020 www.irjet.net p-ISSN: 2395-0072

A Review Paper on Cyber Security

Arti Raj[1] and Sahil Srivastav[1]

[1]*Dronacharya College of Engineering, Khentawas, Farrukh Nagar, Haryana 123506*

Abstract - *This paper aims to explore a range of cyber-attacks that have become the new reality of this technical era. As the stats of the cyber attacks is rising exponentially every year, it has become quite prominent that we need regulated protective measures to keep these threats at the bay. But doing that is not as easy as it requires very intricate knowledge of all the associated domains. We'll be aspiring to look into various cyber threats that are arriving day by day and also to examine various measures present to shield our systems from these threats. We'll be walking over varied strengths and weaknesses of our advanced protective systems against this serious security threat.*

Key Words: Cyber Security, Cyberattack, Cyber threat, Internet, Cyberattacker

1. INTRODUCTION

It was said earlier that the only way to keep your data safe is to lock your system in concrete walls with it bound with lead chains which were true to some extent decades ago when the use of the internet for the transaction of data and information wasn't a thing. But in the modern era where data almost equivalents to the internet, that's not possible.

Cyber Security covers the systems and techniques used to achieve a sound and safe cyber environment. This mentioned environment does not only includes use but also the device, applications, and network as well. It is a prominent need of today as almost everything can be done online today. That makes it convenient and handy, doesn't it? But a coin always have two sides. As expedient it gets, you are also exposed to numerous cyber threats that are lurking around the corner.

Cyber Security is a type of security to safeguard the internet. The very core objective is to provide a set of rules for the users and also measures to protect them from any possible threats.

Almost every industry, be it private or government and even the finance industries deal with a lot of confidential and sensitive data over the internet making it vulnerable to fall in the wrong hands. As we are advancing in devising diverse technology to deal with cyberattacks, we should also keep in mind that the modern-day hackers are also getting more and more creative with their ways to access the data. Cyber attacks are the unauthorized and spiteful set out to outbreak into the data of other individuals or industries even. It could either be led by an individual or an organization.

The level of intelligence and technology at the bay of cyber attackers is also giving rise to this ever-increasing problem. The well-known cyberattack on Yahoo is an example of the extent to which it could reach. 3 billion accounts were hacked as a result of data theft that occurred earlier. Although, it was said that no sensitive data was stolen like bank-details, card-details, and passwords, it affected so many users. The root cause of this attack was said to be the out-dated security systems and improper encryption of information.

2. THREATS

The cyber threats fall into two categories: active attack or passive attack. Active cyber-attack comprises of the system to affect or damage your data and system w individual or organization targeting you're here as Passive cyber-attack goals to access your data to make use of it.

2.1 Passive Attacks

- **Computer or Network Surveillance**

Computer or Network Surveillance is a monitoring process in which systems' data is constantly kept under check which is usually stored in a hard drive. As harmless as it sounds, it could be easily accessed by malicious individuals or organizations granting them access to sensitive data such as passwords, bank details, and whatnot. It is as easy as placing software on the system to tack anything and everything on it.

- **Wiretapping and Fibre Tapping**

Wiretapping or Telephone Tapping as traditionally referred to is the classic method of observing the conversations over phone and internet by a third party. It is legally done by the government in certain circumstances. The network tapping technique is used to reach the data in Fibre Tapping.

- **Port Scan and Idle Scan**

Port Scan is the typical attack in which request is sent over a range of port addresses to look for an active port to search for the data that can be targeted. Idle Scan is the attack done through the transfer of spoofed packets to look for the loose end services on the system. Scanning as an attack is nothing new. It has been there for decades.

- **Data Scraping**

It is the technique where data is extracted from human-readable sources without taking the permission of the authorized owner.

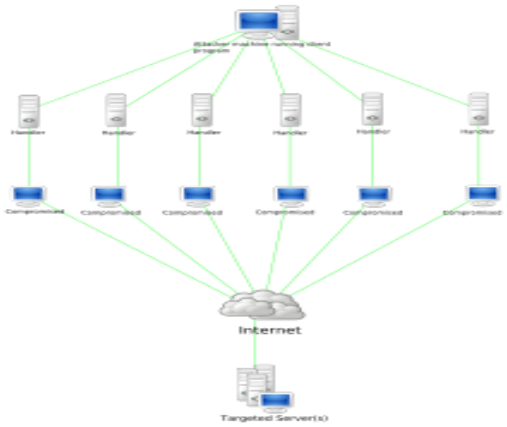
- **Backdoor**

The system might be secured or so it seems to you. There might be some unsecured ends left somewhere like outdated input fields and plug-ins which can become the next target of the cyber attackers.

2.2 Active Attack

- **Denial-of-service attack**

This is a type of cyber attack in which a particular service is made unavailable to the desired user by temporarily or permanently disrupting the host. It is achieved by bombarding the system with redundant and insignificant requests to obstruct genuine requests made by intended users. The problem that is associated with this type of cyber attack is that the requests are generated from multiple sources to a single victim system at once making it a tedious job to recognize the source of the attack.



[1]Fig 1: Denial-of-service diagram

- **Spoofing**

When the attacker poses to be someone else over a network to access the data or to attack the network host or system, it is termed as a spoofing attack.

2.3 Syntactic Attack

- **Virus**

What's the worst thing about this type of cyber attack is that it gets joint to other programs or software aiming to reproduce as it can do self-replication over and over again.

A virus is difficult to trace the attacker as it continuously keeps changing its digital footprints every time it replicates itself. It gets stored anywhere in the memory of the computer and gets attached to any program or file that can run the code of the virus.

Viruses, all over the world cause the industries a whole lot of trouble as well as resources as it damages the systems by leading to corrupting the data, data theft, system failure, and adding onto the maintenance cost of the organization. Viruses are underrated as it seriously affects the system as it alters the files and even corrupts them on the victim computer.

- **Worms**

If viruses are a threat to the users on the internet, worms are another big problem as this kind of cyber attack does not even need a file to get attached to. This type of program is a long-lasting and very independent program that can live up to days. It runs over the network protocols to copy itself again and again.

[2]Fig 2: Hex Dump message left for Bill Gates by the programmer of the worm

The factor that plays a huge role in making the device vulnerable to this attack is the failure of the security system. It always affects the system or network by absorbing bandwidth. Most of the worms do not usually change or modify the data on the computer but it can do some serious damage if programmed so.

- **Trojan Horses**

Trojan horse is a program typically tailored to perform all the legal works but it can also be sneakily used to do the illegitimate tasks secretly. Trojans are often implanted in the code of the software (when in trial period) which is then used to trace the activity and the data of the user without the user having any idea of such happenings.

It works as the platform to host all the types of the cyber attack on the computer. Many worms and viruses can install themselves on the system in the presence of Trojans.

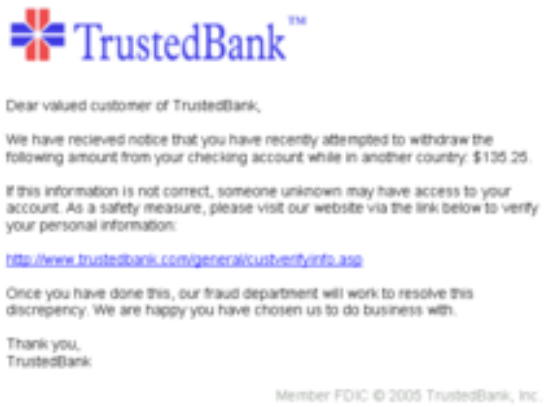
2.4 Malware

As the name suggests, Malware (formed from the words malicious software) is any malicious program that is specifically designed to target and damage the computer of any user or organization. The attacker aims to damage the operations of the system and to reach sensitive and vulnerable data. There is nothing unintentional in this type of cyberattack as it is precisely designed to harm certain users or organizations.

- **Phishing**

Phishing is more of cheating then attacking as the attacker disguises as someone else, trustworthy to the user, to grant access to sensitive data such as credit card details, bank details, passwords, and usernames.

It is very similar to spoofing in many terms. It is achieved by sending messages or emails to the users consisting of links to the websites asking for the personal information of users such as usernames and passwords. It is very often observed that it is carried out by the websites implanted with malware.


TrustedBank™

Dear valued customer of TrustedBank,

We have recieved notice that you have recently attempted to withdraw the following amount from your checking account while in another country: $135.25.

If this information is not correct, someone unknown may have access to your account. As a safety measure, please visit our website via the link below to verify your personal information:

http://www.trustedbank.com/general/custverifyinfo.asp

Once you have done this, our fraud department will work to resolve this discrepency. We are happy you have chosen us to do business with.

Thank you,
TrustedBank

Member FDIC © 2005 TrustedBank, Inc.

[3]Fig 3: Example of a phishing email.

- **Keystroke Logging**

Keystroke logging or often termed as the keyboard capturing or keylogging is tracing the actions of the user on the keyboard. It can either be hardware or software tracing the actions of the unaware user that every key they are pressing is being traced and recorded.

This often leads to the exposed usernames or passwords which are then taken by the attacker.

2.5 Semantic Attacks

This type of attack is done by embedding false information and data which in turn raises questions on the credibility of original data. It does not necessarily cause any direct damage to the user. The aftereffects of this type of cyberattack can be seen till a long time. It targets human-users rather than technical devices or software.

3. REMEDIES OR PREVENTIVE MEASURES

3.1 Computer Access Control

In a general computer system, security consists of the following steps not necessarily carried out in mentioned order:
-identification
-authentication
-authorization
-approval
-audit

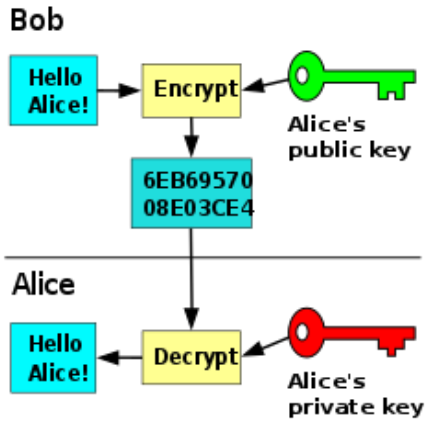
these factors together determine who can access the system and who cannot. So just like one decides who gets to enter their house by giving the key, the same happens in the case of computers as well. It's you who can grant or deny access to your device to anyone.

3.2 Firewalls

Firewalls act as the filter to the incoming traffic to your network. It works on a set of predetermined guidelines to grant or deny access to any program trying to gain access to your system or network. It shields you by forming a barrier between you and the external untrusted network by keeping you on the other side. When you use the internet you are exposing yourself to tremendously large traffic which is not at all trustworthy, and that is where firewall comes into the picture.
Firewalls can be classified into two subgroups- host-based firewalls and network firewalls

3.3 Encryption

Encryption is nothing but encoding the data and information which is in the state of plaintext to the encrypted version referred to as ciphertext. Encryption does not give a hundred percent guarantee that data would not be harmed but it gets protected to some extent as only the authorized users can convert the ciphertext back to the original data and vice-versa.



[4]Fig 4: Cryptography (Public-key)

3.4 Intrusion Detection System

Intrusion Detection System is a software specially designed to trace any activity that violates the predetermined set of policies. When it senses any malicious activity over the network or the system, it immediately informs the administrator of the system. It ranges for the small network or it could even be used for large networks.

3.5 Antivirus

Antivirus software also referred to as anti-malware software is a program tailored to firstly prevent malware from entering the network. It also detects and removes any present malware from the network or device. It was mostly used a few years ago but now with the rise of free software development for the detection of malware, it is outdated.

4. DEDICATED INDUSTRY FOR CYBER SECURITY

Data theft and information attacks have become such an emerging issue that there is a proper dedicated industry today working tirelessly to reduce the likelihood of the cyberattack.

The working of this industry is a matter of understanding. Some of the basic functions of organizations working in this sector are:

-observing the risks
-keep studying the ever-increasing methods of the modern-day hackers to keep the attacks at bay.
-look for the possible backdoors in the systems.
-spread awareness in people by publishing relevant books and magazines.
-check the vulnerabilities of the system.
-fix the damage caused by an attack.
- inventing new and efficient solutions for the potentially high-risk cyberattacks.

5. CONCLUSION

Over the past few decades, the number of cyberattacks has become a major issue of concern for various industries as the technological advancement is not only facilitating us but also the hackers and attackers sitting well shielded behind the screens of the computers targeting the clueless users. The functioning and the type of attacks are becoming more and more sophisticated every day making it very challenging for even the experts to trace the source of the attacks. We are very well aware of the danger prowling at the bay looking for just one opening to sneak in but we fail to take proper measures to prevent it from entering our systems. Some industries are still very ignorant about this threat and they are taking this way too lightly by adopting out-dated security systems. We need to understand that, negligence is exactly what the attackers are looking for.

These modern-day attacks are well equipped to outdo even the most advanced technologies designed to defend the data. What we need to do is to adopt effective and efficient protective measures like the fifth generation security to prevent an attacker from reaching us. And for that, the first step is spreading awareness among the people and industries about cyber threats, their damage-causing effects, and needed protective measures.

Apart from that, we also need to strengthen the industry of cybersecurity by generating new opportunities in this sector to encourage people to take more interest in this field. If we achieve this we will have a dedicated industry of people passionate and well-equipped to handle these attacks and to generate new technologies to reduce the chances of the attack.

This paper aims to tell the very basics of cyber security, its types, and some of the preventive measures we could take to prevent cyberattacks.

6. REFERENCES

https://en.wikipedia.org/wiki/Cyberattack
https://en.wikipedia.org/wiki/Idle_scan
Figures:
[1] Fig 1:
https://upload.wikimedia.org/wikipedia/commons/thumb/3/3f/Stachledraht_DDos_Attack.svg/220px-Stachledraht_DDos_Attack.svg.png
[2] Fig 2:
https://en.wikipedia.org/wiki/File:Virus_Blaster.jpg
[3] Fig 3:
https://upload.wikimedia.org/wikipedia/commons/thumb/d/d0/PhishingTrustedBank.png/220px-PhishingTrustedBank.png
[4]Fig 4
https://upload.wikimedia.org/wikipedia/commons/thumb/f/f9/Public_key_encryption.svg/250px-Public_key_encryption.svg.png