IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 2, March 2022
Impact Factor: 6.252

A Review Paper on Cyber Security

Adish K[1] and Venkatesh[2]
Student, Department of Computer Science and Engineering[1]
Senior Associate Professor, Department of Computer Science of Engineering[2]
Alva's Institute of Engineering and Technology, Mijar, Mangalore, Karnataka, India

Abstract: *Cybersecurity is a broad term that incorporates a wide range of techniques, technologies, and concepts that are closely tied to information and operational technology (OT) security. Cybersecurity is special in that it includes the use of information technology on the offensive to strike adversaries. Customers and security practitioners are confused by the use of the phrase "cybersecurity" as a key challenge and a synonym for information security or IT security, which obscures critical differences between these disciplines.*

Keywords: Cybersecurity.

I. INTRODUCTION

Cyber security refers to the strategies used to safeguard a user's cyber environment. This environment encompasses the person, their devices, networks, applications, and any software, among other things. Cyber security is a subset of computer security that deals with the internet. The main security goal is to project the device using various rules and to set up various safeguards to protect it from online attacks.

The technique of protecting computers, servers, mobile devices, electronic systems, networks, and data from harmful technology security or electronic information security is known as cyber security. The phrase is used in a range of contexts, ranging from business to mobile computing, and it may be broken down into a few categories.

Since the advent of the Internet and the digital change that has occurred in recent years, the concept of cybersecurity has become a common topic in both our professional and personal life. For the last 50 years of technological advancement, cybersecurity and cyber threats have remained constant. Until the invention of the Internet in the 1970s and 1980s, computer security was primarily relegated to academia, where, with growing connectivity, computer viruses and network intrusions began to take off. The 2000s saw the institutionalisation of cyber risks and cybersecurity, following the rise of viruses in the 1990s.

Cloud computing, mobile computing, E-commerce, online banking, and other cutting-edge technologies all require a high level of security. Because these technologies contain sensitive information about a person, their security has become a priority. Enhancing cyber security and safeguarding important information infrastructures are critical to the security and economic well-being of any country. Making the Internet safer (and protecting Internet users) has become a key component of both new service development and government regulation. The fight against cybercrime necessitates a more comprehensive and secure strategy. Given that technical measures alone cannot prevent any crime, it is vital that law enforcement agencies be given the tools they need to properly investigate and prosecute cybercrime. Many countries and governments are enacting severe cyber security legislation nowadays.

II. TYPES OF CYBER SECURITY

2.1 Critical Infrastructure Cyber Security

Because SCADA (supervisory control and data acquisition) systems generally rely on older software, critical infrastructure organisations are more vulnerable to attack than others.

2.2 Network Security

Addressing vulnerabilities in your operating systems and network architecture, such as servers and hosts, firewalls and wireless access points, and network protocols, is part of network security.

2.3 Cloud Security

The security of data, apps, and infrastructure in the cloud is the focus of cloud security.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 2, March 2022
Impact Factor: 6.252

2.4 IoT (Internet of Things) Security

IoT security refers to the protection of smart devices and networks that are connected to the internet of things. Smart fire alarms, lighting, thermostats, and other appliances are examples of IoT devices that connect to the Internet without the need for human involvement.

2.5 Application Security

Addressing vulnerabilities originating from unsafe development processes in the design, coding, and publication of software or a website is what application security is all about.

III. THREATS

3.1 Malware

Malware is a term that refers to malicious software. Malware is software designed by a cybercriminal or hacker to disrupt or damage a legitimate user's computer. It is one of the most common cyber dangers. Malware is commonly disseminated by unsolicited email attachments that appear to be legal downloads. It can be employed by hackers to make money or in politically motivated cyber-attacks.

3.2 Virus

It's a form of malicious software that copies itself by changing other computer programmes when it's run. Computer viruses create financial harm by causing system failure, data corruption, and increased maintenance costs, among other things.

3.3 Worms

A computer worm is a type of malware that copies itself and spreads to other computers. Many worms are merely designed to spread and do not attempt to alter the systems through which they move.

3.4 SQL Injection

An SQL (structured language query) injection is a type of cyber-attack that allows a hacker to take control of a database and steal information from it. Using a malicious SQL query, cybercriminals exploit vulnerabilities in data-driven systems to install malicious code into a database. This provides them with access to the database's sensitive information.

3.5 Trojan Horse

A Trojan Horse, sometimes known as a Trojan, is a term for malicious software that appears to be harmless, allowing it to be downloaded onto a computer by the user's own volition. An attacker can use a Trojan to steal personal information from users, such as banking information, email passwords, and personal identities. It also has an impact on other networked devices.

IV. LATEST CYBER THREATS

4.1 Dridex Malware

The leader of an organised cyber-criminal group was charged in December 2019 by the US Department of Justice (DoJ) for his role in a global Dridex malware attack. This malevolent effort has a global impact on the general public, government, infrastructure, and industry.

Dridex is a financial trojan that can do a lot of things. It has been infecting computers since 2014, infecting them through phishing emails or existing malware. It has caused enormous financial losses equivalent to hundreds of millions of dollars by stealing passwords, banking credentials, and personal data that can be used in fraudulent transactions. The National Cyber Security Centre of the United Kingdom encourages the public to "ensure devices are patched, anti-virus is turned on and up to date, and files are backed up" in reaction to the Dridex attacks.

4.2 Romance Scams

In February 2020, the FBI issued a warning to Americans about confidence fraud perpetrated by cybercriminals through dating sites, chat rooms, and apps. Victims are duped into handing out personal information by perpetrators who take

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 2, March 2022
Impact Factor: 6.252

advantage of those looking for new mates. According to the FBI, romance cyber threats affected 114 people in New Mexico in 2019, resulting in $1.6 million in losses

.

4.3 Emotet Malware

The Australian Cyber Security Centre issued a warning to national entities in late 2019 about a widespread global cyber threat posed by Emotet virus. Emotet is a complex trojan that has the ability to steal data as well as install additional infections. Emotet thrives on simple passwords, which serves as a reminder of the significance of selecting a safe password to protect against cyber attacks.

4.4 Phishing

It's the attempt to get sensitive information like credit card numbers, usernames, and passwords, usually for nefarious purposes. Phishing is most commonly carried out through spoofing of instant messaging or email, and it frequently urges people to enter personal information on a bogus website. Links to malware-infected websites may be included in phishing emails. Phishing is the most common form of social engineering used to deceive people, and it takes advantage of flaws in current web security. Phishing is of Different Types-

- **Phishing with spear:** Spear phishing refers to phishing attempts focused at specific individuals or businesses. With 91 percent of attacks, this is the most successful tactic on the internet today. The attackers acquire information about the companies and their targets in order to improve their chances of succeeding.
- **Phishing with a Clone:** It's a form of phishing attack in which the content and recipient address(es) of an email containing an attachment or link are captured and utilised to construct a nearly identical or cloned email..
- **Whaling:** Several phishing attacks have been directed specifically at senior executives and other people with high-profile targets within businesses so these types of attacks are termed as whaling.

V. KEYSTROKE LOGGING

It's also known as key logging or keyboard capture, and it occurs when the individual using the keyboard is unaware that their actions are being recorded. It's essentially the act of recording the keys pressed on a keyboard. There are a variety of key logging methods available, ranging from software and hardware to auditory analysis.

- **Software Based Key Loggers:** These are computer applications that are designed to work with the software on the target computer. In IT companies, key loggers are used to debug technical issues with computers and business networks. Key loggers are used legally by families and businesses to monitor network activity without their users' knowledge.
- **Hardware Based Key Loggers:** Hardware-based key loggers do not require the installation of any software because they operate at the hardware level of a computer system.

VI. REMEDIES

6.1 Firewall

A computer firewall regulates network access. It includes filters that are specific to one firewall or the other. A firewall is a computer security system that regulates and monitors incoming and outgoing network traffic according to security rules. A firewall is essentially a barrier between a trusted, secure internet network and other outside networks, such as the internet, that are not safe or trustworthy.

6.2 Internet Security Products

1. **Antivirus:** Antivirus and internet security software can protect a programmable device from viruses by identifying and removing them. Antivirus software was employed in the early days of the internet, but with the expansion of the internet, various free security applications are now available.
2. **Password Managers:** A password manager is a piece of software that allows you to save and organise your passwords. Password managers typically encrypt passwords, forcing the user to create a master password; a single, ideally very strong password that grants access to the user's full password database.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 2, March 2022
Impact Factor: 6.252

3. **Security Suits:** Firewalls, anti-virus, anti-spyware, and other security suits are among the security suits. They also provide free theft prevention, security checks for portable storage devices, private internet browsing, and security-related decisions.
4. **Security Tokens:** Some online companies give customers the option of using a security token with a six-digit code that changes every 30-60 seconds. Based on the current time integrated into the gadget, the keys on the token have built computations and manipulated numbers. This implies that every thirty seconds, there is only one potential sequence of digits that will allow you to access your online account.

VII. CONCLUSION

Computer security is a broad topic that is growing increasingly relevant as the world becomes increasingly interconnected, with networks being used to conduct critical transactions. With each New Year that passes, cyber crime and the protection of information continue to split along distinct routes. Organizations are being challenged not just by how they safeguard their infrastructure, but also by how they require new platforms and intelligence to do so, thanks to the latest and disruptive technologies, as well as the new cyber tools and threats that emerge every day. Although there is no ideal answer to cybercrime, we should do everything we can to reduce it in order to ensure a safe and secure future in cyberspace.

REFERENCES

[1]. A Sophos Article 04 12v1.dNA, eight trends changing network security by James Lyne
[2]. Computer Security Practices in Non-Profit Organisations – A NetAction Report by Audrie Krause
[3]. A Look back on Cyber Security 2012 by Luis corrons – Panda Labs
[4]. IEEE Security and Privacy Magazine – IEEECS "Safety Critical Systems – Next Generation "July/ Aug 2013
[5]. https://en.wikipedia.org/wiki/Malware
[6]. Drucker H. Wu D. Vapnik VN. Support vector machines for spam categorization. IEEE Trans Neural Netw Publ IEEE Neural Netw Counc 1999; 10(5):1048–54
[7]. Cyber Attack Trends Analysis Key Insights to Gear Up for in 2019. Available Online: http://www.snt.hr/boxcontent/ CheckPointSecurityReport2019_vol01.pdf