International Journal of Engineering Applied Sciences and Technology, 2024
Vol. 9, Issue 08, ISSN No. 2455-2143, Pages 38-41
Published Online December 2024 in IJEAST (http://www.ijeast.com)

CYBER SECURITY THREATS AND DEFENSES- A REVIEW

Naveen Monga, Dr.Rajesh Kumar
Assistant Professor (Computer Sc.)
Pt. ChiranjiLal Sharma Govt. College Sector-14, Karnal

Abstract: **In the age of the internet, cyberattacks have grown very frequent. Every year, the number of cybercrimes rises along with the severity of the harm. In this digital age, offering protection against cyberattacks becomes crucial. However, maintaining cyber security is a very complex undertaking that calls for both domain knowledge about attacks and the ability to analyze potential risks. The primary obstacle in cyber security is the dynamic character of threats. This paper discusses the importance of cyber security as well as the different threats and preventive measures that exist in the modern digital world.**

I. INTRODUCTION

Generally speaking, cyber security refers to the methods used to safeguard the user's online environment. The user, devices, networks, apps, all software, etc. are all part of this ecosystem.

The primary goal is to lower risk, including that of cyberattacks.

The area of computer security that deals with the internet is called cyber security. Projecting the device using different rules and putting in place different defenses against online attacks are the primary security goals.

Numerous techniques are employed to improve internet security and stop online threats. The number of cyberattacks is growing daily due to the increase in online activities and applications.

Cybersecurity includes protecting data availability and integrity as well as confidentiality and privacy, all of which are essential for the standard and safety of care. Using paper records, fax machines, and even spoken communication can all lead to security breaches. But the repercussions of security lapses are possibly much more serious with digital material since it can be shared more readily and reach a larger audience. Cyber breaches are expensive, both in terms of money spent and the time it takes to recover, as well as reputational harm. According to a 2017 Government Cyber Breaches Survey, 46% of companies had experienced a cyberattack or breach.

Government-oriented organizations are just as susceptible to cyber dangers as private businesses. Any malware can quickly encrypt the victim's files once it has access to any operating system. The increasing complexity of contemporary encryption methods further complicates this, making it very challenging to recover encrypted material without a decryption key. Currently, as the Only the ransom ware host has access to this key; the victim must pay the ransom to obtain the key and unlock the data that the malware operator has hidden. In these situations, the losses sustained go beyond the ransom money and include the price of restoring the compromised system, the abrupt halt to commercial operations being brought to a sudden standstill, and the urgent need to install further anti-malware to tighten the security.[5]

Recovering from a cyberattack's effects, such as lost revenue, reputational harm, and business disruption, may be costly and time-consuming without a specific cyber policy. In addition to creating and testing an incident response and business continuity plan, organizations are also encouraged to create a thorough cybersecurity roadmap.

In order to help its clients effectively tackle new potential cyber risks, even in the early stages of cybercrime growth, Cyble, a cybersecurity services provider, provides them with dark web and cybercrime monitoring capabilities.

In addition to providing enterprises with actionable intelligence and a real-time picture of the threat environment, Cybele's flagship product, Cyble Vision, gives clients comprehensive assessments on malware, potential cyberthreats, and data leaks.

Networks, computer systems, various programs, and data are all protected from cyberattacks, damage, and unauthorized access by a collection of technologies, procedures, and practices known as cyber security. The goal of cyber security is to guarantee the success and safety of the security hazards in the cyber environment, as well as the association's and users' property security attributes.

The fastest-growing infrastructure in daily life today is the Internet. Numerous cutting-edge technologies are changing the face of humanity in today's technological environment. High levels of security are also required for even the newest technologies, such as cloud computing, mobile computing, e-commerce, online banking, etc. Many countries and governments are already enforcing stringent cyber security rules to guard against the loss of some crucial data.[1]

International Journal of Engineering Applied Sciences and Technology, 2024
Vol. 9, Issue 08, ISSN No. 2455-2143, Pages 38-41
Published Online December 2024 in IJEAST (http://www.ijeast.com)

II. DISCUSSION

Protecting cyberspace from online attacks is the focus of cyber security. The concept of "cyber threats" is a little nebulous and suggests that a variety of bad actors may utilize information and communication technology (ICT) as a tool or as a target. Three things are often referred to by the term "cyber security":

➢ A collection of technical and non-technical actions and measures meant to defend computers, computer networks, associated hardware and software, data and information, and other components of cyberspace against all threats, including those to national security.

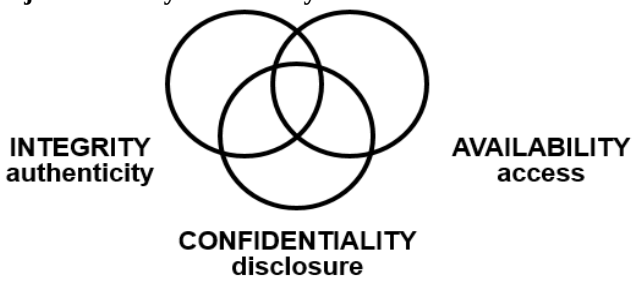
➢ The level of protection brought about by the implementation of these actions and measures.

➢ The related field of professional endeavor, including research and analysis, aimed at putting those actions and measures into practice.

Understanding the ramifications of various cyberattacks and creating defense tactics—that is, countermeasures—that maintain the availability, confidentiality, and integrity of any digital data are also aspects of cyber security . Malware, according to many cyber security experts, is the primary weapon of choice for carrying out malevolent seeks to undermine cyberspace security measures. Malware is a type of attacks that are installed on a system, usually without the owner's knowledge, with the intention of compromising it for the adversary's advantage.

Viruses, worms, Trojan horses, spyware, and bot executables are a few examples of malware.[2]

Objectives of Cyber Security



Confidentiality

The quality that information is not shared or made available to unapproved people, organizations, or procedures is known as confidentiality.

Integrity

Integrity is the quality of ensuring that assets are accurate and comprehensive.

Availability

The quality of being useable and available to an authorized entity upon request. [10]

III. THE MOST COMMON CYBERATTACK TYPES

Advance Persistent Threats

Long-term targeted attacks known as advanced persistent threats, or APTs, infiltrate a network in stages in order to evade discovery. An APT has five stages: reconnaissance, which involves learning about and investigating the target; intrusion, which involves sending malware to the target; Exfiltration (using information that has been taken), capture (accumulating data over a long period of time), and discovery (charting the target's internal defenses).[7]

Distributed Denial of Service

DDoS occur when a server is intentionally overloaded with requests, with the goal of shutting down the targets website or network system. Users will not be able to access your site or network, resulting in a partial or complete shutdown of your business operations, depending on how heavily you rely on the Internet.

Inside attack

An advanced software program might not even be necessary for this kind of cyberattack:

An someone who intentionally abuses their administrative privileges, typically from within the company, credentials in order to access private company data. Your organization should have a procedure in place to quickly revoke all access to company data upon an employee's termination since former employees, in particular, pose a threat if they left on bad terms. Insider attacks can also occur when a hacker impersonates a company your organization collaborates with in order to obtain private information.[12]

Malware or “malicious software

Any application installed on the target's computer with the intention of causing harm or gaining unauthorized access is referred to as malware, or "malicious software."

Malware comes in numerous forms, such as Trojan horses, worms, ransom ware, spyware, viruses, and key loggers.

Password attacks

The most straightforward method for hackers to access their target's databases and accounts is to crack a password. Three primary categories of password assaults exist: brute force assault, in which passwords are guessed until the hacker gains access; dictionary attack, which tries various dictionary word combinations using a program; and key logging, which keeps note of every keystroke a user makes, including passwords and login IDs.[11]

Phishing

Possibly the most widely used type of cybercrime, phishing entails obtaining private data, such as credit card numbers and login credentials, by creating an authentic-looking (but ultimately fake) website, frequently distributed by email to

International Journal of Engineering Applied Sciences and Technology, 2024
Vol. 9, Issue 08, ISSN No. 2455-2143, Pages 38-41
Published Online December 2024 in IJEAST (http://www.ijeast.com)

gullible people. Hackers have gotten more skilled, so it's critical to stay up to date with the most recent strategies to protect yourself as people become more aware of classic phishing techniques—for example, a warning from a financial institution with an unprotected or mismatched URL[3]

IV. CYBER SECURITY ELEMENTS

Using hardware, software, and procedural techniques to protect an application against external threats, viruses, malware, or attacks is known as application security. Application security and the persuade apps to access, steal, alter, or remove private information. [8]

- Communication Security: COMSEC is another name for communication security. Any written sequence that is sent or transferred to another device via any other medium will benefit from this development, which aims to protect or prevent unauthorized access to traffic created by telecommunications systems.

Cryptographic security: It scrawls information on the correspondent surface after encrypting it, waiting for the beneficiary to decrypt it.

- Emission Security**:** Emission security is the process of preventing the release or confinement of equipment emissions in order to prevent unconstitutional interception.
  Physical security: It provides protection against unauthorized access to a network's cryptography. information, documents, and equipment. Transmission security: It is intended to prevent problems like service interruptions and data theft by malicious individuals by defending against unlawful access while data is actually moved from one surface to another surface or medium to another medium.
- Information Security: Information security is the process of protecting data and its vital components, such as the hardware and software systems that are used to gather or disseminate that data. Infosec is another name for information security. It is a set of tactics for overseeing the processes, tools which are utilized in software and policies of software that is primarily used for security purposes and is required to prevent, detect, and counteract attacks to both digital and non-digital systems sequentially. Its duties include a collection of business procedures that will protect the sequence assets, including their formatting, transfer status, processing, and storage space rest. The programs adhere to the CIA's primary goals while upholding discretion.[6]
- Network Security: Network security is used to protect networking equipment, network associations, and network-related content. In order to monitor the network and incorporate security software and hardware, a network security system typically uses layers of security and several components. as well as its appliances. Every piece of equipment cooperates to improve the computer network's overall security and performance.
  Operational Security: Operational security is a methodical procedure that identifies the controls needed to protect resources and arranges them in a certain order. OPSEC is another name for operational security. It usually consists of an iterative five-step process.[9]

4.1 Preventive Measures

1. **Educate your employees**. Employees are one of the most popular ways for cybercriminals to obtain your data. They will send phony emails pretending to be from someone in your company, requesting access to certain files or personal information. To the untrained eye, links frequently appear authentic, and it's simple to fall for the trick. Employee awareness is essential for this reason.

Educating your staff about current cyberattacks and how to prevent them is one of the best strategies to defend against cyberattacks and other forms of data breaches.

They must:

- Verify links before clicking on them.

Verify the email addresses in the received email .

2. **Maintain the most recent versions of your systems and applications**.
   Cyberattacks frequently occur as a result of vulnerabilities left by outdated software or systems. Therefore, hackers take advantage of these flaws to infiltrate your network. It's frequently too late to take precautionary action once they've entered. Purchasing a patch management system, which will oversee all software and system upgrades.
3. **Make sure that endpoints are protected.** Networks that are remotely bridged to devices are safeguarded by endpoint protection. Access points to security risks are provided by laptops, tablets, and mobile devices linked to business networks. Certain endpoint protection software must be used to safeguard these pathways.
4. **Put a firewall in place.**Sophisticated data breaches emerge in a wide variety of forms, and new ones are discovered daily and occasionally even resurface. Using a firewall to protect your network is one of the best defenses against online threats. A firewall system, which we can assist you with, can stop brute force attacks on your network and/or systems before they have a chance to cause any harm.
5. **Make a backup of your data.** To prevent significant downtime, data loss, and severe financial loss in the case of a disaster (often a cyberattack), you must have a backup of your data.

6. **Manage who has access to your systems**. Controlling who has access to your network is crucial since, despite popular belief, physical attacks are one of the threats that can affect your systems. All it takes for someone to gain access to your entire network or infect it is for them to enter your workplace or place of business, plug in a USB key that contains malicious files, and then use one of your computers. Controlling who has access to your computers is crucial. Installing a perimeter security system is a great approach to prevent both cybercrime and break-ins!
7. **Security via Wi-Fi**. In 2020, who doesn't have a gadget with wifi? And that's precisely the issue: By connecting to a network, any device can become infected. If this compromised device subsequently connects to your company's network, your entire system is at significant risk.One of the safest things you can do for your systems is to secure and conceal your wifi networks. There are thousands of devices that could connect to your network and compromise you as wireless technology advances daily.
8. **Personal accounts of employees.** Each employee must have a unique login for each software and application. Your company may be at risk if multiple users connect using the same login credentials. You can lessen the number of attack fronts by giving each employee their own login. Users will only use their personal login credentials and will only log in once every day. Improved usability is just as beneficial as increased security.
9. **Management of Access**. Installing software on company-owned devices that could jeopardize your systems is one of the risks of being a business owner with employees. Your security will benefit from having managed administrator rights and preventing employees from installing or even accessing specific files on your network. It is your company; keep it safe!
10. **Passwords**. It can be risky to use the same password for everything. A hacker may now access every program and file on your computer once they have figured out your password.
    Creating distinct passwords for each application you use is a great way to improve your security, and changing them frequently will keep your defenses against both internal and external threats strong. Learn more about creating strong passwords here.[4]

V. CONCLUSION

Cybersecurity is no longer just a technical challenge; it is a fundamental necessity in our increasingly interconnected world. As digital innovation drives global progress, the risks associated with cyber threats grow in complexity and scale. Protecting sensitive data, securing critical infrastructure, and ensuring user privacy are vital to maintaining trust in technology and safeguarding societal stability.

A robust cybersecurity strategy requires collaboration between individuals, organizations, and governments, underpinned by continuous education, proactive risk management, and cutting-edge technologies. By prioritizing cybersecurity, we can create a resilient digital environment that fosters innovation while protecting against ever-evolving threats, ensuring a safe and sustainable future in the digital age.

REFERENCES:

[1]. Shetty Sudheer etal**.** (2022).Review Paper on Cyber Security, International Journal of Advanced Research in Science, Communication and Technology (IJARSCT) ,(pp. 518-521).

[2]. ObotivereB.A. and NwaezeigwA.O.(2020). Cyber Security Threats on the Internet and Possible Solutions,International Journal of Advanced Research in Computer and Communication Engineering,(pp.92-97).

[3]. https://www.sbir.gov/sites/all/themes/sbir/dawnbreaker/img/documents/Course10-Tutorial2.pdf

[4]. https://leaf-it.com/10-ways-prevent-cyber-attacks/

[5]. https://www.simplilearn.com/tutorials/cyber-security-tutorial/types-of-cyber-attacks

[6]. Asakpa S.O,AdeifeO. T, and Isaiah,O. J.(2018). E-crimes on the internet and possible solutions"- 3rd National Conference of the Academic Staff Union of Polytechnics (ASUP) Zone C, Ado- Ewe at the Federal Polytechnic, Ado Ekiti.

[7]. https://www.imperva.com/learn/application-security/apt-advanced-persistent-threat/.

[8]. JainJitendra and Ram Pal Parashu.(2017).A Recent Study over Cyber Security and its Elements,International Journal of Advanced Research in Computer Science(pp. 791-793)

[9]. Agarwal Kartikey & Dubey Sanjay Kumar.(2014), Network Security: Attacks and Defense" in International Journal of Advance Foundation and Research in Science & Engineering (IJAFRSE) Volume 1(3).

[10]. https://sprinto.com/blog/cyber-security-goals/

[11]. https://www.portnox.com/cybersecurity-101/password-attack/

[12]. https://www.geeksforgeeks.org/what-is-insider-attack/