International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 8, Issue 10, pp 289-292, October-2024

https://doi.org/10.47001/IRJIET/2024.810039

Cyber Security Study on Attack, Threat, Vulnerability

[1]Samiksha S Kanse, [2]Dr. S. B. Sarvaiya

[1]MCA-II, Department of MCA, Vidhya Bharti Mahavidyalaya, Amravati, Maharashtra, India

[2]Head, Department of MCA, Vidhya Bharti Mahavidyalaya, Amravati, Maharashtra, India

Authors E-mail: [1]Samikshakanse04@gmail.com, [2]sarvaiya.shilpa@gmail.com

***Abstract* - This research aims to investigate risks linked to cyber infrastructure, including hardware, software systems, networks, and intranets, with an emphasis on cyber intrusions. The objective is to underscore the importance of network intrusions and cyber theft by examining factors that have fueled the growth of cybercrime. This paper offers a detailed definition of cybersecurity and its role in counteracting network intrusions and cyber theft, while analyzing the drivers behind the rise in cybercriminal activities and their impacts. Additionally, preventive strategies and potential remedies to reduce cybersecurity vulnerabilities are discussed. The paper concludes that while technology can diminish the effects of cyberattacks, human behavior and psychological aspects are key vulnerabilities. Nonetheless, there is optimism about the role of educational initiatives within organizations in mitigating cyber threats.**

Keywords: Cyber-attack, Malware, Phishing, DoS attack, Threat, Vulnerability, AES, DES.

I. INTRODUCTION

With the rapid rise in digitalization and cashless transactions, even governmental and defense organizations have increasingly encountered cyber losses and disruptions. However, enforcing cybercrime laws presents unique challenges due to the distinct nature of cyberspace versus the physical world. For instance, verifying age in cyberspace is challenging, as individuals can easily misrepresent their age to access restricted content, unlike in the physical world where age verification is more straightforward. Cybersecurity involves strategies designed to prevent, detect, and respond to cyber threats.

While the widespread use of computers marks societal advancement, it also introduces new challenges. Sophisticated hacking techniques pose risks to network security, making it difficult for professionals to detect vulnerabilities and trace perpetrators. Defense mechanisms in cybersecurity focus on understanding potential attackers, their motivations, and assessing network vulnerabilities to strengthen future security measures.

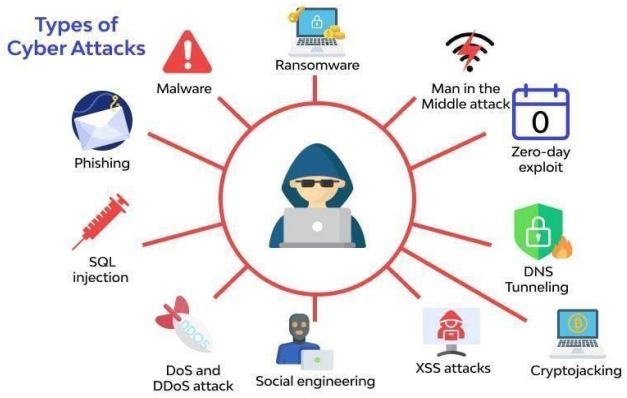

Figure 1: Types of Cyber-Attacks

II. METHODOLOGY

Despite numerous updates since the initial Symantec Internet Security Threat Report, the latest version includes an array of new insights. The report not only identifies industry trends but also provides an analysis of specific threats identified through our research. Security entails a comprehensive approach, emphasizing the need to understand attacks, threats, and vulnerabilities, which are interconnected concepts. For example, outdated software can make a computer vulnerable to viruses and other malicious activities, highlighting the importance of regularly updating both the computer's software and antivirus programs.

Advanced Encryption Standard (AES):

The AES, established by the U.S. National Institute of Standards and Technology (NIST) in 2001, is a well-known encryption standard for securing electronic data. It offers higher security than DES and triple DES, though it is more complex to implement. AES operates as a block cipher with key sizes of 128, 192, or 256 bits, encrypting data in 128-bit blocks.

Data Encryption Standard (DES):

DES, a 56-bit key block cipher, played an important role in data security historically but has become less popular due to its vulnerability to powerful attacks. It operates on 64-bit plaintext blocks, yielding ciphertext of the same length. The same algorithm and key are used for encryption and decryption, albeit with slight variations.

International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 8, Issue 10, pp 289-292, October-2024

https://doi.org/10.47001/IRJIET/2024.810039

Threats:

Cybersecurity threats cover a wide range of potentially illegal activities conducted online. While concerns about cybersecurity threats to essential utility assets have long existed, there has been a notable increase in cyberattacks on commercial power distribution systems by criminal organizations and foreign entities. Such attacks could result in severe power outages, impacting economies and public health, thus drawing heightened attention to securing critical infrastructures.

A) Cyber Theft:

Cyber theft, often referred to as hacking, involves the unauthorized acquisition of information or assets via the internet. Cyber thieves use various methods, such as plagiarism, piracy, hacking, espionage, DNS cache poisoning, and identity theft, to gain access to sensitive information.

B) Cyber Vandalism:

Cyber vandalism occurs when data is damaged or misused rather than stolen, disrupting network services and preventing authorized users from accessing information. This type of cybercrime often involves the distribution of harmful software or the intentional insertion of malicious code like viruses into networks.

C) Web Jacking:

This form of cyber intrusion involves unauthorized access and control over another website, which could allow the attacker to alter data on the web server, thereby endangering online spaces.

D) Card Information Theft:

Cybercriminals frequently target e-commerce servers to obtain sensitive credit or debit card information, putting financial data at risk.

E) Cyber Terrorism:

Cyber terrorism involves using online platforms to carry out politically motivated violence against civilians.

F) Child Exploitation Materials:

This refers to the production, distribution, or access to materials that exploit underage children, a criminal activity conducted through computer networks.

G) Cyber Contraband:

Cyber contraband involves the illegal distribution of prohibited materials or information over the internet.

H) Spam:

Spam is the unauthorized sending of unsolicited emails to promote illegal products or inappropriate content, violating the SPAM Act.

I) Cyber Assault via Threats:

Cyber assault by threat uses electronic communications to intimidate individuals into transferring money to an untraceable bank account through online payment services.

J) Denial of Service (DoS):

A DoS attack disrupts the availability of computer resources by overwhelming the target with excessive requests. Such attacks can vary in methods and targets but are generally aimed at disabling internet services or sites for prolonged periods. When performed via email, these are called email bombings, with notable platforms such as eBay, Yahoo, and Amazon having fallen victim to such attacks.

Attacks:

Cyber-attacks present significant global challenges due to their impact on critical infrastructure and data. With advancing technology, it has become increasingly difficult to identify and thwart these attacks, leading to user apprehension and skepticism about new technologies. A cyberattack occurs when an individual gains unauthorized access to a computer with malicious intent.

A) Untargeted Attacks:

Untargeted attacks indiscriminately affect as many users and services as possible by exploiting network vulnerabilities. Attackers employ tactics such as phishing, ransomware, and scanning to compromise systems on a large scale.

B) Targeted Attacks:

In targeted attacks, specific individuals or organizations are selected for cyber intrusions, often through spear-phishing emails or botnet-driven Distributed Denial of Service (DDoS) attacks. Attackers may probe systems for vulnerabilities, such as hardware or software weaknesses, before executing these attacks.

International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 8, Issue 10, pp 289-292, October-2024

https://doi.org/10.47001/IRJIET/2024.810039

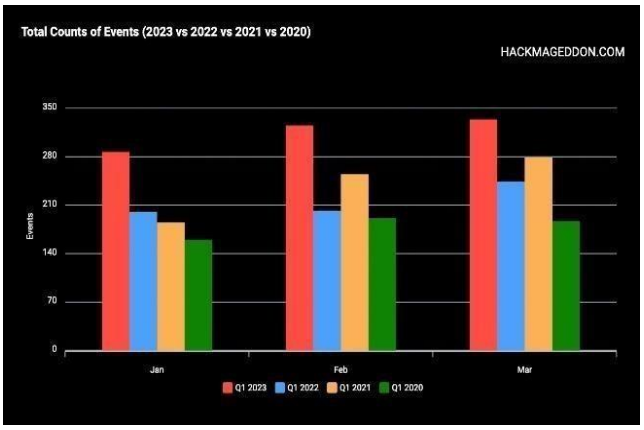

Figure 2: Ratio of Cyber Attack

Vulnerabilities:

System vulnerabilities, or weaknesses, allow unauthorized access, data breaches, or service disruptions. These can arise from issues within the system's hardware, software, procedures, or user behaviors. They are often discovered due to hardware compatibility issues or software design flaws and are exacerbated by human error or system complexity. The risks associated with unaddressed vulnerabilities—such as negligence or complacency—are well-documented, with recent trends showing a surge in zero-day exploits and rapid advancements in exploit kits. As devices become more interconnected, the potential for vulnerabilities to be exploited continues to grow.

III. RESULTS AND ANALYSIS

Securing systems requires a three-pronged strategy involving prevention, detection, and response. Prevention includes implementing firewalls, security software, and antivirus programs. Detection necessitates monitoring for signs of compromise, and response involves promptly addressing detected issues. Security measures also include preventing viruses, mitigating social engineering attacks, and securing wireless networks.

IV. CONCLUSION

Cybersecurity incidents underscore the need for computer-literate users, as they remain the first line of defense against cyber threats. New employees are particularly at risk, with attackers often targeting them to obtain personally identifiable information. Psychological factors contribute to network vulnerability, highlighting the importance of user education. While technology plays a significant role in reducing cyber attacks, addressing behavioral and psychological factors remains essential. Adopting comprehensive cybersecurity models can help reduce threats in the future.

REFERENCES

[1] Jibril, A. B., et al. Customers' perception of cybersecurity threats toward e-banking adoption and retention: A conceptual study. in ICCWS 2020 15th International Conference on Cyber Warfare and Security. 2020. Academic Conferences and publishing limited.

[2] Al-Mohannadi, Hamad, et al. "Cyber-Attack Modeling Analysis Techniques: An Overview." Future Internet of Things and Cloud Workshops (FiCloudW), IEEE International Conference on. IEEE, 2016.

[3] Panja, B., et al. Cybersecurity in banking and financial sector: Security analysis of a mobile banking application. in 2013 international conference on collaboration technologies and systems (CTS). 2013. IEEE.

[4] Rowe, Dale C., Barry M. Lunt, and Joseph J. Ekstrom. "The role of cyber-security in information technology education." Proceedings of the 2011 conference on Information technology education.ACM, 2011.

[5] Abomhara, M., & Køien, G. M. (2015). Cyber security and the internet of things: vulnerabilities, threats, intruders and attacks. Journal of Cyber Security and Mobility, 65-88.

[6] Ahmad, A. (2012). Type of security threats and it's prevention. Int. J. Computer Technology & Applications, 3(2), 750-752.

[7] Al-Mohannadi, H., Mirza, Q., Namanya, A., Awan, I., Cullen, A., &Disso, J. (2016, August). Cyberattack modeling analysis techniques: An overview. In 2016 IEEE 4th international conference on future internet of things and cloud workshops (FiCloudW) (pp. 69- 76). IEEE.

[8] "Internet Security Threat Report Internet Report "Volume 21, April 2016. https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.

[9] Ten, C. W., Liu, C. C., & Manimaran, G. (2008). Vulnerability assessment of cybersecurity for SCADA systems. IEEE.

[10] Yadav, V. (2020). A Study of Threats, Detection and Prevention in Cybersecurity. International Research Journal of Engineering and Technology (IRJET), May, 1150-1153.

International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 8, Issue 10, pp 289-292, October-2024

https://doi.org/10.47001/IRJIET/2024.810039

Citation of this Article:

Samiksha S Kanse, Dr. S. B. Sarvaiya. (2024). Cyber Security Study on Attack, Threat, Vulnerability. *International Research Journal of Innovations in Engineering and Technology - IRJIET*, 8(10), 289-292. Article DOI https://doi.org/10.47001/IRJIET/2024.810039

****

