IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Cybersecurity: A Study On Attacks, Threats, And Vulnerabilities

[1]Adam Musa Safiyanu, [2] Abubakar Suleiman, [3]Awal Jibrin Yakubu
[1, 2,3] Department of Computer Science, Nasarawa State University, Keffi

Abstract: The broad objective of this study is to examine the attacks, threats, and vulnerabilities of cyber infrastructure, including hardware and software systems, networks, enterprise networks, and intranets. To achieve this objective, the paper explains the significance of network intrusions and cyber-theft. It discusses in detail the reasons for the rapid increase in cybercrime, provides comprehensive definitions and descriptions of cybersecurity, and examines its role in network intrusions and cyber-theft. The paper analyses the factors contributing to the rise in cybercrime and their impacts. In conclusion, the authors recommend preventive measures and possible solutions to mitigate the attacks, threats, and vulnerabilities in cybersecurity. The study concludes that while technology is crucial in reducing the impact of cyber-attacks, human behaviour and psychological predispositions significantly contribute to vulnerabilities. Despite the risks posed by psychological susceptibilities, investment in organizational education campaigns offers hope that cyber-attacks can be mitigated.

Index Terms - Cyber-Warfare, Vulnerability, Cyber-attack, Threat

1. Introduction

The world is rapidly transitioning to digitalization and cashless transactions. Even government and defense organizations have experienced significant cyber losses and disruptions. The crime environment in cyberspace differs significantly from real space, presenting unique challenges for enforcing cybercrime laws. For example, age in real space is a self-authenticating factor, but in cyberspace, an underage individual can easily hide their age and access restricted resources. Cybersecurity involves protecting information by preventing, detecting, and responding to cyber-attacks [1].

The increasing integration of computers into society is a step toward modernization but requires better preparation to tackle the associated challenges. New hacking techniques and undiscovered security vulnerabilities pose difficulties for security professionals in identifying hackers. Defense mechanisms must focus on understanding their own network, the nature of the attacker, their motivations, attack methods, and network security weaknesses to mitigate future attacks [6].

2. Background

Currently, media, government sectors, and organizations are engaged in extensive discussions about cybersecurity. Some experts argue that the topic is over-hyped and driven by fear, with terms like "cyber-warfare" designed to provoke emotional responses. A recent Intelligence study suggests that the threat of cyber-war is grossly overstated. Cybersecurity is a crucial topic that inspires independent thinking among researchers and experts.

Many cybercrimes result from poor security practices rather than a lack of government policies. The president of the Electronic Privacy Information Center suggests opposing mandatory Internet identification requirements, pointing out that such requirements have led to censorship and human rights violations in some countries. Regardless of differing views, it is clear that cybersecurity is a critical and current topic deserving of healthy discussion.

This paper provides a realistic definition of cybersecurity and suggests key elements for inclusion in Information Technology programs, based on research documents and reports. With the recurrence of cyber-attacks on the rise, governments and security organizations worldwide are taking proactive measures to reduce the risk of successful attacks against critical infrastructures. This emphasizes the relationship between the physical and cyber domains. Cybersecurity involves protecting infrastructure by preventing, detecting, and responding to cyber incidents [13].

The association between military strikes on civilians and government-based Internet suppression is evident, with actions in the physical world paving the way for cyber-events. IT professionals may be aware of recent incidents involving malware targeting Supervisor Control and Data Acquisition (SCADA) systems, which exploit both patched and new vulnerabilities. These issues can have severe physical and financial impacts globally. Fortunately, not all cyber-events result in loss of life, but the economic impact can still be substantial. Information and electronic data theft have surpassed all other forms of fraud, despite a reduction in other fraud categories [11].

The Comprehensive National Cybersecurity Initiative (CNCI) is part of a broader U.S. cybersecurity strategy with the following goals:

1. Establish a frontline defense against immediate cyber threats.
2. Defend against the full spectrum of threats.
3. Strengthen the future cybersecurity environment.

These goals align with the CNCI's initiatives and highlight the need for global cooperation in addressing cybersecurity challenges, as no single group, country, or agency can claim ownership. According to a 2009 report by the U.S. Department of Homeland Security, a Roadmap for Cybersecurity Research identifies research and development opportunities to address eleven "hard problems" outlined by the INFOSEC Research Council (IRC).

Cybersecurity is defined as the "preservation of confidentiality, integrity, and availability of information in cyberspace," with cyberspace being "the complex environment resulting from the interaction of people, software, and services on the Internet via technology devices and networks." This makes cybersecurity a topic of significant discussion, interest, and attention [13].

3. Methodology

This is the 21st edition of the Symantec Internet Security Threat Report, which has evolved significantly since its inception. This report provides a fresh look at its structure and contents, focusing on threats and findings from our research, while also tracking industry trends. It highlights important developments and anticipates future trends, extending beyond computer systems, smartphones, and other products to encompass broader concepts such as national security, the economy, data protection, and privacy [12].

3.1 Threats

Cybersecurity threats encompass a wide range of illegal activities on the internet. These threats against utility assets have been recognized for decades, especially following terrorist attacks that have drawn attention to the security of critical infrastructures. Insecure computer systems can lead to fatal disruptions, disclosure of sensitive information, and fraud. Cyber threats arise from the exploitation of system vulnerabilities by unauthorized users. These crimes can target computer networks or services directly, such as malware, viruses, or denial of service attacks, or be facilitated by networks or devices, targeting independent entities like fraud, identity theft, phishing scams, and cyberstalking.

a. **Cyber Theft:** Cyber theft, commonly referred to as hacking, involves using the internet to steal information or assets. This includes illegal access through malicious scripts that break or crack computer system or network security without user knowledge or consent. Major companies like banks, Microsoft, Yahoo, and Amazon have been victims. Tactics include plagiarism, hacking, piracy, espionage, DNS cache poisoning, and identity theft.
b. **Cyber Vandalism:** Cyber vandalism involves damaging or exploiting data rather than stealing it, disrupting or stopping network services and depriving authorized users of access. This can include the creation and dissemination of harmful software, entering malicious code into networks, and other severe actions without the network owner's permission.
c. **Web Jacking**: Web jacking refers to gaining unauthorized control over a web server and manipulating information on the site.

d. **Stealing Card Information** This involves stealing credit or debit card information by hacking into e-commerce servers and misusing the information.
e. **Cyber Terrorism**: Cyber terrorism involves politically motivated violence committed against civilians using the internet.
f. **Child Pornography**: This includes using computer networks to create, distribute, or access materials that sexually exploit underage children.
g. **Cyber Contraband**: Transferring illegal items or information through the internet that is banned in some locations.
h. **Spam**: Unauthorized transmission of spam, including illegal product marketing or immoral content via emails.
i. **Cyber Trespass**: Unauthorized access to network resources without altering or damaging the data or system, such as snooping on network traffic.
j. **Bombs:** Event-dependent programs that activate after specific triggers, like the Chernobyl virus.
k. **Drive-by Download**: Automatic installation of malicious software on a user's computer while browsing the internet to steal confidential information or use the victim's terminal as a botnet.
l. **Cyber Assault by Threat**: Using computer networks to threaten individuals, instilling fear for their lives or the lives of others, often involving blackmail.
m. **Script Kiddies**: Novices using scripts or programs developed by others to attack computer systems and deface websites.
n. **Denial of Service (DoS):** DoS or Distributed Denial of Service (DDoS) attacks aim to make a computer resource unavailable to its users by overwhelming it with requests, causing it to crash. This can also be known as email bombing. Major victims include eBay, Yahoo, and Amazon [1].

3.2 Attacks

Cyber-attacks pose a significant threat to critical infrastructure and data security. The advancement of technology is accompanied by cybersecurity threats, which can compromise users' security. The difficulty in identifying and preventing cyber threats and attacks often leads users to hesitate in adopting new technologies. A cyber-attack occurs when someone maliciously gains or attempts to gain unauthorized access to a computer system [11].

a. **Untargeted Attacks**: Untargeted attacks indiscriminately target as many users and services as possible, exploiting vulnerabilities in services or networks. Common techniques include:

- **Phishing:** Sending emails that appear to be from legitimate sources to trick recipients into providing personal information, such as banking or credit card details. This often involves directing users to fake websites with enticing offers [8].
- **Watering Hole Attack:** Setting up fake websites or compromising legitimate ones to exploit visitors' information.
- **Ransomware:** Spreading malware that encrypts a victim's data and demands payment for decryption.
- **Scanning:** Randomly probing wide areas of the internet for vulnerabilities.

b. **Targeted Attacks**: Targeted attacks focus on specific individuals or organizations. Techniques include:

- **Spear-Phishing:** Sending targeted emails containing links or attachments with malicious software to specific individuals.
- **Deploying Botnets:** Using networks of infected computers to carry out Distributed Denial of Service (DDoS) attacks.
- **Subverting the Supply Chain:** Attacking network or software supply chains to compromise an organization's systems.

In general, attackers initially use tools and techniques to probe systems for exploitable vulnerabilities [3].

3.3 Vulnerabilities

Vulnerabilities are weaknesses in a system or its design that allow intruders to execute commands, access unauthorized data, or conduct denial-of-service attacks. These vulnerabilities can arise in various areas, including system hardware, software, policies, procedures, and even users themselves.

Hardware vulnerabilities often relate to compatibility and interoperability issues and may be challenging to fix. Software vulnerabilities can be present in operating systems, application software, and control software, including communication protocols and device drivers. Factors such as human error and software complexity can lead to design flaws [10].

No system is automatically immune from cyber threats, and ignoring these risks can lead to severe consequences. In 2015, an unprecedented number of vulnerabilities were identified, including zero-day exploits that were quickly weaponized and incorporated into web attack exploit kits. As more devices become interconnected, the potential for exploiting vulnerabilities increases [12].

4. Results and Analysis

Securing the System: There are three primary methods to secure systems against external threats and attacks:

1. **Prevention:** Implementing firewalls, security software, and antivirus programs to keep threats out.
2. **Detection:** Regularly updating security software and hardware to identify potential breaches.
3. **Reaction:** Responding effectively to detected breaches, with security software providing alerts when incidents occur.

4.1 Preventing Attacks and Threats

- Recovering from Viruses, Worms, and Trojan Horses
- Avoiding Social Engineering and Networking Attacks
- Avoiding the Pitfalls of Online Trading
- Using Caution with USB Drives
- Securing Wireless Networks

4.2 Preventing Email and Communication Threats

- Using Caution with Email Attachments
- Reducing Spam
- Using Caution with Digital Signatures
- Using Instant Messaging and Chat Rooms Safely
- Staying Safe on Social Networking Sites

4.3 Safe Browsing

- Evaluating Your Web Browser's Security Settings
- Shopping Safely Online
- Understanding Website Certificates
- Using Bluetooth Technology Safely [5].

5. Conclusion

The research suggests that the most effective defense against cybersecurity incidents involves increasing computer literacy among users. It highlights that new employees in an organization are particularly vulnerable, as attackers often seek personal identifiable information from them. The study also emphasizes the role of psychological factors in user and network vulnerability. While technology can help reduce the impact of cyber attacks, human behaviour and psychological predispositions significantly contribute to vulnerabilities. Education can influence these factors, offering some mitigation against cyber threats. However, an absolute solution to eliminate cybersecurity threats has yet to be developed. Future work in this field will focus on implementing cybersecurity models to reduce network vulnerabilities and threats.

References

1. 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
2. Ahmad, A. (2012). Type of security threats and it's prevention. *Int. J. Computer Technology & Applications*, *3*(2), 750-752.
3. Al-Mohannadi, H., Mirza, Q., Namanya, A., Awan, I., Cullen, A., & Disso, J. (2016, August). Cyber-attack modeling analysis techniques: An overview. In *2016 IEEE 4th international conference on future internet of things and cloud workshops (FiCloudW)* (pp. 69-76). IEEE.
4. Byres, E., & Lowe, J. (2004, October). The myths and facts behind cyber security risks for industrial control systems. In *Proceedings of the VDE Kongress* (Vol. 116, pp. 213-218).
5. Conteh, N. Y., & Schmick, P. J. (2021). Cybersecurity risks, vulnerabilities, and countermeasures to prevent social engineering attacks. In *Ethical hacking techniques and countermeasures for cybercrime prevention* (pp. 19-31). IGI Global.
6. Mohammad, I., Pandey, R., & Khatoon, A. (2014). A Review of types of Security Attacks and Malicious Software in Network Security. *International Journal of Advanced Research in Computer Science and Software Engineering (IJARCSSE)*, *4*(5).
7. Parikh, T. P., & Patel, A. R. (2017). Cyber security: Study on attack, threat, vulnerability. *Int. J. Res. Mod. Eng. Emerg. Technol*, *5*, 1-7.
8. Razzaq, A., Hur, A., Ahmad, H. F., & Masood, M. (2013, March). Cyber security: Threats, reasons, challenges, methodologies and state of the art solutions for industrial applications. In *2013 IEEE Eleventh International Symposium on Autonomous Decentralized Systems (ISADS)* (pp. 1-6). IEEE.
9. Rowe, D. C., Lunt, B. M., & Ekstrom, J. J. (2011, October). The role of cyber-security in information technology education. In *Proceedings of the 2011 conference on Information technology education* (pp. 113-122).
10. Teymourlouei, H. (2015). Quick reference: Cyber attacks awareness and prevention method for home users. *International Journal of Computer and Systems Engineering*, *9*(3), 678-684.
11. Teji, J., Chuchra, R., Mahajan, S., Gill, M. K., & Dandi, M. (2013). Detection and Prevention of Passive Attacks in Network Security. *Int. J. Eng. Sci. Innov. Technol*, *2*(06), 247-250..
12. Ten, C. W., Liu, C. C., & Manimaran, G. (2008). Vulnerability assessment of cybersecurity for SCADA systems. *IEEE Transactions on*
13. Yadav, V. (2020). A Study of Threats, Detection and Prevention in Cybersecurity. *International Research Journal of Engineering and Technology (IRJET)*, *May*, 1150-1153.