iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 12 **Issue:** II **Month of publication:** February 2024

DOI: https://doi.org/10.22214/ijraset.2024.58472

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 12 Issue II Feb 2024- Available at www.ijraset.com

Cyber Security: Study on Attack, Threat, Vulnerability

Dhyan Patel
ICT, Ganpat University

Abstract: ***The main aim of this research is to examine the various aspects of cyber infrastructure, encompassing both hardware and software systems, networks, enterprise networks, intranets, and the occurrence of cyber intrusions. The paper intends to elucidate the significance of network intrusions and cyber-theft, along with delving into the factors contributing to the proliferation of cybercrime. Furthermore, it provides a comprehensive definition of cyber security and its role in addressing network intrusion and cyber theft, while also exploring the drivers behind the surge in cybercrime and their repercussions. The authors conclude by suggesting preventive measures and potential solutions to mitigate the risks associated with cyber attacks. They emphasize that while technological advancements can aid in minimizing the impact of cyber attacks, human behavior and psychological tendencies remain significant vulnerabilities. Despite this, the authors express optimism in reducing cyber attacks through investment in organizational education campaigns that address psychological susceptibilities.***
Keywords: Cyber-Warfare, Vulnerability, Cyber-attack, Threat

I. INTRODUCTION

The world is rapidly embracing digitalization and cashless transactions, leading to a manifold increase in their usage. However, this transition has also brought about significant cyber losses and disruptions for government and defense organizations. The cybercrime landscape differs vastly from that of the physical world, posing numerous challenges in enforcing cybercrime laws compared to traditional laws. For instance, while age is easily verifiable in real space, it is not as straightforward in cyberspace. This makes it easier for individuals, particularly minors, to conceal their age online and access restricted resources. Cybersecurity plays a crucial role in safeguarding information by preventing, detecting, and responding to cyber-attacks.

Although the integration of computers into society represents a positive step towards modernization, there is a pressing need to enhance our capabilities to effectively address the challenges posed by evolving technology. Hackers employ new techniques to infiltrate networks, exploiting security vulnerabilities that often go undetected, thereby complicating the task of security professionals in identifying and thwarting cyber threats. Defense mechanisms primarily revolve around comprehending the intricacies of one's own network, understanding the nature and motives of potential attackers, as well as the methods they employ. It is essential to identify security weaknesses within the network in order to mitigate future attacks effectively.

II. BACKGROUND

Currently, there is a widespread discussion about cybersecurity in various sectors including media, government, and organizations. However, experts argue that the topic is often exaggerated and driven by fear, using terms like 'cyberwarfare' to evoke emotional rather than rational responses. A recent study by Intelligence has found that threats like cyber-war are often overstated.

Despite differing opinions, cybersecurity remains an important and relevant topic that fosters independent thinking among researchers and experts. Many security experts suggest that cybercrimes are often a result of poor security rather than a lack of government policy implementation. Suggestions against mandatory Internet identification requirements have been made, citing concerns about censorship and human rights violations in countries where such requirements are enforced.

Cybersecurity involves protecting critical infrastructure from cyber incidents through prevention, detection, and response strategies. The relationship between physical and cyber domains is significant, as seen in instances where military actions in the physical world precede cyber-events. Recent events, such as attacks on Supervisor Control and Data Acquisition (SCADA) systems, highlight the potential physical and financial impact of cyber-attacks on a global scale.

While cyber-events may not always result in loss of life, their economic impact can be substantial. Data theft has surpassed other forms of fraud, indicating the growing threat posed by cyber-attacks. The Comprehensive National Cybersecurity Initiative (CNCI) aims to establish a robust cybersecurity strategy, emphasizing the importance of global cooperation in addressing cyber threats.

The US Department of Homeland Security's 2009 report proposes a roadmap for cybersecurity research, focusing on preserving the confidentiality, integrity, and availability of information in cyberspace. Cyberspace is defined as the complex environment resulting from the interaction of people, software, and services on the Internet, facilitated by technology devices and networks.
Overall, cybersecurity remains a topic of significant discussion, interest, and attention, highlighting the need for proactive measures to address evolving cyber threats.

III. METHODOLOGY

This is the 21st edition of the Symantec Internet Security Threat Report and much has changed since the first one. We take a fresh look at the structure and contents of the report. As well as focusing on the threats and findings from our research, it is also tracks industry trends. We try to highlight the important developments and look to future trends. This goes beyond just looking at computer systems, smartphones, and other products, and extends into broad concepts like national security, the economy, data protection, and privacy [14].

A. Threats

Cybersecurity threats encompass a broad spectrum of potentially illegal activities conducted on the internet. Concerns regarding cybersecurity threats against utility assets have been acknowledged for many years. The attention to security of critical infrastructures has increased following terrorist attacks. Insecure computer systems pose risks such as significant disruptions, unauthorized disclosure of sensitive information, and fraudulent activities. Cyber threats arise from the exploitation of vulnerabilities within cyber systems by unauthorized users.
There are two main categories of cybercrimes: those that directly target computer networks or services, such as malware, viruses, or denial of service attacks, and those facilitated by networks or devices where the primary target is independent of the network or device. Examples include fraud, identity theft, phishing scams, and cyber stalking.

1) Cyber Theft

This is the most common cyber-attack that committed in cyberspace. This kind of offence is normally referred as hacking in the generic sense. It basically involves using the internet through steal information or assets. It also called the illegal access, by using the malicious script to break or crack the computer system or network security without user knowledge or consent, for tampering the critical data and. It is the gravest cybercrimes among the others. Most of the banks, Microsoft, Yahoo and Amazon are victim of such cyber-attack. Cyber thieves use tactics like plagiarism, hacking, piracy, espionage, DNS cache poisoning, and identity theft. Most of the security web sites has described the various cyber threats.

2) Cyber Vandalism

Damaging or exploiting the data rather than stealing or misusing them is called cyber vandalism. It means effect on network services are disrupted or stopped.
This deprives the authorized users for accessing the information contained on the network. This cybercrime is like a time bomb, can be set to bring itself into action at a specified time and damage the target system. This creation and dissemination of harmful software which do irreparable damage to computer systems, deliberately entering malicious code like viruses, into a network to monitor, follow, disrupt, stop, or perform any other action without the permission of the owner of the network are severe kind of cybercrimes.

3) Web Jacking

Web jacking is the forceful control of a web server through gaining access and control over the web site of another. Hackers might be manipulating the information on the site.

4) Stealing Cards Information

Stealing of credit or debit card information by stealing into the ecommerce server and misuse these information.

5) Cyber Terrorism

Deliberately, usually politically motivated violence committed against civilians through the use of, or with the help of internet.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 12 Issue II Feb 2024- Available at www.ijraset.com

6) Child Pornography

The use of computer networks to create, distribute, or access materials that sexually exploit underage children pornography in shared drives of community networks.

7) Cyber Contraband

Transferring of illegal items or information through internet that is banned in some locations, like prohibited material.

8) Spam

It includes the Violation of SPAM Act, through unauthorized transmission of spam by sending illegal product marketing or immoral content proliferation via emails.

9) Cyber Trespass

cyber trespass" refers to unauthorized access or intrusion into computer systems or networks for malicious purposes. It involves activities like hacking, malware infections, or unauthorized use of digital resources. It's a serious cybersecurity threat addressed through security measures and may lead to legal consequences for perpetrators.

10) Legal accessing of network resources without altering disturbs, misuse, or damage the data or system. It may include accessing of private information without disturbing them or snooping the network traffic for gets some important information.

11) Logic Bombs

These are event dependent programs. These programs are activated after the trigger of specific even. Chernobyl virus isa specific example which acts as logic bomb and can sleep of the particular date.

12) Drive by Download

A survey is undertaken by search engine companies. Numbers of websites were acting as hosts for malware. The term “Drive by Download (DbD)” is maneuvering in software industry since its inception with different variations. It is a phenomenon in which any software program is installed automatically on a user computer while surfing on the internet. The intent of installing malicious software is to gain benefit over victim machine, e.g. it could be a stealing of confidential information like stored passwords, personal data, using victim terminal as botnet to further spread malicious contents.

13) Cyber Assault by Threat

The use of a computer network such as email, videos, or phones for threatening a person with fear for their lives or the lives of their families or persons whose safety they are responsible for (such as employees or communities). An example of this is blackmailing a person to a point when he is forced to transfer funds to an untraceable bank account through an online payment facility.

14) Script Kiddies

Novices, who are called script kiddies, script bunny, script kitty, script running juvenile is a derogatory term used to describe those who use scripts or programs developed by others to attack computer systems, networks and get the root access and deface websites.

15) Denial of Service

A denial of service attack (DoS) or distributed denial of service attack (DDoS) is an attempt to make a computer resource unavailable to its intended users. The computer of the victim is flooded with more requests than it can handle which cause it to crash. Although the means to carry out, motives for, and targets of a DoS attack may vary, it generally consists of the concerted efforts of a person or people to prevent an Internet site or service from functioning efficiently or at all, temporarily or indefinitely. This is also known as email bombing if via used is email. E-bay, Yahoo, Amazon suffered from this attack [1].

B. Attacks

Cyber-attacks pose a significant threat to critical infrastructure and data security in the digital realm, necessitating focused attention. The advancement of technology brings with it the proliferation of cyber security threats, commonly known as "cyber-attacks," which jeopardize the security of users utilizing these technologies.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 12 Issue II Feb 2024- Available at www.ijraset.com

Detecting and preventing cyber threats and attacks proves challenging, leading to a lack of acceptance of new technologies among users due to concerns about data security. Essentially, a cyber-attack occurs when an individual maliciously gains or attempts to gain unauthorized access to a computer system.

1) Untargeted Attacks

Un-targeted attacks involve attackers indiscriminately targeting as many users and services as possible, exploiting vulnerabilities within the service or network. Attackers may leverage various technologies to carry out these attacks, including phishing.

Phishing is a tactic where malicious actors impersonate legitimate entities, typically via email, to deceive users into divulging personal information such as banking or credit card details. These fraudulent emails often lure recipients with enticing offers or urgent requests, prompting them to click on links that lead to fake websites. Unaware of the scam, users willingly provide their sensitive information, unaware that they have fallen victim to fraud.

2) Targeted attacks

Targeted attacks in attackers, attack on the targeted users in the cyber world. Spear-phishing

Sending links of malicious software and advertisement via emails to targeted individuals that could contain for downloads malicious software. Deploying a botnet. It is deliver a DDOS (Distributed Denial of Service) attack Subverting the supply chain.

To attack on network or software being delivered to the organization In general attackers will, in the first instance use tools and techniques to probe your systems for an exploiting vulnerability of the service [3].

C. Vulnerability

Vulnerabilities represent weaknesses within a system or its design that enable an intruder to execute commands, gain unauthorized access to data, or conduct denial-of-service attacks. These vulnerabilities can manifest in various areas within systems, including hardware, software, policies, procedures, and user behaviors. Hardware vulnerabilities may stem from compatibility issues or interoperability challenges, while software vulnerabilities can be found in operating systems, applications, and control software such as communication protocols and device drivers. Factors contributing to software design flaws include human errors and the complexity of software systems. Technical vulnerabilities often arise from human weaknesses.

No system is inherently immune to cyber threats, and the consequences of disregarding risks due to complacency, negligence, or incompetence are evident. In 2015, an unprecedented number of vulnerabilities were identified as zero-day exploits that had been weaponized, and web attack exploit kits are adapting and evolving at a rapid pace. As the number of connected devices increases, vulnerabilities will continue to be exploited.

IV. RESULTS AND ANALYSIS

Securing a system from outsider threats and attacks typically involves three fundamental methods:

1) *Prevention:* This involves implementing measures to keep threats out of the network. Examples include using firewalls, security software, and ensuring end-users have antivirus software installed. The goal is to proactively prevent unauthorized access and potential breaches by implementing robust security measures.
2) *Detection:* It's essential to have mechanisms in place to detect when security failures or breaches occur. This includes regularly updating both security software and hardware to ensure they can effectively identify and respond to emerging threats. Continuous monitoring and analysis of system logs and network traffic are also important for timely detection of suspicious activities.
3) *Reaction:* Once a security failure or breach is detected, it's crucial to have the capability to respond promptly and effectively. This involves having predefined response plans and procedures in place to mitigate the impact of the incident. For example, if security software detects a potential threat, it should trigger alerts or notifications to prompt immediate action from system administrators or security personnel. Additionally, having backup and recovery plans in place can help minimize downtime and data loss in the event of a security incident.

V. CONCLUSION

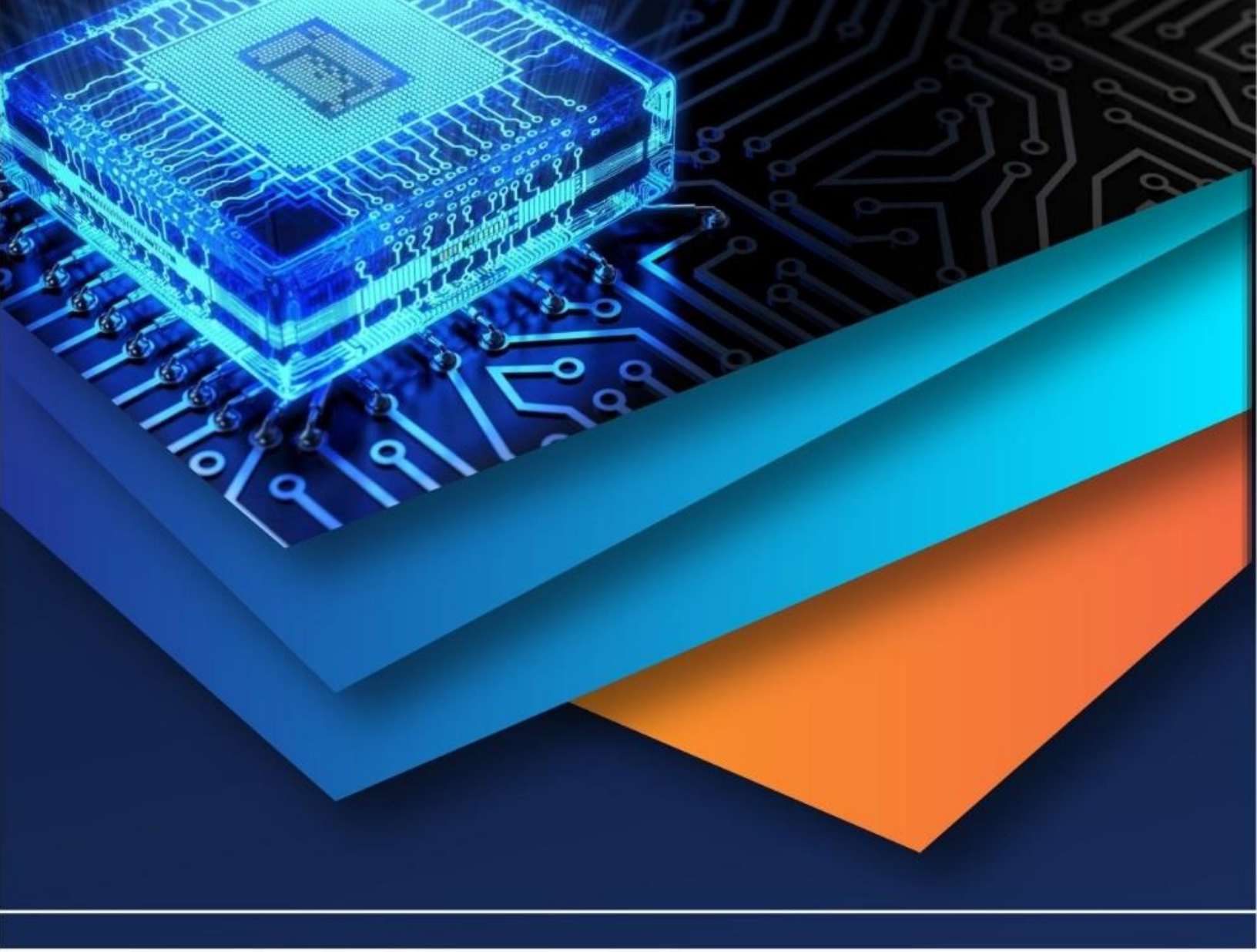
Cybersecurity incidents involving attacks highlight the importance of having computer-literate users as the most effective defense. Research indicates that individuals who are well-versed in computer technology are better equipped to defend against cyber threats. Particularly vulnerable in this regard are new employees within organizations, who may be targeted by attackers seeking personal identifiable information.

Additionally, psychological variables play a significant role in user and network vulnerability. This research concludes that while technology plays a role in mitigating cyber attacks, the primary source of threat and vulnerability lies in human behavior, impulses, and psychological predispositions. Education and awareness programs aimed at addressing these psychological factors can contribute to reducing cyber attacks.

While cyber attacks can be mitigated, this research acknowledges that there is no absolute solution to overcoming cybersecurity threats. Future work in this area should focus on implementing cyber security models to reduce the risk of cyber attacks, threats, and vulnerabilities within networks.

REFERENCES

[1] Razzaq, Abdul, et al. "Cyber security: Threats, reasons, challenges, methodologies and state of the art solutions for industrial applications. "Autonomous Decentralized Systems (ISADS), 2013 IEEE Eleventh International Symposium on. IEEE, 2013.
[2] Byres, Eric, and Justin Lowe. "The myths and facts behind cyber security risks for industrial control systems." Proceedings of the VDE Kongress. Vol. 116. 2004.
[3] "Common Cyber Attacks: Reducing The Impact Gov.uk" https://www.gov.uk/...data/.../Common_Cyber_Attacks-Reducing_The_Impact.pd
[4] "CYBERSECURITY: CHALLENGES FROM A SYSTEMS, COMPLEXITY,KNOWLEDGE MANAGEMENT AND BUSINESS INTELLIGENCE PERSPECTIVE" Issues in Information Systems Volume 16, Issue III, pp. 191-198, 2015
[5] "Cyber security: risks, vulnerabilities and countermeasures to prevent social Engineering attacks" International Journal of Advanced Computer Research, Vol 6(23) ISSN (Print): 2249-7277 ISSN (Online): 2277-7970 http://dx.doi.org/10.19101/IJACR.2016.623006
[6] Ahmad, Ateeq. "Type of Security Threats and It's Prevention." Int. J. Computer Technology & Applications, ISSN (2012): 2229-6093.
[7] Ten, Chee-Wooi, Chen-Ching Liu, and Govindarasu Manimaran. "Vulnerability assessment of cyber security for SCADA systems." IEEE Transactions on Power Systems 23.4 (2008): 1836-1846.
[8] "Cyber Crime-Its Types, Analysis and Prevention Techniques", Volume 6, Issue 5, May 2016 ISSN: 2277 128X www.ijarcsse.com
[9] "A Review of types of Security Attacks and Malicious Software in Network Security" Volume 4, Issue 5, May 2014 ISSN: 2277 128X www.ijarcsse.com
[10] Abomhara, Mohamed, and G. M. Kien. "Cyber security and the internet of things: vulnerabilities, threats, intruders and attacks." Journal of Cyber Security 4 (2015): 65-88.
[11] "Quick Reference: Cyber Attacks Awareness and Prevention Method for Home Users" International Journal of Computer, Electrical, Automation, Control and Information Engineering Vol:9, No:3, 2015
[12] "Detection and Prevention of Passive Attacks in Network Security" ISSN: 2319-5967 ISO 9001:2008 Certified International Journal of Engineering Science and Innovative Technology (IJESIT) Volume 2, Issue 6, November 2013
[13] 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.
[14] "Internet Security Threat Report Internet Report "VOLUME 21, APRIL 2016 https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf
[15] 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.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY