International Journal of Electrical, Electronics and Computer Engineering **13**(1&2): 67-70(2024)

ISSN No. (Online): 2277-2626

Cyber Security: Study on Threat, Attack & Vulnerability

Prajwal Katoch*, Smriti Sharma and Prince
Department of School of Computer Science and Engineering
Govt. P.G College Dharamshala, Himachal Pradesh Technical University (HPTU), India.

(Corresponding author: Prajwal Katoch)*
(Received: 07 February 2024, Accepted: 22 April 2024)
(Published by Research Trend, Website: www.researchtrend.net)

ABSTRACT: The broad goal of this investigation is to learn more about cyber infrastructure attacks, threats, and vulnerabilities. These encompass hardware and software systems, networks, organization networks, intranets, and the utilization of cyber intrusions. To achieve this objective, the paper research into the significance of network invasions and cyber theft. It also explores the reasons behind the rapid expansion of cybercrime. The study provides a comprehensive definition of cyber security, its role in community infiltration, and understanding cyber theft. Additionally, it examines the factors contributing to the rise in cybercrime and their impact. The paper concludes by offering preventive measures and practical remedies to address cyber security attacks, threats, and vulnerabilities. While technological knowledge plays a role in mitigating the impact of cyber-attacks, the vulnerability primarily lies in human behaviour and psychological predispositions. This research highlights the risks posed by psychological vulnerabilities in cyber-attacks, but investments in organizational education programs offer hope for effective mitigation.

Keywords: Threat, Vulnerability, Cyber-attack, Cyber-Warfare

INTRODUCTION

The world's shift toward digitalization has led to reduced reliance on physical currency and fewer traditional transactions. However, this transition also exposes governments and security agencies to significant cyber losses and disruptions. Unlike real-life crime, the cyber environment presents unique challenges for enacting effective cybercrime legislation. For instance, while age serves as a self-authenticating factor in the physical world, it loses relevance in cyberspace. A child under 18 can easily conceal their age online and gain access to restricted resources, a feat that would be difficult in the real world. Cyber security plays a crucial role in safeguarding information by preventing, detecting, and responding to cyber-attacks (Razzaq *et al*., 2020). Despite the positive impact of widespread computer usage on modernization, society must remain vigilant in addressing technological challenges. New hacking techniques continually emerge, infiltrating communities and exploiting previously undetected security weaknesses. Security specialists focus on understanding attacker's perspectives, motivations, and strategies to prevent recurring attacks (Ahmad, Ateeq (2019). In summary, cyber security is essential, and proactive measures are necessary to protect against evolving cyber threats in our interconnected world.

THREATS

Cybersecurity threats span a broad spectrum of potentially unlawful activities occurring on the internet. Cyber security threats against utility assets have been perceived for a quite a long time. Insecure or shaky PC framework may lead to fatal disruption, disclosure of sensitive information, and frauds. Cyber threats result from exploitation of cyber system vulnerabilities by users with unauthorized access (Ten *et al.*, 2008). There are wrongdoings that targets PC organizations or administrationsimply like infections, malware or denial of organization assault and violations worked with by organizations or widgets, the primary aim is to ensure freedom from organizational or widget involvement, such as extortion, scams, deceitful tactics, or any other form of digital tracking.

1. Cyber Theft

This is the most prevalent cyber-attack occurring in cyberspace, often referred to as hacking in a broad sense. It primarily involves exploiting the internet to steal information or assets. Termed illegal access, this entails the use of malicious scripts to breach computer systems or network security without user consent, aiming to manipulate critical data. Amongst various cybercrimes, it stands out as one of the most severe. Numerous institutions including banks, Microsoft, Yahoo, and Amazon have fallen victim to this digital onslaught. Copyright infringement, hacking, theft, surveillance, DNS reserve hurting, and data fraud are among the tactics employed by digital criminals.

Numerous security websites have documented various digital threats.

2. Cyber Vandalism

Cyber vandalism refers to the act of damaging or exploiting data instead of simply stealing or misusing it. This involves disrupting or halting network services, thereby preventing authorized users from accessing the information within the network. This type of cybercrime can be likened to a time bomb, as it can be programmed to activate at a designated time and inflict harm upon the target system. Such acts entail the creation and dissemination of harmful software that causes irreparable damage to computer systems. Deliberately injecting malicious code, such as viruses, into a network to monitor, track, disrupt, halt, or execute any unauthorized action constitutes a severe form of cybercrime.

3. Web Jacking

Web jacking involves forcefully seizing control of a web server by gaining unauthorized access to and control over another party's website. Hackers may manipulate or alter the information present on the site as part of this illicit activity.

4. Stealing Cards Data

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

5. Cyber Terrorism

Deliberately, usually politically motivated violence committed against civilians using, or with the support of internet.

6. Child Pornography

The utilization of computer networks to produce, disseminate, or retrieve materials that exploit minors sexually, including pornography stored 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

The lawful utilization of network resources without modifying, disrupting, misusing, or harming the data or system. It may include accessing of private information without disturbing them or snooping the network traffic for getting some important information.

10. Logic Bombs

These are event dependent programs. These programs are activated after the trigger of specific event. Chernobyl virus is a specific example which acts as logic bomb and can rest of specific time.

11. Drive by Download

It installs malicious software on your device without your consent or knowledge. It can happen when you visit a website that has been compromised by hackers, or when you click on a link or an ad that leads to a malicious site. The malicious software can then harm your device, steal your data, or spy on your activity. To prevent drive by download attacks, you should keep your browser, apps, and operating system updated, avoid clicking on suspicious links or ads, and use a reliable antivirus software.

12. Cyber Assault by Threat

Utilizing computer network platforms such as email, video, or phones to install fear in an individual regarding their own safety or that of their family members or those under their care (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.

13. Script Kiddies

They are novice hackers who use scripts or programs developed by others, primarily for malicious purposes. They usually have little or no technical skills and do not understand the effects or consequences of their actions. They may hack for fun, attention, or thrill, without having a specific motive or goal.

14. Denial of Service

A denial-of-service (DoS) attack, or its more powerful variant, a distributed denial-of-service (DDoS) attack, aims to disrupt the availability of a computer resource for its intended users. Attackers achieve this by flooding the targeted system with overwhelming amounts of requests, causing it to slow down significantly or even crash. The motives and targets of DoS attacks vary, but the common goal is to hinder the normal function of an internet site or service temporarily or indefinitely. While attacks can be carried out through various means, email bombing is one specific method. Notable victims of past DoS attacks include companies like eBay, Yahoo, and Amazon (Razzaq, Abdul, *et al,* 2020).

ATTACKS

Digital assault is a big problem in the digital world that needs to be addressed due to its impact on the fundamental structure and information. The advancement of technology is accompanied by network security threats or "digital assaults," which jeopardize client security when using such advancements. Digital threats and assaults are difficult to spot and avoid. As a result, clients are resisting the innovation because digital tends to prioritize information security. A digital assault occurs when someone gains or tries to get unapproved access to a computer in an obnoxious manner Razzaq *et al.,* 2020).

UNTARGETED ATTACKS

An untargeted attack is a type of cyberattack that does not target a specific person, group, or organization, but rather tries to exploit as many devices, services, or users as possible. The attackers do not care about the identity or characteristics of their victims, if they can cause damage, steal data, or gain access to their systems. Some examples of untargeted attacks are phishing emails, malware infections, denial of service attacks, and zero-day exploits. Attacker can take the advantage of technologies like:

1. Phishing

Phishing is a type of cyber-attack where the attacker attempts to deceive the victim into revealing sensitive information or performing harmful actions. It involves sending fraudulent communications that appear to come from reputable sources ("Cyber Crime-Its Types, Analysis and Prevention Techniques," May 2020). It is commonly done through email. The goal is to:

1. Steal sensitive data like credit card and login information.
2. Install malware in the victim's machine.

2. Malware:

It refers to any software designed to harm or disrupt a computer system, network, or device. It encompasses a wide range of malicious programs with varying functionalities and purposes.

3. Ransomware:

Ransom ware is a type of malware that permanently blocks access to the victim's personal data unless a ransom is paid. It deceptive emails or messages that trick recipients into revealing sensitive information.

TARGETED ATTACKS

Targeted attacks, also known as advanced persistent threats (APTs), are sophisticated cyber-attacks aimed at a specific individual, organization, or group. Unlike widespread spam campaigns, these attacks are meticulously planned and executed with a high degree of customization ("Common Cyber Attacks: Reducing the Impact Gov.uk").

1. Spear phishing:

Emails crafted to appear legitimate and sent to a specific individual, often containing malicious attachments or links.

2. Watering hole attacks:

Compromising legitimate websites frequented by the target, infecting visitors with malware when they visit.

Before attacking a network or software deployed within an organization, attackers typically employ tools and techniques to scan the systems for exploitable vulnerabilities within the services ("Common Cyber Attacks: Reducing the Impact Gov.uk").

VULNERABILITY

Vulnerabilities are flaws within a system or its design that enable attackers to execute unauthorized commands, steal sensitive data, or disrupt services (known as denial-of-service attacks). These weaknesses can exist in various parts of a system, including its hardware, software, policies, or even user practices. Hardware vulnerabilities may arise from compatibility issues or difficulties in patching problems. Software vulnerabilities often occur within operating systems, applications, communication protocols, and device drivers, frequently stemming from design flaws caused by human error or the sheer complexity of the software. In many cases, technical vulnerabilities ultimately originate from human oversight or mistakes (Byres, Eric, and Justin Lowe, 2020). No system is inherently immune to cyber threats. Ignoring these threats due to complacency, negligence, or a lack of expertise can have severe consequences. In 2015, a record number of vulnerabilities were discovered and weaponized as zero-day exploits. Moreover, web attack exploit kits are constantly evolving to exploit these vulnerabilities at an alarming rate. As the number of interconnected devices grows, so too does the potential for vulnerability exploitation (Ahmad, Ateeq 2019).

RESULT AND ANALYSIS

Securing systems from external threats and attacks involves a multi-layered approach. Here are the three principal methods:

PREVENTION:

This method focuses on proactively blocking threats before they breach your system. It is like securing your home with a locked door and alarm system. Common preventive measures include:

1. Firewalls: These act as a barrier between your internal network and the external world, filtering incoming and outgoing traffic based on security rules.

2. Security software: This software scans for and blocks malicious software (malware) such as viruses, worms, and Trojans, preventing them from infecting your system (Mohamed and Kien 2020).

3. Antivirus software: This specific type of security software focuses on detecting and eliminating viruses, a particular type of malware.

DETECTION:

Even with robust prevention measures, vulnerabilities can exist. Detection helps identify ongoing attacks or breaches that have bypassed the initial defences. This is akin to having motion detectors in your home to alert you of unauthorized entry. Crucial aspects of detection include:

1. Regularly updating security software and hardware: Updates often contain critical security patches that fix vulnerabilities exploited by attackers.

2. Security monitoring: Continuously monitoring system activity and logs can help identify suspicious behaviours indicating potential attacks.

REACTION:

Detection allows for timely response to identified threats. This response is analogous to having a fire

extinguisher and knowing how to use it in case of a fire. Here is where your security software plays a crucial role:

1. **Alerting:** Upon detecting suspicious activity, security software should immediately notify you, allowing you to take appropriate action.
2. **Response options:** Depending on the severity of the threat and your security policies, the response may involve isolating infected systems, blocking malicious activity, or restoring from backups (Ten *et al.*, 2008).

CONCLUSIONS

This research emphasizes that the most effective defence against cyber-attacks involving personal information theft may be a computer-literate user base. New employees are often identified as particularly vulnerable, as attackers may specifically target them for their credentials.

This research further highlights the critical role of psychological factors in both user and network vulnerability. While technology plays a part in mitigating the impact of cyber-attacks, the ultimate source of threats and vulnerabilities often lies in human behaviour, impulses, and psychological predispositions.

The paper concludes that educating users can significantly reduce cyber-attacks. However, it acknowledges that an absolute solution remains elusive. Future research could focus on implementing cyber security models within networks to further reduce threats and vulnerabilities.

REFERENCES

Razzaq, A., Hur, A., Ahmad, H. F., & Masood, M. (2013). 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.

Byres, E., & Lowe, J. (2004). The myths and facts behind cyber security risks for industrial control systems. In *Proceedings of the VDE Kongress*, *116,* 213-218.

Cybersecurity: Challenges From a Systems, Complexity, Knowledge Management And Business Intelligence Perspective" *Issues in Information Systems, 16*(3), pp. 191-198, 2019

Ahmad, Ateeq (2019). Type of Security Threats and It's Prevention. *Int. J. Computer Technology & Applications,* ISSN (2019): 2229-6093.

Ten, C. W., Liu, C. C., & Manimaran, G. (2008). Vulnerability assessment of cybersecurity for SCADA systems. *IEEE Transactions on Power Systems*, *23*(4), 1836-1846.

"Cyber Crime-Its Types, Analysis and Prevention Techniques," Volume 6, Issue 5, May 2020 ISSN: 2277 128X www.ijarcsse.com

Mohamed A., and. Kien G. M. (2020). Cyber security and the internet of things: vulnerabilities, threats, intruders and attacks. *Journal of Cyber Security 4* (2020), 65-88.