IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 12, Issue 10, October 2024

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.625

© 2024 IJIRCCE | Volume 12, Issue 10, October 2024| DOI: 10.15680/IJIRCCE.2024.1210016

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Cyber-Security Today: The Threats in Cyber-Security and Preventions

Sakshi Kadam[1], Kevali Shete[1], Srushti Shingade[1], Asmita Varma[1], Sharmila .S. Bahirgunde[2]

Student, Department of CSIT, Sharad Institute of Technology Polytechnic, Ichalkaranji, Maharashtra, India[1]

Lecturer, Department of CSIT, Sharad Institute of Technology Polytechnic, Ichalkaranji, Maharashtra, India[2]

ABSTRACT: Cybersecurity is becoming a major worry for everyone in the hyperconnected digital age-individuals, businesses, and governments alike. The growing dependence on the internet and digital platforms has led to an increase in the sophistication, frequency, and destructiveness of cyber-attacks. This study examines how cyber security is developing, with a particular emphasis on advanced security features techniques, penetration measures for safeguarding vital digital infrastructure. Recognizing ransomware, social engineering, advanced persistent threats (APT), and vulnerabilities in key infrastructure. Looking into how ethical hacking helps find vulnerabilities before they may be used on us. In order to identify vulnerabilities in networks, systems, & applications, penetration techniques are examined in this part. Exploring cutting edge solutions including endpoint protection to improve resilience, blockchain for safe transactions, & artificial intelligence (AI) and machine learning (ML) for predictive threat analysis. This article emphasizes the necessity for a complete strategy that integrates penetration testing, preventive measures, & the deployment of cutting-edge cyber security features by looking at real-world case studies & security frameworks. In order to counter the quickly changing threat landscape, stakeholders must prioritize collaboration, innovation, & constant monitoring. In order to improve protection, this version emphasizes the value of security features that are directly incorporated into infrastructure and systems. It also combines cybersecurity features approaches.

KEYWORDS: penetration, reconnaissance, advanced persistent threat, vulnerability, foot printing.

I. INTRODUCTION

Cybersecurity, also referred to as “information technology security,” focuses on protecting computers, networks, data, and programs form accidental or intentional modification, loss, alteration, and access. Large amounts of personal data are stored, gathered, and used by government organizations, business, hospitals, financial institutions, the armed forces, and other groups on computers. The data is then sent via the network to the other computers, because cyberattacks are becoming more frequent and severe, it is imperative that secure sensitive information and trade while simultaneously protecting national security.

People are completely reliant on technologies are developed worldwide, but many are unaware of the risks and attacks posed by the cybercriminals. Cybercriminals are always developing new ways to get around security measures and access our personal data. Therefore, in order to prevent our sensitive data from getting into the wrong hands, it is imperative that we put strong cybersecurity practices in place. The issues that are being confronted now a days are: The 5G networks potential maybe unlawfully misused by

third parties. The promise of more effective use of their cherished devices has piqued the interest of younger people in the introduction of 5G networks. The possibility of psychological or physical assaults on this tech-savvy generation presents a problem, though. Cybercriminals might illegally access 5G wireless networks & take advantage of the information gathered or saved by quick and intelligent devices. These attackers, who are frequently outside parties, use cutting-edge marketing strategies to carry out their malevolent operations while taking advantage of the intricate architectures of 5G networks. The growing need for machine-to-machine (M2M) connectivity is expected to propel the 5G infrastructure industry, which is expected to reach 47.775 million US dollars by 2027. It is imperative to detect and impede the actions of these external attackers who persistently aim to obtain illegal access to customer’s information, jeopardizing privacy and confidence in customer-focused enterprises.

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

- **CIA Model: -**

The "CIA" is an acronym for the 3 words Confidentiality, Integrity & Availability. One popular model that serves as the foundation for the creation of security systems is the CIA triad.Information availability, confidentiality, & integrity are essential to a business's operations, and the CIA trinity divides these three concepts into distinction is useful because it directs security teams in identifying the many approaches to addressing each issue. When all three requirements are satisfied, the organization's security profile is ideally stronger and more capable of handling threat occurrences.

Figure 1: CIA Triad Model

1. Confidentiality-

It is the capacity to protect information so that only authorized users can access it, which means no unauthorized user should have access to confidential information. Data encryption, user authentication are examples of procedures used to ensure confidentiality. The purpose is to ensure that only those with permission to examine the data, thereby securing the data & maintaining privacy.

2. Integrity-

Maintaining integrity means ensuring that your data is reliable and unaltered. Only when the data is true, accurate, & dependable is its integrity preserved. Change control, digital signatures, & audit logs are some of the strategies used to ensure data integrity. These procedures aid in detection &prevention of unauthorized data modifications

3. Availability-

Information should be easily available to authorized individuals. This includes correctly maintaining the hardware, technical infrastructure, & systems that store and show the data.

II. ATTACKS

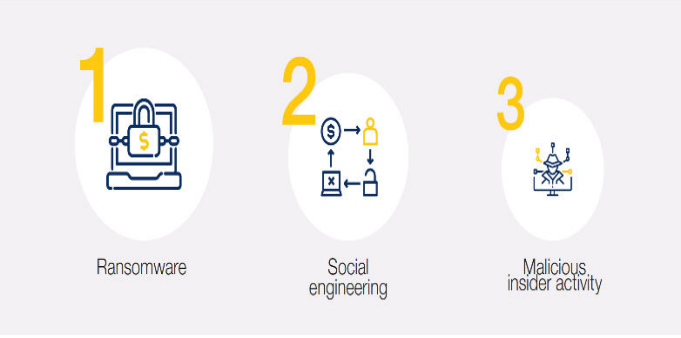

Figure 2: Top three attacks in Cyber-security

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

1. Ransomware-

It is a sort of malware assault in which the attacker encrypts & locks the victims' data, including the essential file, & then demands for the payment to open & decode it. This sort of assault exploits human, system, network, cell phones, etc. When a device is exposed to malicious code, the ransomware begins as follows:

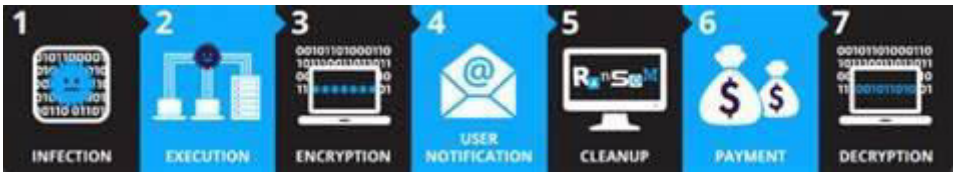

Figure 3: Seven stages of ransomware attack

2. Social Engineering-

These attacks in cyber security entail tricking people into disclosing sensitive data.These attacks take use of human psychology, such as trust, anxiety, & urgency. Awareness & training are critical defences against such attacks. Educating employees & individuals on how to recognize suspicious behaviour & verify requests can dramatically lower the likelihood of falling prey to social engineering.

3. Malicious insider activity-

Malicious insider activity in cyber-security refers to destructive actions conducted by someone within an organization that purposefully use their allowed access to systems, data or resources for malicious objectives. These insiders, who could be workers, contractors or other trusted individuals, may participate in actions such as data theft, which involves stealing sensitive or proprietary information for personal gain or to sell to competitors.

4. Phishing-

These attacks are the practice of delivering false messages that appear to be from a legitimate source. It is normally done by email. The purpose is to steal sensitive data, such as credit card &login information, or to install malware on the victim's computer.

5. Advanced Persistent Threat (APT)-

APT is a stealthy cyber attack on a computer network in which the attacker acquires& maintains illegal access to the target network while remaining undiscovered for an extended period of time. An APT's goal is to exfiltrate or steals data, not cause a network outage, denial of service or infect systems with malware.

6. Reconnaissance's-

This attack is a sort of security attack in which an attacker collects all available information about the target before starting an actual attack. Reconnaissance attacks are used by attackers to prepare for actual attacks.

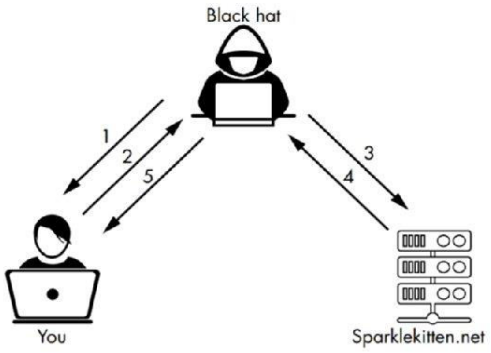

Figure 4: Flow of Reconnaissance's.

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

The most common form of this attack is scanning networks for vulnerabilities, such as email messages, websites, social media sites, messaging applications& a company's internal network, in order to gain access to systems & computers software or security systems.

III. PENETRATION TESTING

Penetration testing is used as a proactive measure to detect vulnerabilities in services & organizations before other attackers do.

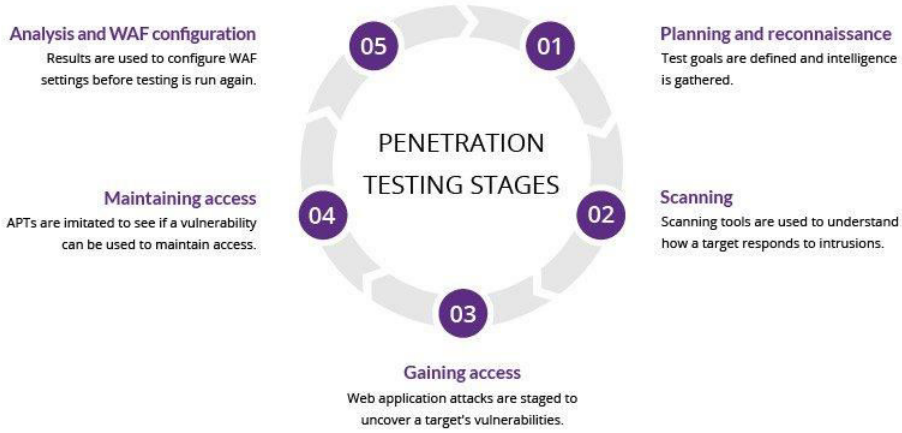

Figure 5: Stages of Penetration Testing.

A security exercise in which a cyber-security professional seeks to locate and exploit vulnerabilities in a computer system. The goal of this simulated attack is to identify any weakness in a system's defences that attackers could exploit.

IV. EMERGING ADVANCED PREVENTIVE AND SAFETY METHODS IN CYBER SECURITY

1. **Firewalls-**
Firewalls protect your website or web application by monitoring network traffic & blocking potentially harmful connections.

2. **User Account Control (UAC)-**
This built-in security feature on windows systems distinguishes between the capabilities of an administrator user &a normal user.

3. **Software updates-**
Updating software and systems with the most recent security with the most recent security patches and upgrades can help reduce vulnerabilities and prevent cyber-attacks.

4. **Backup strategy-**
A backup and recovery plan can help you secure your data and avoid paying a ransom.

5. Multiple-factor authentication (MFA)-
MFA provides two pieces of evidence when logging into an account, such as six-digit security codes or one-time passwords, to prevent hackers from accessing the app.

6. **Antivirus software-**
Installing antivirus software can dramatically minimize the chances of a virus entering your computer.

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

To further protect your accounts, use unique & unpredictable passwords for each. Be cautious when using third-party computers. Use HTTPS instead of HTTP while browsing.

V. CONCLUSION

The aim of this paper is to gain a fundamental grasp of the function of cyber-security in the global context, the types of attacks that cyber-security includes, and the numerous methods, strategies, preventive & safety measures used to manage cybercriminals attacks. This research also demonstrates that while we cannot control cyber-attacks, we may take steps to mitigate them. So, stay cautious, safe, and vigilant to such scams.

REFERENCES

1. Hua, T. K., & Biruk, V. (2021). Cybersecurity as a Fishing Game: Developing Cybersecurity in the Form of Fishing Game and What Top Management Should Understand. Partridge Publishing Singapore.
2. Ravi Sharma, Study of Latest Emerging Trends on Cyber Security and its challenges to Society, International Journal of Scientific & Engineering Research, Volume 3, Issue 6, June-2012 1 ISSN 2229-5518 IJSER © 2012.
3. Cisco, Cisco 2009 Annual Security Report: Highlighting Global Security Threats and Trends, December 4, 2009.
4. J. Li. The research and application of multi-firewall technology in enterprise network security. Int'l J. of Security and Its Applications, 9(5):153–162, 2015.
5. Ravi Sharma Study of Latest Emerging Trends on Cyber Security and its challenges to Society International Journal of Scientific & Engineering Research, Volume 3, Issue 6, June-2012 1ISSN 2229-5518.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi crossref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details