iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** III **Month of publication:** March 2023

DOI: https://doi.org/10.22214/ijraset.2023.49764

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 11 Issue III Mar 2023- Available at www.ijraset.com

A Review on Major Cyber Threats and Recommended Counter Measures

Shejin T R[1], Sudheer K T[2]
[1]*Lecturer in Computer Engineering, S.R.G.P.C Thriprayar, Kerala*
[2]*Lecturer in Computer Engineering, I.P.T & G.P.C Shoranur, Kerala*

Abstract: ***It was predicted that the number of cyber attacks will rise by a factor of two every year. There have been several high-profile cyber attacks on government organizations in India in recent years. Ransomware attacks, Advanced Persistent Threats, Internet of Things, Cloud security risks, Insider threats, Social engineering attacks, Supply chain attacks, Zero-day exploits in cyber threats are some of the significant types of cyber attacks affecting Indian government entities. Security measures, such as regularly backing up important data, installing antivirus software, training employees on how to identify and avoid phishing emails, and maintaining up-to-date software and operating systems are common countermeasures against significant cyber attacks. Preventing cyber attacks requires a multi-layered approach that addresses vulnerabilities in people, processes, and technology. Empowering, the agencies like CERT-In for cyber resilience, strengthening the penalty framework for non-compliance, advisories on information and data security practices are some of the strategies adopted by the government to secure cyberspace. It is necessary to stay informed about the latest threats and continually reassess and update security measures as needed.***

Keywords: Cyber attack, Ransomware, Internet of Things, Cloud Security, Advanced Persistent, Insider threats, Zero-day exploits.

I. INTRODUCTION

The increasing frequency and sophistication of cyber attacks have become a major concern for government organizations around the world, as these attacks can have serious consequences for national security and public trust. There have been several high-profile cyber attacks on government organizations in India in recent years. These attacks have targeted a range of government entities, including defense organizations, financial institutions, and critical infrastructure providers. It is important for government organizations in India to stay up-to-date on the latest cyber threats and adopt a proactive approach to cybersecurity to stay ahead of potential attackers. India is expected to see 1.16 million cyber breaches in 2020, a threefold increase over 2019 [1]. “Around 14.02 Lakh cybersecurity incidents were reported in 2021 while 11.58 Lakh such instances were reported to CERT-In in 2020” [2]. One notable example is the 2020 cyber attack on the Indian electricity grid. Another recent example is the cyber attack on the Indian Space Research Organisation (ISRO) in 2021, which targeted employees with phishing emails and attempted to steal sensitive data related to India's space program. A cyber attack causing disruption of online services that lasted over two weeks hit on All India Institute of Medical Science (AIIMS). Five AIIMS servers were compromised during the attack and nearly 1.3 terabytes of data were encrypted by hackers as reported by India’s nodal cybersecurity agency, Computer Emergency Response Team (CERT-In).

II. METHODOLOGY

This study comprises a review of cyber attacks and major threats and challenges along with countermeasures to be taken for addressing the risks. As the number of cyber-attacks are increasing hugely on a daily basis all around the world, as well as the companies usually disclose limited information when they are the victim of cyber-crime, secondary sources for data on cyber attacks were used for the study.

III.AN OVERVIEW OF CYBER ATTACKS : TYPES AND PATTERN

1) *Ransomware Attacks:* Ransomware attacks are increasing in frequency and sophistication. The over-all cost of ransomware will go beyond $20 billion worldwide [3]. Ransomware is a type of malicious software (malware) that is designed to block access to a computer system or data until a ransom is paid to the attacker. Cyber criminals use ransomware to encrypt a victim's files and demand payment in exchange for the decryption key. The ransom amount is usually requested in cryptocurrency, which can make it difficult to trace the attacker. Ransomware attacks can be delivered via a variety of methods, including phishing emails, malvertising, and malicious downloads. They can target individuals or organizations of all sizes, and the costs of a successful attack can be significant, including financial losses, business disruptions, and reputational damage.

2) *Advanced Persistent Threats (APTs):* APTs are a type of targeted cyber attack that is designed to gain access to a network or system and remain undetected for an extended period of time. APT can be focused on large organisations and industry sectors, causing severe damage, e.g., intellectual property theft, failure of essential services, and destruction of critical infrastructure. These attacks are usually undetected, and the damage caused can be critical [4]. These attacks are typically conducted in several phases, including reconnaissance, infiltration, and data exfiltration. The attackers may use a variety of techniques, such as social engineering, spear-phishing, or exploiting vulnerabilities in software or hardware, to gain initial access to the targeted network or system. Once inside the network or system, the attackers will often move laterally to gain access to additional resources and data. The goal of an APT is often to steal sensitive information, such as trade secrets, intellectual property, or financial data, or to conduct espionage or sabotage.
3) *Internet of Things (IoT) Security Risks:* Internet of Things (IoT) are interconnected systems of devices that facilitate seamless information exchange between physical devices [5]. IoT devices are becoming increasingly common, but many lack adequate security measures, making them vulnerable to hacking and other cyber attacks. IoT is a term used to describe the network of devices, sensors, and other objects that are connected to the internet and capable of transmitting and receiving data. While the IoT has the potential to revolutionize many industries, it also presents a number of security risks, including lack of security features, Distributed denial-of-service (DDoS) attacks, data privacy risks, physical safety risks, supply chain risks, firmware vulnerabilities and lack of updates.
4) *Cloud Security Risks:* The cloud model provides three types of services: (1). Software as a Service (SaaS), (2). Platform as a Service (PaaS) & (3). Infrastructure as a Service (IaaS) [6]. As more organizations move their data and applications to the cloud, the risk of data breaches and cyber attacks on cloud infrastructure is increasing. Cloud computing has become increasingly popular in recent years, offering organizations scalability, flexibility, and cost-effectiveness. However, cloud computing also presents a number of security risks, including Data breaches, Data loss, Insider threats, Compliance, and regulatory risks, lack of visibility and control, Shared infrastructure risks, and Vendor lock-in. Cloud vendors are emerging solutions to solve privacy issues to allow companies more secure with transitioning their data to the cloud [7].
5) *Insider Threats:* Insider threats refer to cyber security risks posed by employees, contractors, and other trusted insiders who have access to sensitive information or systems. Insider threats are cyber threats that come from within an organization, and they can be intentional or unintentional. Insider threats can be carried out by employees, contractors, or other individuals who have access to the organization's systems and data. Efforts to combat and predict insider threats comprise similarities and differences in cases throughout history. While the human factor has remained somewhat constant, the methods and skills that apply to insider exploits have changed drastically in the last few decades [8]. Examples of insider threats include malicious insiders, Careless or negligent insiders, and Compromised insiders.
6) *Social Engineering Attacks:* Are a group of sophisticated cyber-security attacks which exploit the innate human nature to breach secure systems and thus have some of the highest rate of success. [9]. Social engineering attacks, such as phishing and pretexting, use deception to trick individuals into divulging sensitive information or taking actions that are harmful to an organization's security. Social engineering attacks are a type of cyber attacks that rely on manipulating individuals into divulging sensitive information, such as login credentials or personal information, or performing actions that can be exploited by the attacker. Social engineering attacks can take many forms, including:

a) *Phishing:* Purposively trick individuals into clicking on a malicious link or downloading a malicious attachment which involves sending emails or other communications that appear to be from a trusted source, such as a bank or a social media platform.
b) *Spear Phishing:* This is a more targeted form of phishing. This involves researching individuals or organizations in order to craft a more convincing email or message.
c) *Vishing:* This involves using voice calls or voicemail messages to trick individuals into divulging sensitive information or performing actions that can be exploited by the attacker.
d) *Smishing:* Often trick individuals into divulging sensitive information or downloading malicious software and which involves using text messages or SMS messages for this.
e) *Baiting:* Leaving physical media, such as a USB drive or a CD, in a public place in the hope that someone will use it, thereby inadvertently downloading malware or giving an attacker access to sensitive information. Exploiting human vulnerabilities, such as trust or curiosity, rather than relying on technical vulnerabilities in software or hardware is characteristic nature of social engineering attacks and so they are particularly effective.

7) *Supply Chain Attacks:* Supply chain attacks occur when hackers target third-party suppliers or vendors to gain access to a larger organization's network or systems. Supply chain attacks are a growing threat in the field of cyber security. These attacks target the supply chain components of an organization, including hardware, software, and firmware, and are designed to compromise the security of the entire supply chain. Supply chain attacks can take many forms, including Malware insertion, Counterfeit components, and Third-party vendor compromise. Supply chain attacks can be particularly effective because they can be difficult to detect and mitigate. They can also be used to attack multiple organizations that rely on the same supply chain components.
8) *Zero-day Exploits:* A zero-day vulnerability refers to a newly discovered vulnerability that is unknown to the affected vendor and has no security patch. These are vulnerabilities in software or hardware that are unknown to the vendor and for which no patch or fix is available. Once a vendor learns about a zero-day vulnerability, releasing a timely fix becomes vital given the risk of zero-day exploits [10]. Cyber criminals can exploit these vulnerabilities to launch attacks before the vendor is aware of the issue. Zero-day exploits can be very effective and dangerous because they can be used to attack systems that are otherwise considered to be secure. They are often used in targeted attacks against high-value targets, such as government agencies or large corporations. There are several ways in which zero-day exploits can be used to compromise systems, including Remote code execution: Denial-of-service attacks, and Privilege escalation.

IV. COUNTERMEASURES AGAINST SIGNIFICANT CYBER ATTACKS

Ransomware attacks: Preventing ransomware attacks involves implementing a variety of security measures, such as regularly backing up important data, installing antivirus software, training employees on how to identify and avoid phishing emails, and maintaining up-to-date software and operating systems.

Preventing APTs involves implementing a variety of security measures, such as network segmentation, access controls, monitoring and detection systems, and regular security assessments. It is also important to maintain up-to-date software and operating systems, train employees on how to identify and avoid social engineering attacks, and conduct regular security audits and incident response planning.

To mitigate IoT security risks, it is important to implement strong authentication and encryption mechanisms, regularly update software and firmware, and limit access to sensitive data. It is also important to conduct regular security audits and risk assessments, and to design IoT devices with security in mind from the outset.

Cloud security risks: To mitigate cloud security risks, it is important to carefully evaluate cloud service providers and select providers that meet security standards and comply with relevant regulations. Organizations should also implement strong access controls, encryption, and monitoring tools to protect their data in the cloud.

Insider threats: As insiders often have legitimate access to systems and data and may not raise suspicions, insider threats can be particularly difficult to detect and prevent. The first step in developing efficient threat detection and response processes is understanding the threats that exist in the cyber environment. “Organizations should have a committee which deals with these attacks and who are ready to take action, so that in future these attacks can be minimized”[11]. There are several measures that organizations can take to mitigate insider threats, like implementing strict access controls, employee training providing regular security training and awareness programs, implementing monitoring and auditing tools and incident response planning which outlines procedures for responding to insider threats.

Social engineering attacks: To mitigate social engineering attacks, it is important to provide regular security training and awareness programs to employees, to implement strong access controls, such as two-factor authentication, and to carefully monitor for suspicious activity. It is also important to have a response plan in place in case a social engineering attack is successful, including procedures for reporting and responding to incidents.

Supply chain attacks: To mitigate the risk of supply chain attacks, organizations should take a number of steps, including vendor selection, supply chain visibility, Incident response planning, security testing and security awareness.

Zero-day exploits: To mitigate the risk of zero-day exploits, organizations should take a number of steps, including proper updation of software and hardware, installation of intrusion detection and prevention systems, conducting regular security assessments and implementing strong access controls like the restriction of access to sensitive systems and data.

Increased dependency on IT makes military and intelligence agencies more susceptible to cyber threats globally. In India, a cybersecurity lab for officers to learn about signal and data transmission network security is established at the Military College of Telecommunications Engineering in Madhya Pradesh.

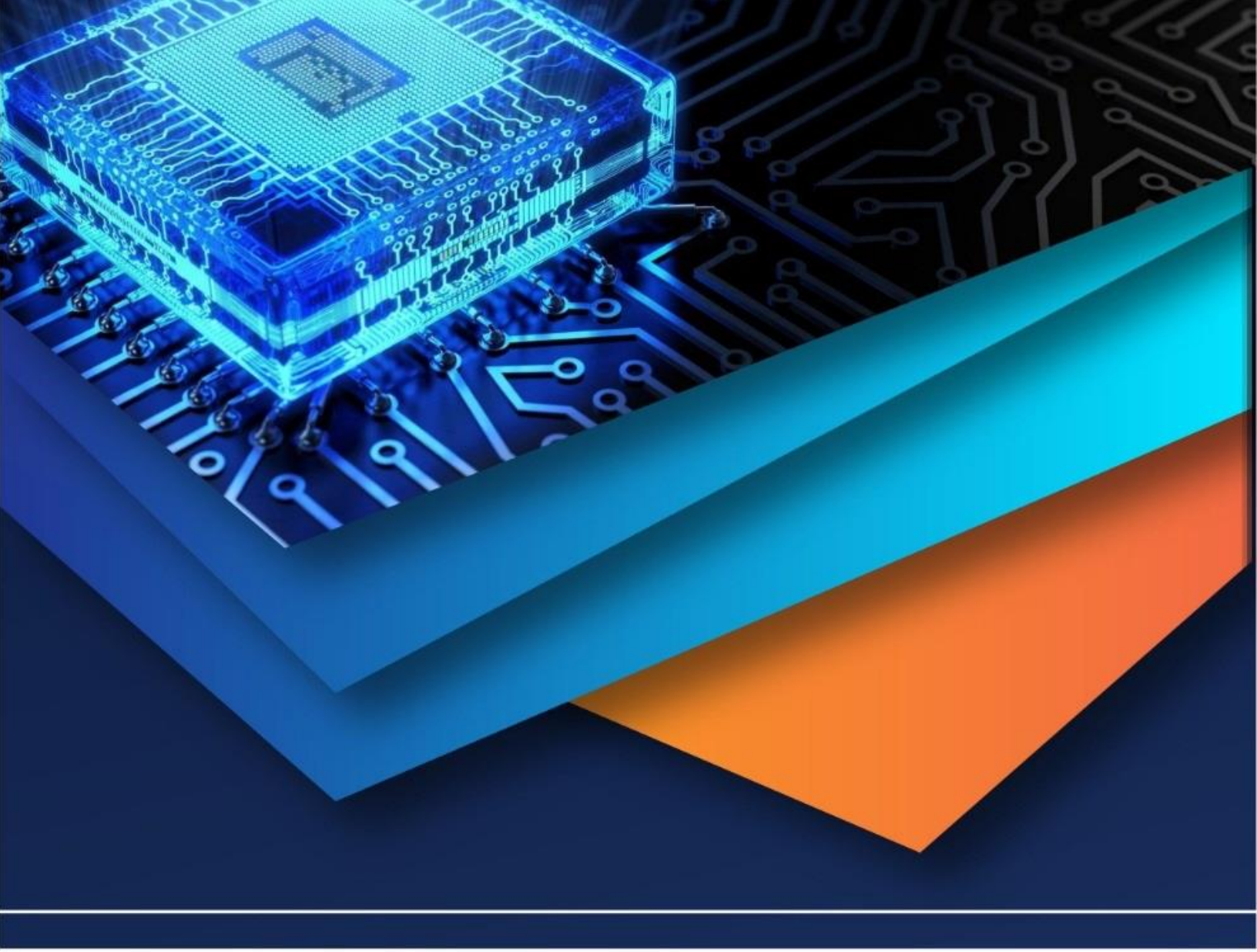
A national cybersecurity policy that prioritized infrastructure, development, and public-private partnerships (DEITY 2012) were drafted in March 2011 by our Ministry of Communications and Information Technology (MCIT). The country's critical infrastructure was to be safeguarded through the use of CERTs at the national and state levels. DRDO developed a national cyber defense system to protect network sectors. The Technical Intelligence Communication Centre and the National Defense Intelligence Agency developed a joint team to raise public awareness of cyber vulnerabilities. Our government overspent on cyber security in 2021–2022 for the first time in eight years as stated by Business Standard reports. For 2022– 2023, the government has budgeted 515 crore rupees for cyber security. Digital India Bill proposes to bring smartwatches, spy camera glasses or any other wearable devices under stringent regulation. The bill, which will replace Information Technology Act (IT Act) 2000, will mandate the consumers for these products to go through a 'strict KYC' process. The Bill also proposes ethical usage of artificial intelligence (AI)-based tools to protect the rights or choices of users. To secure cyberspace, the government is mulling to empower agencies like CERT-In for cyber resilience; strengthening the penalty framework for non-compliance, advisories on information and data security practices, etc. Indian military and intelligence agencies are more vulnerable to cyberattacks as they are increasingly reliant on IT. A cybersecurity lab for officers to learn about signal and data transmission network security is established at the Military College of Telecommunications Engineering in Madhya Pradesh. A national cybersecurity policy that prioritised infrastructure, development, and public-private partnerships (DEITY 2012) was drafted in March 2011, by India's Ministry of Communications and Information Technology (MCIT). State's critical infrastructure was to be safeguarded through the use of CERTs at the national and sectoral levels. Defense Research and Development Organization developed a national cyber defence system to protect network sectors. Project completion reached a half-way point in May 2012. The Technical Intelligence Communication Centre and the National Defense Intelligence Agency developed a joint team to raise public awareness of cyber vulnerabilities. Business Standard reports that in 2021–2022 the government overspent on cyber security for the first time in eight years. The government budgeted 515 crore rupees for cyber security for the years 2022– 2023.

V. CONCLUSION

Preventing cyber attacks requires a multi-layered approach that addresses vulnerabilities in people, processes, and technology. Here are some general steps that individuals and organizations can take to prevent cyber attacks: Regularly applying security updates and patches to software, operating systems, and network devices can help address known vulnerabilities and reduce the risk of cyber attacks. Passwords should be complex, unique, and changed regularly. Multi-factor authentication adds an extra layer of security by requiring additional verification steps beyond just a password. Anti-virus, anti-malware, and firewall software can help detect and block cyber attacks. Encrypting sensitive data can protect it from being intercepted and stolen by attackers. Regular backing up data will prevent data loss in the context of a cyber attack. Regular security assessments aids in identifying potential vulnerabilities and address them before they can be exploited. Restricting access to sensitive systems and data can limit the damage that can be caused by cyber attacks. Educating employees on how to recognize and respond to cyber threats will prevent cyber attacks from being successful. By implementing these steps, individuals and organizations can take a proactive approach to cybersecurity and reduce the risk of cyber attacks. However, it's important to note that cybersecurity is an enduring process, and it's crucial to stay informed about the latest threats and continually reassess and update security measures as needed.

REFERENCES

[1] A. A. Shairgojri, S. and A. Dar. "Emerging Cyber Security India's Concern and Threats" Int. J. Info. Tech. Computer Eng. -2022, 5290 Vol: 02, No. 04, June-July
[2] The Hindu, 2021., August 4th. https://www.thehindu.com/business/cert-in-observed-more-than-607-lakh-cyber-security-incidents-till-june-2021-government/article35726974.ece
[3] A. Sheth, S. Bhosale, F. and Kurupkar. **"**Research Paper on Robotics-New Era" Contemporary Research In India (ISSN 2231-2137): April , 2021
[4] Q. Bonilla, and M. Rey . A New Proposal on the Advanced Persistent Threat: A Survey. Applied Sciences. 2020; 10(11):3874. https://doi.org/10.3390/app10113874
[5] A. Khraisat and A. Alazab . 2021. "A critical review of intrusion detection systems in the internet of things:techniques, deployment strategy, validation strategy, attacks, public datasets and challenges" Cybersecurity (2021) 4:18 .https://doi.org/10.1186/s42400-021-00077-7
[6] K. Hashizume , D. Rosado , E. F. Medina and E. B Fernandez . 2013. An analysis of security issues for cloud computing . J. Internet Services and Applications, 4:5 http://www.jisajournal.com/content/4/1/5
[7] V. Sureshkumar and B. Baranidharan, . "A study of the cloud security attacks and threats". 2021. J. Phys.: Conf. Ser. 1964 042061
[8] Greitzer, Frank L. , Ph.D. and Hohimer, Ryan E.. "Modeling Human Behavior to Anticipate Insider Attacks." J. Strategic Security 4 (2), 2011,:25-48. DOI:http://dx.doi.org/10.5038/1944-0472.4.2.2
Available at: https://digitalcommons.usf.edu/jss/vol4/iss2/3
[9] V. Sushruth · K. R. Reddy ·and B. R. Chandavarkar. " Social Engineering Attacks During the COVID-19 Pandemic". SN Computer Science (2021) 2:78 https://doi.org/10.1007/s42979-020-00443-
[10] Y. Roumani. "Patching zero-day vulnerabilities: an empirical analysis**".** J. of Cybersecurity,2021,1–13 https://doi.org/10.1093/cybsec/tyab023



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY