INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

www.ijprems.com
editor@ijprems.com

Vol. 04, Issue 06, June 2024, pp: 415-420

e-ISSN : 2583-1062

Impact Factor: 5.725

INTRODUCTION TO CYBERSECURITY CHALLENGES AND EMERGING TRENDS ON LATEST TECHNOLOGY: A FOCUS ON SOCIAL MEDIA ATTACKS

Mithilesh D. Pakhare[1], Purva R. Shinde[2]

[1,2]Post-Graduate Student, MCA Department, Finolex Academy of Management and Technology, Ratnagiri, Maharashtra, India.

DOI: https://www.doi.org/10.58257/IJPREMS34766

ABSTRACT

Our reliance on technology has brought immense convenience, but also introduced significant cybersecurity challenges. This paper explores the evolving landscape of cyber threats, particularly those targeting the ever-growing realm of social media. We will delve into the common social media attacks, analyze the challenges they pose for individuals and organizations, and examine emerging trends in cybersecurity that aim to combat these threats.

Keywords: Cyber security, Cybercrime, Cyber ethics, Social media, Cloud computing, Android apps.

1. INTRODUCTION

The ever-growing reliance on technology necessitates a robust and constantly evolving field of cybersecurity. Data privacy and security remain paramount considerations for any organization. In our current digital-centric world, where virtually all information is stored in digital or cyber formats, social networking platforms offer users a perceived sense of security as they engage with friends and family. However, cyber-criminals persistently target social media sites, especially given the escalating adoption of these platforms among individuals. This trend not only increases the threat of attack but also underscores the importance of implementing robust security measures, particularly during sensitive activities like bank transactions.

The prevalence of social media among individuals amplifies the risk of cyber-attacks. As these platforms are integral to daily life for many users, they have become lucrative targets for cybercriminals seeking to exploit personal information and pilfer valuable data. The review paper examines the current challenges faced by cybersecurity professionals in the context of the latest technological advancements. We delve into the growing sophistication of cybercrime, the ethical considerations surrounding data privacy, and the unique vulnerabilities introduced by social media platforms, cloud computing and the proliferation of Android applications.

By analysing these key areas, this paper aims to:

- Identify the most pressing cybersecurity challenges associated with social media, cloud computing, and Android apps.
- Explore the emerging trends in cybercrime tactics and how they exploit these new technologies.
- Discuss the ethical considerations surrounding data collection, storage and access within these evolving technological landscapes.
- Analyse the latest advancements in cybersecurity solutions and their effectiveness in mitigating these emerging threats.

The review paper will utilise existing research and industry reports to provide a comprehensive overview of the current state of cybersecurity in relation to these specific technologies. It aims to inform researchers, developers and the users alike about the critical need for continuous vigilance and adaptation in the face of a constantly evolving threat landscape.

The review paper will work and dive deep in understanding various cyber security techniques to avoid such attacks or the preventive measures in order to adapt the vast growing digital world of technology and be secure too. Some of the main techniques that the review paper will cover are as follows:

- Access Control & Password Security.
- Authentication of Data.
- Malware Scanners.
- Firewalls.
- Anti-virus software

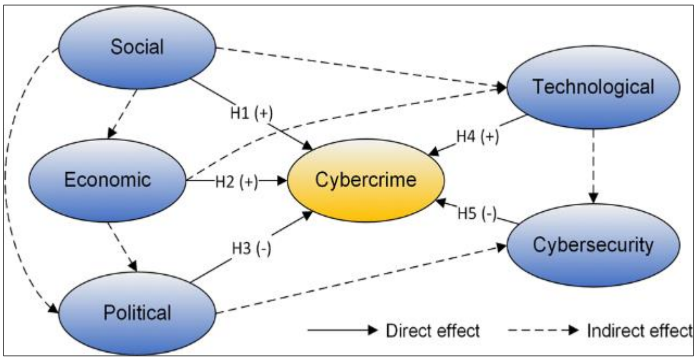

Figure 1 : The Impact of Cybercrime on Society

2. METHODOLOGY

Research Design :

This paper employs a qualitative research design, synthesizing a wide range of existing literature, industry reports, and case studies to explore the evolving landscape of cybersecurity. The focus is on social media, cloud computing, and Android applications, aiming to offer a thorough understanding of current cybersecurity challenges, emerging trends, ethical, considerations, and technological advancements in these areas.

2.1 The Evolving Landscape of Cybersecurity :

The digital age has revolutionized communication, commerce, and information access. However, this interconnectedness has created fertile ground for cybercriminals. Cyberattacks are on the rise, targeting both individuals and organizations. These attacks aim to steal sensitive data, disrupt operations, or extort money. The cost of cybercrime is staggering, with estimates reaching trillions of dollars annually [1].

The rise of new technologies further complicates the cybersecurity landscape. The Internet of Things (IoT), cloud computing, and artificial intelligence (AI) introduce novel vulnerabilities that attackers can exploit.

2.2 Social Media :

Social media platforms have evolved into essential components of contemporary existence. However, this popularity makes them a prime target for cyberattacks. Here's why:

User Trust: Users often trust the information they see on social media, making them susceptible to phishing attacks and social engineering tactics.

Data Sharing: Social media platforms hold a wealth of personal data, making them attractive targets for data breaches.

Platform Vulnerabilities: Social media platforms are complex systems, and vulnerabilities can be exploited to spread malware or gain unauthorized access

2.3 Common Social Media Attacks :

Social media attackers employ various methods to achieve their goals. We will delve into some of the most widespread methods :

Phishing Attacks: These attacks use deceptive emails, messages, or fake profiles to trick users into revealing sensitive information or clicking on malicious links.

Social Engineering: Attackers manipulate users' emotions or trust to gain access to their accounts or personal information.

Malware Propagation: Social media platforms can be used to spread malware through infected links or attachments disguised as legitimate content.

Account Takeovers (ATOs): Attackers gain control of a user's social media account to spread misinformation, launch further attacks, or damage the user's reputation.

Deepfakes and Disinformation: Deepfakes - manipulated videos or audio - are used to spread false information or create chaos on social media.

2.4 Challenges Posed by Social Media Attacks :

Social media attacks pose a significant threat to both individuals and organizations:

Individual Risks: Data breaches can expose personal information, leading to identity theft, financial loss, and reputational damage. Malware can compromise devices or steal sensitive data.

Organizational Risks: Social media attacks can disrupt operations, damage brand reputation, and lead to data breaches of sensitive information. Disinformation campaigns can undermine trust in organizations.

2.5 Emerging Trends in Cybersecurity :

The fight against cybercrime is a continuous battle. Here are some emerging trends in cybersecurity that address the challenges posed by social media attacks:

Machine Learning (ML) for Threat Detection: Machine learning algorithms can analyse vast amounts of data to identify and prevent social engineering attacks and malware dissemination on social media platforms.

User Education and Awareness: Empowering users with knowledge about social media threats and best practices is crucial for mitigating risks. Security awareness training can help users identify and avoid social engineering tactics.

User Education and Awareness: Empowering users with knowledge about social media threats and best practices is crucial for mitigating risks. Security awareness training can help users identify and avoid social engineering tactics.

Biometric Authentication: Fingerprint or facial recognition technology can strengthen account security and prevent unauthorized access.

Social Media Platform Security Enhancements: Social media platforms are constantly improving their security measures with features like suspicious login alerts, content moderation tools, and improved reporting mechanisms.

3. CYBERSECURITY STRATEGIES

The realm of cyberspace faces escalating threats as cybercriminals exploit novel techniques. These individuals frequently adapt malware signatures and exploit emerging technological vulnerabilities to perpetrate cyber-attacks. Leveraging the expansive user base of emerging internet technologies, cybercriminals target millions of active users with relative ease and efficiency.

3.1 User Authentication and Password Management:

User Authentication and Password Management: User authentication through usernames and passwords stands as a fundamental pillar in safeguarding private information and upholding privacy standards. It remains among the most crucial cybersecurity measures.

3.2 Data Verification and Authentication:

Data Verification and Authentication: Ensuring the authenticity of transmitted information is imperative. Documents must be verified to confirm their origin from a trusted source and ascertain that they remain unaltered. This verification process often involves the utilization of robust antivirus software, which is indispensable in protecting devices from malicious threats.

3.3 Malware Scanners :

Malware Scanners : A software system which sometimes scans all files and documents for malicious code or harmful viruses inside the system.

In this domain, malicious software systems are typically identified and categorized as malware, encompassing viruses, worms, and Trojan horses[4].

3.4 Firewall :

Firewall is a software or hardware package which helps separate hackers, viruses and worms trying to access your PC through the web. The firewall examines every incoming message and filters out those that do not meet the specified security criteria, thereby playing a crucial role in detecting malware[4].

3.5 Role of social media in Cyber Security :

Role of social media in Cyber Security: In recent modern world, there is a need of interactive businesses which needs to find new ways to secure personal information in more entangled environment. Social media plays a crucial role in both cybersecurity and personal cyber-attacks.

The uptake of social media among employees is on the rise, consequently heightening the risk of attacks. Given that the majority of employees now utilize social media or social networking sites on a daily basis, the vulnerability to cyber threats has escalated accordingly.

In the contemporary landscape, the sharing of personal information has become exceedingly effortless, raising the imperative for businesses to swiftly identify, promptly respond, and proactively avert any form of breaches.These social media has easily make people to share their private information and hackers can use these information. Therefore, people have to take reasonable steps to avoid misuse and loss of their information through these social media [2].

4. CURRNRT SURVEY CONCERNS REGARDING CYBERSECURITY TRENDS

Cybersecurity encompasses the awareness surrounding diverse cyber threats and the deployment of defensive strategies (i.e., countermeasures) to uphold the confidentiality, integrity, and availability of digital or IT infrastructures.[5]

Many experts in cybersecurity view malware as the primary weapon used by malicious actors to breach cyber protection measures. Malware encompasses a broad category of attacks that target devices, typically without the user's knowledge. This category includes viruses, worms, Trojan horses, spyware, and bot executables, among others. Malware infiltrates computers through various means, such as spreading from infected devices, tricking users into opening compromised files, or luring users to visit websites hosting malware. In more concrete scenarios, malware can self-propagate by loading onto a USB drive inserted into an infected computer and subsequently infecting any device it connects to. Malware can infiltrate devices and equipment at any stage of their lifecycle, posing threats to end-users, servers, network devices like routers and switches, and even critical systems like SCADA (Supervisory Control and Data Acquisition). The proliferation and increasing complexity of malware represent significant concerns in today's digital landscape.

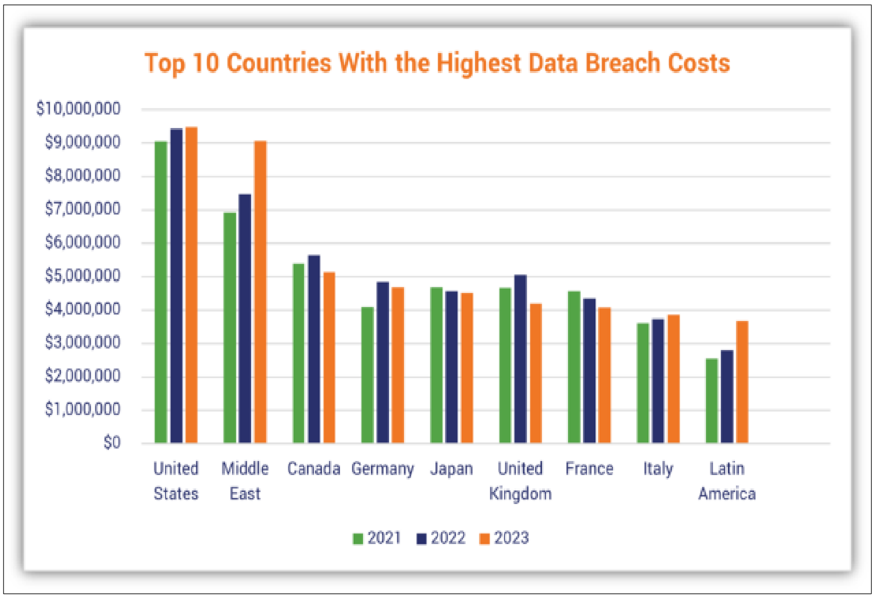

Figure 2 : Top 10 Countries With the Highest Data Brach Coats.

4.1 Deceptive Attacks :

As per the most recent data breach analysis by Verizon, approximately 32% of confirmed data breaches can be attributed to deceptive practices. The objective of these attacks is to acquire sensitive information, including usernames, passwords, social security numbers, and credit card details, by deceiving victims into believing they are interacting with a trustworthy entity. This deception can occur through various mediums such as email, text messages, and increasingly, phone calls.

4.2 IoT Extortion :

The realm of Internet of Things (IoT) encompasses numerous interconnected devices, ranging from household appliances to service sensors, all linked to a network. While devices like climate control systems and refrigerators may not inherently store confidential data, they can still be targeted by cybercriminals who hold them hostage through ransomware attacks. These attackers exploit vulnerabilities in backend systems, such as power supplies and communication networks, to gain unauthorized access and extort valuable information.

4.3 Increased Data Privacy Regulation :

The General Data Protection Regulations for Europe(GDPR) was introduced in May 2018 to strengthen European citizens' rights of data privacy and to implement compliance with more rigorous global regulations or severe financial penalties for non-compliance.

4.4 Mobile Device Cyber Attacks :

Recent findings from RSA research indicate a substantial surge in fraudulent mobile transactions, with an increase of up to 80% since 2015. As mobile devices have become integral to both personal and professional spheres, their pervasive use has led to heightened risk perceptions regarding cyber threats.

4.5 Increased Investment in Automation[3] :

Automation technology is gaining ground in organisations by allowing underemployed cyber security teams to focus on more complex problems, not on routine, often worldly work. According to a recent Ponemon Institute survey, 79% of respondents use security automation tools and frameworks and 50% expect to use security automation in their businesses. In these situations, the first approach to data protection provides an ultimate defense against Cyber-attacks such as database fraud and fitness, and its profound effect on business. While automation can indeed improve efficiency, it's important to note that expertise and skill remain essential in mitigating cyber security risks effective.

Strengthening Application and Data Protection in Production Environments: Production centers are enhancing their security measures to safeguard both applications and data from cyber-attacks, recognizing the critical importance of protecting these assets.

Ultimately, combating cybercrime requires a multifaceted approach that encompasses technological advancements, skill development, organizational restructuring, and global cooperation, complemented by legislative measures to address emerging threats effectively.

5. CYBERSECURITY STRATEGIES

5.1 User Access Management and Password Security the traditional method of utilizing usernames and passwords has long been a cornerstone of safeguarding sensitive information. This foundational approach remains a primary component of cybersecurity measures.

5.2 Data Authentication it is imperative to verify the authenticity of documents before downloading them, ensuring they originate from reputable and unaltered sources. Typically, this authentication process is facilitated by antivirus software installed on devices. Therefore, employing reliable antivirus software is crucial for protecting devices against viruses and malicious content.

5.3 Malware scanners This is software that usually scans all the files and documents present in the system for malicious code or harmful viruses. Viruses, worms, and Trojan horses represent just a few instances of malicious software, commonly categorized collectively under the term "malware”.

5.4 Firewalls A firewall is a software program or piece of hardware that helps screen out hackers, viruses, and worms that try to reach your computer over the Internet. Every communication transmitted to or from the internet undergoes scrutiny by the firewall in place, evaluating each message against predefined security standards. Consequently, firewalls assume a critical function in identifying and intercepting malware, blocking any messages that fail to adhere to the specified security parameters.

5.5 Anti-virus software Antivirus software is a computer program that detects, prevents, and takes action to disarm or remove malicious software programs, such as viruses and worms. Most antivirus programs include an auto-update feature that enables the program to download profiles of new viruses so that it can check for the new viruses as soon as they are discovered. Utilizing antivirus software is essential and imperative for the security of every system.

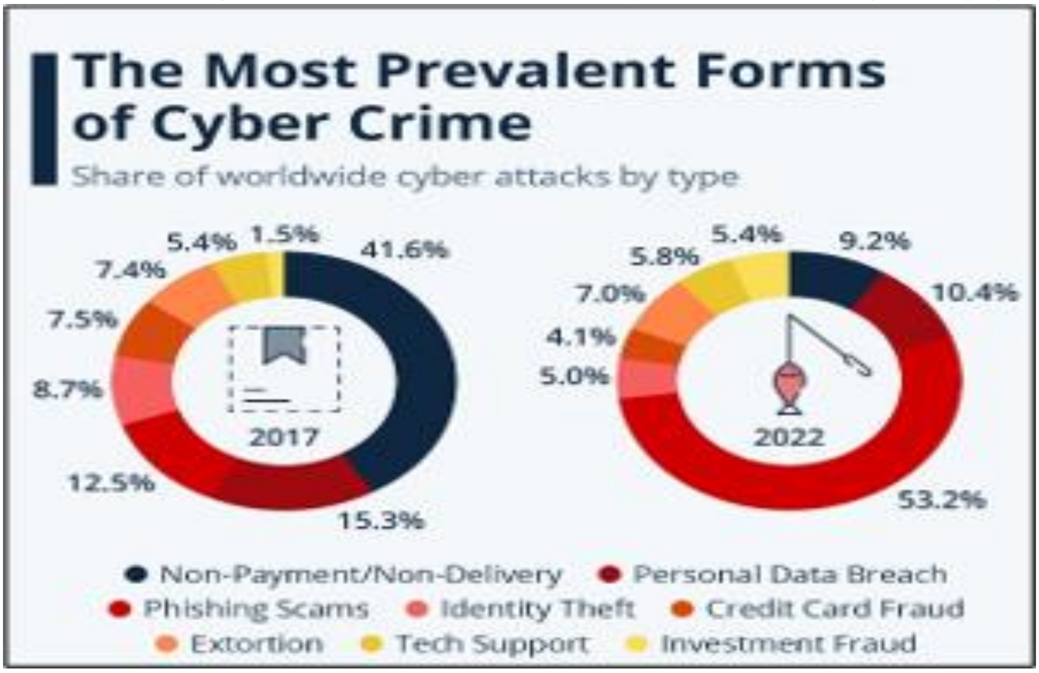

Figure 3 : The Most Prevalent Forms of Cyber Crime

6. CONCLUSION

Cybersecurity challenges will continue to evolve alongside technology. While social media attacks pose significant risks, the field of cybersecurity is actively developing solutions. By staying informed about social media threats, adopting secure practices, and embracing emerging technologies, individuals and organizations can better defend themselves in the digital landscape.

Further Research : This paper provides a foundational understanding of cybersecurity challenges and social media attacks. For further exploration, consider researching specific types of social media attacks, technical details of cyber defence strategies, and the legal implications of cybercrime.

7. REFERENCES

[1] Ravi Sharma Study of Latest Emerging Trends on Cyber Security and its challenges to Society International Journal of Scientific and Engineering Research, Volume 3, Issue 6,June-2012 1ISSN 2229-5518.

[2] Lee, H.Lee, Y.Lee, K.Yim, K. Assessment of Mouse Data Integrity Using Mouse Loggers. Presented at the International Symposium on Broadband and Wireless Computing, Communication, and Applications, Asan, South Korea, 5–7 November 2016.

[3] Mellado, D.; Mouratidis, H.; Fernández-Medina, E. Development of a Secure Tropos Framework for Requirements Engineering in Software Products Lines. Computer Standards & Interface 2014, 36, 711-722.

[4] Mohsin, M.; Anwar, Z.; Zaman, F.; Al-Shaer, E. IoT Checker: A data-driven framework for security analytics of Internet of Things configurations. Computer Security 2017, 70, 199–223.

[5] Veenoo Upadhyay, Suryakant Yadav Study of Cyber Security Challenges Its Emerging Trends: Current Technologies International Journal of Engineering Research and Management (IJERM) ISSN: 2349- 2058, Volume-05, Issue-07, July 2018.