IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 25, Issue 5, Ser. 1 (Sept. – October. 2023), PP 42-46
www.iosrjournals.org

Current Trends In Cyber Security

Dr. Rupali Pawar,
Assistant Professor,
Zeal Institute of Business Administration, Computer Application & Research, Narhe Pune-41
Miss. Chirayu Kulkurni,
Student,
Zeal Institute of Business Administration, Computer Application & Research, Narhe Pune-41

Abstract:
This paper focuses on basic types of cyber security and provides solutions and precautions for current cyber threats. The Current world walks hand in hand with Technology and network connections and Cyber Security helps us to work with it effectively and securely. Important data files will get used in the wrong way by hackers if we don't provide security to it. Cyber Security is essential not only in government and military areas but also in IT sectors, private companies, banks and in your day today life. An important data like it can be sensitive information, personal information, financial details can get illegal access without Cyber security. Currently in cyber security the trending topics are Automotive Hacking, Mobile is new target, Insider Threats, Remote Working.
This paper only used secondary data. The data is collected from different research papers, books, websites articles, government reports regarding cyber security.
Keywords: *Cyber Security, Information, IT, Cyber Crime, Internet*

Date of Submission: 16-09-2023 Date of Acceptance: 26-09-2023

I. INTRODUCTION

Nowadays technology advancements have rendered man totally dependent on the internet, which has an impact on both us as individuals and as a society. People may now easily reach anything while remaining stationary thanks to this. Everything you may imagine is possible with the use of the Internet, including social networking, online shopping, data storage, gaming, online education, and employment chances. It is used and consumed in many conceivable ways. The notion of cybercrimes grew together with the development of the web and its attendant benefits. When the Internet was initially developed, its creators had no clue that it may be abused for nefarious purposes. [8]

According to research, more than 50% of online users fall victim to cybercrime every year, which includes identity theft, credit card fraud, phishing, spyware, and computer infections.

India has seen a 60% annual increase in crime, with 3500 cases reported in 2012 compared to 2070 cases in 2011. According to a study from the National Crime Records Bureau (NCRS), crimes committed by people between the ages of 18 and 30 were reported in 561 instances in Maharashtra, 454 incidents in Andhra, and 437 cases in Karnataka in 2012 [6]. In Haryana, 116 instances were reported in 2012, a sharp increase from the 3 cases reported in 2011. In contrast to other crimes, this cybercrime may be carried out anywhere and doesn't involve any expenditure.

Cyber Security:

Cyber security is the protection of internet-connected systems such as hardware, software and data from cyber threats. The practice is used by individuals and enterprises to protect against unauthorized access to data centers and other computerized systems.

Cyber Crime:

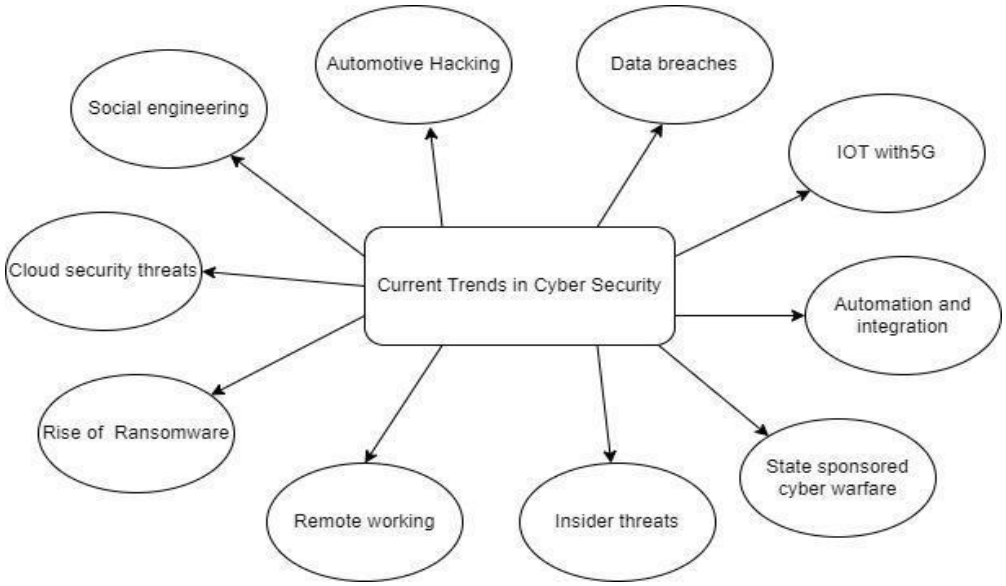
Cybercrime is criminal activity that either targets or uses a computer, a computer network or a networked device. Most cybercrime is committed by cybercriminals or hackers who want to make money. However, occasionally cybercrime aims to damage computers or networks for reasons other than profit.

Types of Cyber Crime:
Two Mail Targeting computers
Types of Cyber Crimes

This type of cybercrimes includes every possible way that can lead to harm to computer devices for example malware or denial of service attacks.

Using computers
This type includes the usage of computers to do all the classifications of computer crimes.
Current Trends in Cyber Security:

1. Automotive Hacking
2. Data Breaches
3. IOT with 5G
4. Automation and Integration
5. State-Sponsored cyber warfare
6. Insider Threats
7. Remote Working
8. Rise of Ransomware
9. Cloud Security threats
10. Social engineering



1) Automotive hacking: Automotive hacking refers to the practice of manipulating vehicles using technology. Automotive hackers access data and systems to either control the vehicle or steal information and blackmail manufacturers.

There are multiple ways for hacker to get access to Automotive hacking

- Tricking the car's sensors
- Access the cloud / Internet
- Wireless networks

2) Data Breaches: A data breach is a security violation or incident that leads to the theft of sensitive or critical data or its exposure to an unauthorized party. These incidents can be intentional, such as a database hack, or accidental, such as an employee emailing confidential files to the wrong recipient

3) IOT with 5G: The fact that 5G can handle a huge number of linked devices, including Internet of Things (IoT) devices, is one of the technology's key advantages. However, as the number of linked devices grows, so does the chance of cyberattacks on those devices. IoT devices are frequently not adequately secured, leaving them open to hackers. IoT device vulnerabilities may be used by cybercriminals to get into networks and conduct attacks
***(have to recheck this point)**

4) Automation and Integration: It involves integrating multiple technologies that can detect, prevent, contain, and recover from cyber-attacks. Cyber security automation uses both hardware-based solutions (e.g., sensors) that monitor physical systems and software-based solutions that automate tasks using machine learning techniques.

5)State-Sponsored cyber warfare: State sponsored cyber warfare is something that happens all the time, and there are quite a lot of people who are caught in the crossfire. State sponsored hacking and state sponsored cyber-attacks affect targeted countries and their people in many ways including loss of privacy, data theft, weakened national security, and infrastructure shutdown.

6) Insider Threats: It includes corruption, espionage, degradation of resources, sabotage, terrorism, and unauthorized information disclosure. It can also be a starting point for cyber criminals to launch malware or ransomware attacks. Insider threats are increasingly costly for organizations.

7) Remote Working: Remote work security is the branch of cybersecurity specifically concerned with protecting corporate data and other assets when people do their jobs outside of a physical office. Employees who work remotely require remote work cybersecurity due to a variety of scenarios, such as when they work from home, travel for business, or when they do their jobs in any location outside of the company's offices.

8) Rise of Ransomware: Ransomware is a type of malware that prevents users from accessing their system or personal files and demands ransom payment in order to regain access. While some people might think that a virus has locked their computer, ransomware is a different form of malware than a virus.

9) Cloud Security threats: The high volume of data flowing between organizations and cloud service providers generates opportunities for accidental and malicious leaks of sensitive data to untrusted 3rd parties. Human error, insider threats, malware, weak credentials and criminal activity contribute to most cloud service data breaches. Malicious actors, including state-sponsored hackers, seek to exploit cloud service security vulnerabilities to exfiltrate data from the victim organization's network for profit or other illicit purposes

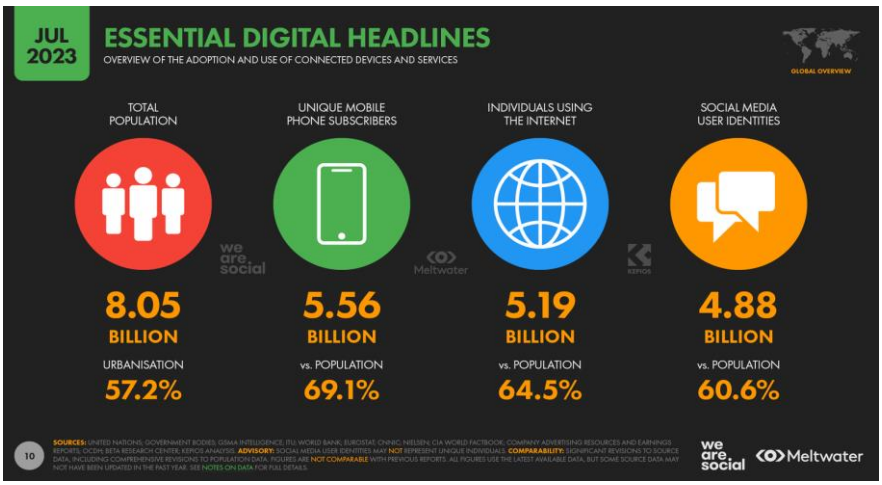
10) Social engineering: Social engineering is the tactic of manipulating, influencing, or deceiving a victim in order to gain control over a computer system, or to steal personal and financial information. It uses psychological manipulation to trick users into making security mistakes or giving away sensitive information.

Why is Cyber Crime more nowadays?

The world is now more connected through the internet. Cybercrime is a criminal activity that targets individuals or electronic devices, networks, or data centers. Cybercrimes are committed by both individuals and threat groups There are five prevalent tendencies that increase the likelihood of cybercrime.

More use of internet

Nowadays, internet users are increasing. Based on a report of Essential Digital Headlines, 64.5% people are now using the internet and 60.6% social media user identities worldwide. According to current trends, two-thirds of the world's population should be online within the next 12 months.



Global Overview of Use of internet [5]

More online transactions

India's digital payment system is a promising success story in the making, driven by recent regulatory measures and technology advancements. The use of digital payments in the nation has significantly increased during the past few decades. The accessibility of a range of simple and practical digital payment options has improved financial inclusion, boosted business and economic growth, and made life easier for individuals.

Less awareness about cyber security

People who have not received proper training and are non-educated may move towards dangerous cybercrimes. Security awareness training encourages an organizational culture that is centered on increased security while also aiding in stopping threat actors in their tracks.

Strong viruses, spywares and malicious software

Current antivirus software's protects electronic devices from more than just viruses. Nowadays viruses are becoming stronger as compared to antivirus software. It is one of the reasons for increasing cybercrime cases.

Advanced technologies and hackers

Hackers using more advanced technology and organized cybercrime are becoming prevalent. For instance, a hacker may be paid to install malware on an end user's device. Modern malware is hard to track down and steals data to make money. Some individuals believe that becoming hackers will earn them more money than working as security personnel.

II. SOLUTION:

Cyber intelligence and cyber platform are one of the upcoming solutions for a cyber crime

There is a need to increase the likelihood of arrest and conviction. To persuade the judiciary, India has evidence laws that assess admissibility, legitimacy, correctness, and completeness.[9]

The ICSS security testing team has safeguarded apps and networks in industries ranging from manufacturing to banking. Our experts' penetration testing and vulnerability analysis strives to understand the organization's security posture and assesses vulnerabilities based on their criticality.

ICSS training and development offers courses in Cyber Security (Ethical Hacking), IoT, Cloud Computing (AWS/Azure), Machine Learning, Python Programming, CCNA (networking), Block Chain, and other emerging technologies where cyber security is critical.[10]

III. CONCLUSION:

The digital world transformed our life through a changed way of communication, organizing information and shopping habits etc. In today's digital world, securing our data is more challenging.

In this research paper we have covered types of cyber security, why it is essential and the precautions for cybercrimes. We have also tried to solve the problem of cyber threats.

More Research are required in categorized cybercrimes as well as more research is needed in solution-based research on cyber security

In the future, cybersecurity firms will need to devise ways to make crucial components of infrastructure, such as those that would be attractive targets in a cyberwar, more resistant to digital incursions. Multiple levels of protection could be added to traffic systems, airport management networks, and hospital databases as part of this study.[11]

In the future, cybersecurity companies will have to devise ways to make crucial components of infrastructure, such as those that would be attractive targets in a cyberwar, more impervious to digital assaults. This work could entail adding many levels of protection to traffic systems, airport management networks, and hospital databases [11].

References

[1]. Deborah Golden And Irfan Saif, ―The Future Of Cyber Survey 2019‖, Deloitte, 2019, Https://Www2.Deloitte.Com/Us/En/Pages/Advis Ory/Articles/ Future-Of-Cyber-Survey.Html Https://Www2.Deloitte.Com/Content/ Dam/Deloitte/Covid19 2.
[2]. Https://Www.Rbi.Org.In/Scripts/BS_Pressrele Asedisplay. 3. Http://Www.Compitjournal.Org/Paper/348/Aliterature-Review-On-Cyber-Securityin-Indiancontext
[3]. Simi. Bajaj, 'Cyber Fraud: A Digital Crime, 'Www.Academia.Edu/Cyber_Fraud_A_Digital_ Crime
[4]. Www.Researchgate.Net
[5]. Https://Datareportal.Com/Global-Digital-Overview
[6]. Puja Gupta And Rakesh Kumar, "Security Risk Management With Networked Information System: A Review " 4 (2) IJEE193– 197 (2012).
[7]. Veenooupadhyay, Dr.Suryakantyadav, "Study Of Cyber Security Challenges Its Emerging Trends: Current Technologies" 5 IJERM 2349-2058 (2018).
[8]. ADITI SINGH, A Study On Emerging Issues Of Cyber Attacks & Security: In India

Http://Ijariie.Com/Adminuploadpdf/A_Study_On_Emerging_Issues_Of_Cyber_Attacks___Security__In_India_Ijariie13501.Pdf
[9]. Shri Talwant Singh , CYBER LAW & INFORMATION TECHNOLOGY (Indiancybersecurity.Com)
[10]. Indian Cyber Security Solutions (ICSS)
[11]. Https://Www.Cybersecurityintelligence.Com/Indian-Cyber-Security-Solutions-Icss-9491.Html
[12]. Https://Www.Techradar.Com/News/What-Is-The-Future-Of-Cybersecurity
[13]. Sheth, Mrs & Bhosale, Sachin & Kurupkar, Mr & Prof, Asst. (2021). Research Paper On Cyber Security. 2021. Https://Www.Researchgate.Net/Publication/352477690_Research_Paper_On_Cyber_Security
[14]. H. Geldiyev, M. Churiyev, R. Mahmudov, Issues Regarding Cybersecurity In The Modern World, Springer Fachmedien Wiesbaden Gmbh, Part Of Springer Nature 2020 H.-C. Brauweiler Et Al. (Hrsg.), Digitalization And Industry 4.0: Economic And Societal Development, Https://Doi.Org/10.1007/978-3-658-27110-7_1
[15]. Honeycutt, J. (2002). Microsoft Windows XP Registry Guide. (1 Ed.). Microsoft Press.