Cyber Security: Cyber Fundamentals and Cyber Crime Impact in 21 century

Yashvi , Amity university Haryana
Ms. Juhi Singh, Assistant Professor, Department of computer science and engineering,
Amity university Haryana

Abstract

The objective of this paper is to provide people with the basic information about the cyber terms as most of the work is online and knowing basic fundamentals is important .also looking into the cybercrimes that are happening in the digital world .Through this paper, one can understand the importance of security , how it can be carried and how one can keep themselves cyber safe.

Keywords: factors of cyber security, structure of cyber security,*cyber terrorism, cyber crime*

Introduction

In this age of rapid technological advancement, the world faces numerous challenges in combating the phenomenon of cyber threats, particularly cybercrime and cyberterrorism as new types of topsy-turvy dangers in the twenty-first century[1].To shield security frameworks from arising dangers, for example, digital psychological oppression and cybercrime, suitable exercises should be embraced, essentially on a public rather than provincial scale. Security from cybercrime and cyberterrorism is identified with assurance in all circles that have resources with those exercises. The justification for the development of such dangers is technological advancements. Furthermore, the general public is concerned that the internet provides opportunities for illegal activity that is not thoroughly examined. As a result, it is also necessary to change our laws in order to combat cybercrime and give basic information about technology to the users.

.

1.The main factors in cyber security :

Confidentiality: (Information is private) Confidentiality means preventing information from falling into the hands of people who do not have authorization to access the information.

Integrity:(Information has not been altered) Integrity means making sure the information stays accurate and consistent, and ensuring that unauthorized people cannot makes any changes to the information.

Availability :(Information can be accessed when required) Availability means timely and reliable access to and use of the information when required**.**

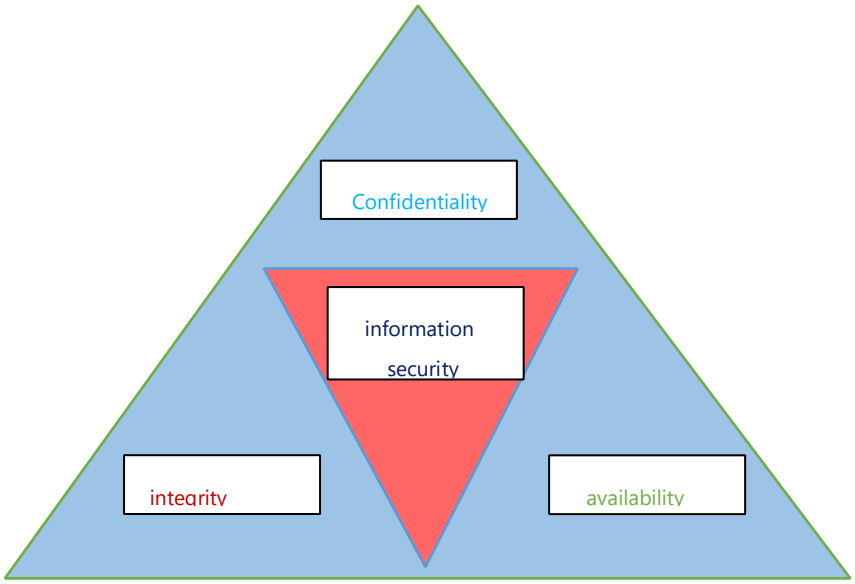

Fig :3.1 CIA model

2.Structure of cyber security

The Kill chain technique is depicted by the US Department of Defense to attack an objective , where they have defined the Kill Chainwith a few phases, for example, find, fix, track, target, draw in and assess. The Kill Chain has been applied in different regions including Cyber Security. In network protection, it is utilized to describesome assault ventures inside a counter measure system. There search has driven the Kill Chain to have seven stages of attack, which can be depicted beneath as[3]:

Surveillance: During this stage, the aggressor assembles data about the objective. This can be accomplished through examining advanced servers, talking with individuals near the objective, or simply perusing the news!

Weaponization: Once a particular weakness has been recognized, a piece of malware is intended to take advantage of it. This cycle can go from downloading an example of an information base, buying an apparatus from an outsider, or creating something custom.

Conveyance: The picked malware should be shipped off the objective in some way. Notwithstanding progress throughout the long term, the most widely recognized technique is still by means of email. Different techniques can incorporate site downloads and tainted or altered USB gadgets.

Abuse: Once malware is given to the objective, it enacts and plays out a progression of educated advances. How this happens is profoundly factor and relies upon many insights concerning the projects and working framework being used. This interaction is known as "taking advantage of a weakness" and the product used to do it is known as take advantage of code or an adventure.

Establishment: The malware endeavors to get some component of ingenuity inside the objective framework. This can be accomplished through the production of secondary passages, which can incorporate making new records, introducing

remote access programs, or bringing new weaknesses into the framework. These variables imply that assuming the first weakness is fixed, it is past the point of no return for the protector as the assailant's entrance remains.

Order and Control (C2): A strategy for the assailant to speak with the compromised frameworks should be set up. This empowers directions and moves up to be shipped off the objective and for information to be sent back to the assailant. This should be possible utilizing sites, direct associations, and even Twitter.

Activities on Objectives: Once every one of the past advances have been finished, the assailant is allowed to finish the first aim. This could go from taking information, adjusting information, or annihilating key framework components.

3.Cyber crime

Cyber-crime can be defined as the crimes committed by criminals using computers or networks, i.e., all illegal activities are done via the internet.
Cybercrime can be either cybercrime or cyber-related crime. The difference between them is ,cybercrime and cyber-related crime are divided into the following parts[4]

- **cyber crime:cyber crime has the following types:**
  → Cyber-specific means the crime is completely done by using the internet .Cyber-specific consists of the following types:
  Cyber piracy: piracy is a crime in cyberspace where one can find all the paid software, movies, series, etc. for free. According to Indian government policy, piracy is a criminal offense, and under the Cinematography Act of 2019 [5,] anyone found guilty must pay a ten lakh rupee fine and serve three years in prison. For instance, torrent

  → Cyber trespass: is defined as the type of crime where one is logged in without proper authentication. In a nutshell, we can say that using paid content with forged credentials is a good idea.
  For example, on Netflix, one can use someone's ID password by hacking and logging into the account without the user's consent. This comes under cyber trespass.

  → Cyber vandalism: Cyber vandalism is simply vandalism in digital form. It's like a crime without any intention of criminality. These types of attacks are usually done by script kiddies or grey-hat hackers. They are the ones who are in the learning stage of cybersecurity.

- **Cyber-related crimes**: these types of crimes do not directly qualify as cybercrimes but partially violate cyber security. In plain language, we can say the internet is used as an assistance for doing something illegal. It has two parts.
  cyber exacerbated :the situation. cyber-assisted: causing a nuisance and breaking legal cyber laws. exacerbated has the following types of It refers to the use of the internet and other technology to stalk or harass someone by texting inappropriate content, sending emails with illegal content, etc. Or someone is checking out some organization's website and then targeting them online by joining the same.

  Cyber pedophiles: are those who use cyber technology to buy and sell children for illegal purposes.

2. Cyber-assisted crime: This is a type of crime in which cyber technology is simply used to aid in the commission of another crime. A phishing attack comes under this type of attack where the hacker uses technology to commit the crime. For example, online tax

4.Cyber terrorism

Nowadays, there is no single definition for the term terrorism. The origins of definitions used to define the term terrorism vary, with some focusing on terrorism actors and others on terrorism tactics, aims, and methods used.[6]In simple terms, cyber terrorism occurs when terrorist organisations use the internet to achieve their goals and objectives. ICT, or information and communication technology, has revolutionised the world as we know it, but it also provides lots of opportunities for terrorist organisations to expand, recruit, and propagate on numerous ICT platforms. Terrorists can utilise the internet to fund activities, train other terrorists, and plan terrorist acts [7]. Hacking of government or private servers to get access to critical information or even steal funds for use in terror activities is a more widespread definition of cyber terrorism.
As indicated by news reports distributed in the New York Times, the huge blackout in Mumbai was a digital assault and reports proposed that China was behind everything, as per the review, as a result of the galvanic emergency among India and China, China Cyber is utilizing its weapon.[8]

The framework disappointment caused huge blackouts in Mumbai and its rural areas on October 12, wrecked on the tracks, upset work from home and didn't influence financial exercises. It required two hours to reestablish the power supply for the necessary administrations. Different pockets started to get power in stages.

Around 14 Trojan ponies (regularly camouflaged as authentic programming) may have been presented on Maharashtra State Electricity Board (MSEB) servers, moving roughly 8GB of information from unaccounted for unfamiliar servers, just as being signed in through a boycott on MSEB servers IP (Internet Protocol) After the control and information assortment (SCADA) network examination, the digital police made the disclosure, "Deshmukh told a visitor on Monday[9]. Told journalists in the House. SCADA is an overall structure for control frameworks utilized in modern activities.

5.Covid an opportunity for hackers:

During the covid time where everyone is concern about their health's and family all the lifestyle turned digital, it is the cherry moment for the hackers as many of online user don't know about cyber security and even those who know they are also som how get trapped in ,the very common attack's that happen in those time were ransomware ,phishing ,frauds, sim swapping etc. Cyber-attackers see the pandemic as an opportunity to step up their criminal activities by exploiting the vulnerability of employees working from home and capitalizing on people's strong interest in coronavirus-related news (e.g. malicious fake coronavirus related websites)[10]. Even the big companies cannot save themselves from the cyber attack's and it was due to the negligence in the digital security. covid effect on health as well as cyber sector to.In India things were not that bad as compare to other countries but still need to educate basic security processes to everyone specially to those who earns lakhs of followers, companies who have details of very customers, clients. India ranked as 2nd in cyber attacked countries in the year between 2016-2019. it is evident that 22 percent increase in cyberattacks in India on IoT deployments. It happened in 2nd time further India faced large number of assaults in the many departments.[11]
It also exposed that Bengaluru, Mumbai, and New Delhi faced the large number of cyberattacks in the Indian cities According to Kaspersky's telemetry, when the world went into lockdown in March 2020, the total number of bruteforce attacks against remote desktop protocol (RDP) jumped from 93.1 million worldwide in February 2020 to 277.4 million 2020 in March—a 197 per cent increase[12].
Data reports:
1.the most hitted attack was ransomware ,where the attacker demands heavy Ransome from the victim in return for their data. In Q3 2020 it was researched, a 50% increase in the daily average of ransomware attacks compared to the first half of the year[13]. the top ransomware that hits in Q3 is named Maze and ryuk.
below graph represents the countries data that were affected by ransomware in Q3
The top 5 countries that are affected by ransomware attack.

- US (98.1% increase)

- India (39.2% increase)
- Sri Lanka (436% increase)
- Russia (57.9% increase)
- Turkey (32.5% increase)

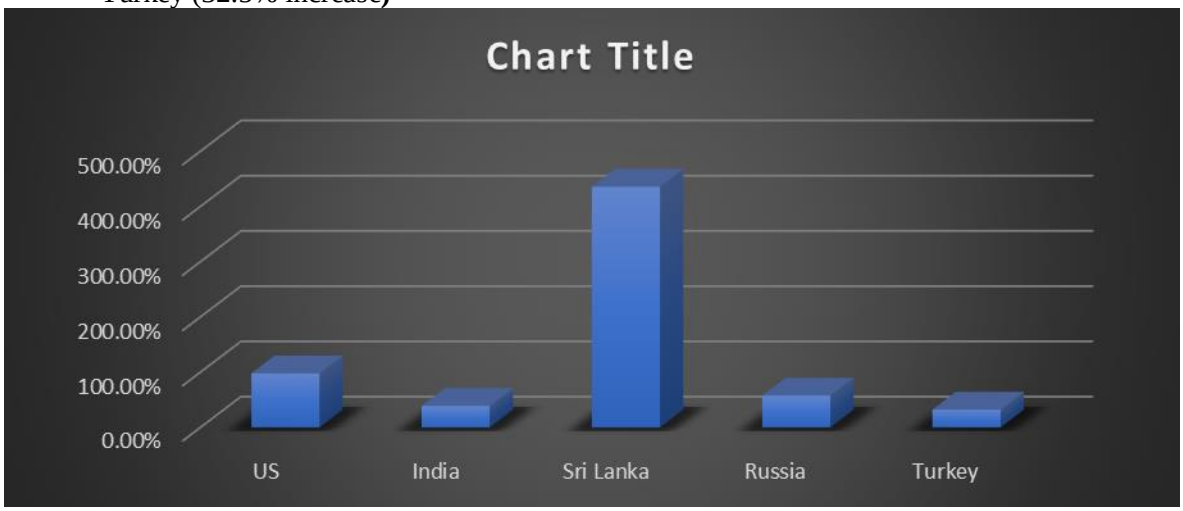

Fig 1 :ratio of top 5 ransomware attack affected country

Case study:

Ransomware assault on Haldirams: As we all know, Haldirams is a well-known snack manufacturer. In 2020, the company was cyber-attacked by ransomware. Hackers launched malware on their server, encrypting all of their data files and demanding a ransom of 7.5 million dollars in exchange for their data. Following the proof of evidence, the FIR was filed under IPC sections 384 (extortion), 420 (cheating), and section 66 of the IT Act[14] for "coming crime of criminal trespass." Data was eventually retrieved.

Colonial Pipeline Corporation :is a pipeline company based in the In May of this year, the US oil pipeline system colonial pipeline firm was hit by a significant cyber-attack known as ransomware.
Instead of only disrupting IT systems, the colonial pipelines firm shut down its whole pipeline operation to prevent future loss[15]. The corporation paid the hackers a ransom of $4.4 million in bitcoin.

Recommendation to protect your data:

1.Always use anti-virus and anti-spyware software in your systems.
2.Always Use secure verification methods.
Such as: use strong passwords (use special characters for your passwords) and change your passwords regularly.
• Use secure authentication, such as PIN or security questions beyond the password.3
• Use biometric tools such as fingerprints, voice tags, facial recognition scanning.
• Never store passwords on a computer or network. Use safe password manager if required.
3.Always update your software.
4.Limit your app rights.
An intruder only needs an open door to get inside your business. Limit the amount of access that is possible by restricting application rights to your devices. Only allow app features and functions that are absolutely necessary to get the job done. try not open mistrustful links or click on any download attachments from unknown sources

5.Personal information:
Keep your online site private information locked. attackers can easily access your information from just few data pointers, so the less you share publicly, the more secure your privacy is. For example, if you submit your nickname or reveal your mother's name, you can provide answers to two most common security questions.

6.Always Use Network Protection Methods
Protecting your network is important. To keep your network and its traffic secure you must follow:
- Install a firewall
- Ensure proper access control
- Use IDS / IPS to track potential packet floods

7. Use Standardize Software regularly
Keep your systems safe by modifying software. allow permission setting on on your system and do not install programs without permission.Not knowing about the software on your network is a security risk.

8.Encrypt and back up data

9.Do not insert unverified pen drives, CDs .

10.Do not sign in to unwanted websites.

Conclusion:

As per the above information ,we can conclude that cyber security is the not just a country issue but it is an global concern.as we know coming generation is going to be fully digital and it is difficult to assume how big chaos it can make if the individual's are not aware about the digital security and lack in the digital security is the major cause of increasing cyber-crime. the provided cyber-crime data is really a topic of concern, and in covid times the ration of digital user increased rapidly due to the sudden shifting of physical life to digital life, and because of it many user who are not fond of technology are the one who are targeted by the hacker and get hacked easily. So discussion is the not solution, it just help us to figure out the problem and solution to this problem is that government and even at personal stage we should take initiative to teach people about the basic security keys and try to save them from cyber-crime.

References:

1. 1.A Review on Cyber Security and the Fifth Generation Cyberattacks
June 2019 Saravanan Arumugam, Sri Krishna College of Technology ,Sathya Bama Subramanian
3. Cyber-Attack Modeling Analysis Techniques: An Overview
August 2016 Conference: FiCloud2016: 2016 IEEE 4th International Conference on Future Internet of Things and CloudAt: Vienna, AustriaVolume: 4th Hamad Al-Mohannadi University of Bradford
Qublai Khan Ali Mirza University of Bradford Anitta Patience Namanya
University of Bradford Irfan Awan
4. Cyber Security in the Age of COVID-19: A Timeline and Analysis of Cyber-Crime and Cyber - Attacks during the Pandemic June 2020 Harjinder Singh Lallie The University of Warwick
Lynsay Shepherd Abertay University Jason R. C. Nurse University of Kent Arnau Erola University of Oxford
5. THE BANARAS LAW JOURNAL Faculty of Law Banaras Hindu University National Advisory Board
Dr. Justice Balbir Singh Chauhan Former Judge Supreme Court of India & Former Chairman Law Commission of India Justice A.P. Sahi Chief Justice Patna High Court Prof. (Dr.) S.K. Verma Former Secretary General Indian Society of International Law New Delhi Prof. (Dr.) Manoj K. Sinha Director The Indian Law Institute New Delhi Prof. (Dr.) K.C. Sunny Vice-Chancellor

The National University of Advance Legal Studies Kochi

6. Cyber Terrorism and Cyber Crime – Threats for Cyber Security
June 2012 Conference: Global Security and Challenges of the 21st Century - MIT University – Skopje ,Jugoslav Achkoski,Goce Delcev University of Štip

7. https://www.jigsawacademy.com/blogs/cyber-security/cyber-terrorism /

8. https://theprint.in/opinion/how-chinese-cyber-attacks-mumbai-blackout-depict-a-new-era-of-low-cost-high-tech-warfare/61489

9. https://www.hindustantimes.com/cities/mumbai-news/maharashtra-cyber-police-suspects-cyber-attack-behind-mumbai-power-outage-101614654439868.html

10. https://www2.deloitte.com/ch/en/pages/risk/articles/impact-covid-cybersecurity.html

11. Cyber Crimes against the State: A Study on Cyber Terrorism in India Dr.T. Ambika Assistant Professor, School of Law, Sathyabama Institute of Science and Technology, Chennai. Dr.K. Senthilvel Assistant Professor, Faculty of Law, SRM Institute of Science and Technology, Chennai. 2020
12. .https://www.business-standard.com/article/technology/india-becomes-favourite-destination-for-cyber-criminals-amid-covid-19-121040501218_1.html
13. https://blog.checkpoint.com/2020/10/06/study-global-rise-in-ransomware-attacks

14. .https://timesofindia.indiatimes.com/city/noida/haldirams-hit-by-ransomware-attack-hackers-asked-for-7-5l/articleshow/78712465.cms
15. https://analyticsindiamag.com/5-ransomware-attacks-of-2021-that-blew-the-internet/