IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 7.39 ⁜ Vol. 11, Issue 5, May 2022

DOI: 10.17148/IJARCCE.2022.115143

A STUDY OF CYBER SECURITY CHALLENGES AND ITS EMERGING TRENDS ON LATEST TECHNOLOGIES

Shilpa S. Kalwal[1], P.T. Tandekar[2], S.K Purve[3]

Student, Computer Science & Engineering, Shri Sai college of Engineering & Technology, Bhadrawati, Chandrapur, M.S, India[1]

Assistant Professor, Computer Science & Engineering, Shri Sai College of Engineering & Technology, Bhadrawati, Chandrapur, M.S, India[2]

Assistant Professor, Computer Science & Engineering, Shri Sai College of Engineering & Technology, Bhadrawati, Chandrapur, M.S, India[3]

Abstract: cyber security is the state of process of protecting and recovering computer systems network devices and program from any type of cyber-attack. It plays important role in field of information technology. Today in the modern life style most of the people use internet, and uses new technologies in which they give their data to many apps and websites. Securing the information have become one of the biggest challenges in the present day. In this present time cyber-attacks are increasingly rapidly; cyber threats can come from any level of organization. whenever we think of cyber security we first think about cybercrime. Information theft is the most expensive and fastest – growing segment of cybercrime. This paper primarily focuses on cyber security concerns related to the new technology latest cyber security techniques, principals, trends and developments that impacts cyber security.

Keywords: Cybercrime, cyber security, cyber ethics, cybersecurity techniques, social media.

1.INTRODUCTION

Technology in the network security space has been through many dramatic changes recently. Like any other space in the life, technology has its own benefits and challenges. While it enhances a human's life in almost all the aspects whether its healthcare, transport, communication, education, business etc. In these sector's storage of all sorts of information, including sensitive data, credential etc., securing these details is extremely essential. Tons of data and sensitive information are constantly being shared over the internet. the internet is mostly private and secure, but it can also be an insecure channel for exchanging information, with a risk of intrusion by hackers and cybercriminals. Internet security is a top priority for individuals and businesses and alike.

While the web presents users lots of information and services, it also includes several risks. Cyberattacks are only increasing in sophistication and volume, with many cybercriminals using a combination of different types of attack to accomplish the single goal. Even the latest technologies like cloud computing, mobile computing, internet banking, e-commerce website needs high level

security but due to advance technologies we are unable to protect our private information in a very effective way and this leads to cybercrimes.

It is necessary to enhance security defense mechanism and different techniques and trending topics in the area of information security. Everyone should be trained on this cyber security and save their sensitive their valuable particulars.

2.CYBER CRIME

Cyber-crime is a term for any illegal activity that uses a computer as its primary means of commission and theft. The United States department of justice has extended the scope of cyber-crime to cover any crime that uses a device for evidence storage. Since most information processing these days depends on the use of information technology, the control, prevention and investigation of cyber activates paramount to the success of the organization, Government's agencies individuals.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

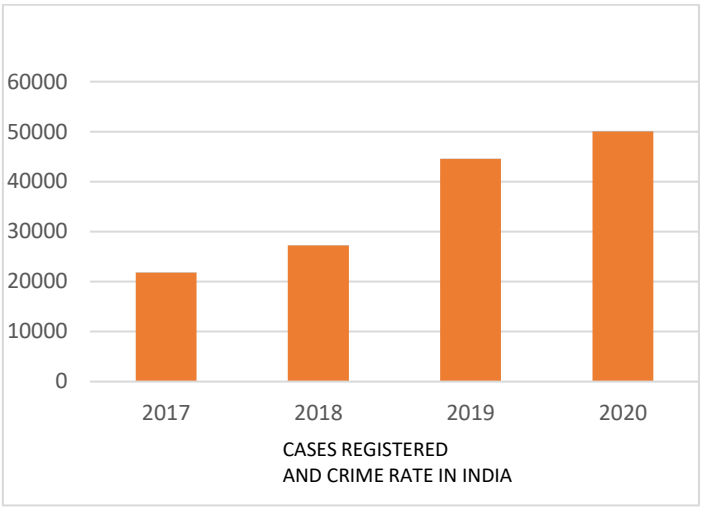
ISO 3297:2007 Certified ⁜ Impact Factor 7.39 ⁜ Vol. 11, Issue 5, May 2022

DOI: 10.17148/IJARCCE.2022.115143

Although prevention as they say better than cure irrespective of the deterrent measures to prevent and or control cyber-crime, there may still be breaches, where this occurs. As technology has a major role in the lives of an extremely individual day by day, cybercrime too can increase alongside technological.

3. CYBER SECURITY

Cyber security is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks. It's also known as information technology security or electronic information security. Privacy and information protection can be the primarily security behavior which any company cares about continually. Social networking sites provide an environment wherever user feel secure while they function with friends and family, cyber criminals also seek to steal personal information via social media sites.



Cybercrimes in the country have increased in the past years. In 2017,21,796 cases of cybercrime registered and in 2020, this increased to 50,035. this means that India registered 136 cybercrime cases every day in 2020, according to the National Crime Records Bureau. India's cybercrime rate, or the number of cybercrimes per one lakh of population, also shout by 270% in four years -in 2017 it was 1.7 and in 2020 saw it climb up to 3.7.

4. CYBER ETHICS

The term cyber ethics refers to a set of moral rules or a code of behavior applied to the online environment. As a responsible netizen, you should observe these rules to help make cyberspace a safe place. The below are few of them:

- DO not operate others accounts using their passwords.
- Never try to send any kind of malware to other's system and make them corrupt.
- Always adhere to copyrighted information and downloads games or video's only if they are permissible
- Don't be a bully on the internet. Do not call people names, lie about them, send embarrassing pictures of them, or do anything else to try to hurt them.

5. CYBER SECURITY TECHNIQUES

There are sheer variety of cyber security solution at play in the market, from endpoint anti-virus software, to firewalls, to host-and-network-based IDS/IPS solutions, the security professionals (of enterprises and businesses).

5.1 INTRUSION DETECTION SYSTEM(IDS): Intrusion detection system (IDS) is typically installed behind a firewall, offline, and is focused on the detecting and logging security events that affect the private network of a business. The IDS primarily reports on animalities and known threats detected within the private network, and comes with a group of 'signatures' that use bit patterns (1s and 0s) and RFC application compliance to detect known malware threats. IDS solutions can also be linked to access control and management systems to detect unauthorized access and activity. the IDS is purely a reporting tool

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 7.39 ⁜ Vol. 11, Issue 5, May 2022

DOI: 10.17148/IJARCCE.2022.115143

5.2 FIREWALL

A firewall is a network security system that monitors and controls the incoming and outgoing network traffic based on predetermine security rules. A fire wall typically establishes a barrier between a trusted, secure internal network and another outside network, such as the internet, that is assume to not be secure or trusted. A firewall is a protective system that lies, in essence, between user's computer network and the internet. When used correctly, a firewall prevents unauthorized use and access to user's network. Without a firewall, all the traffic directly moves form the internet to user's computer. In this diagram, the "valid" traffic is colored green, and "malicious" traffic is red.

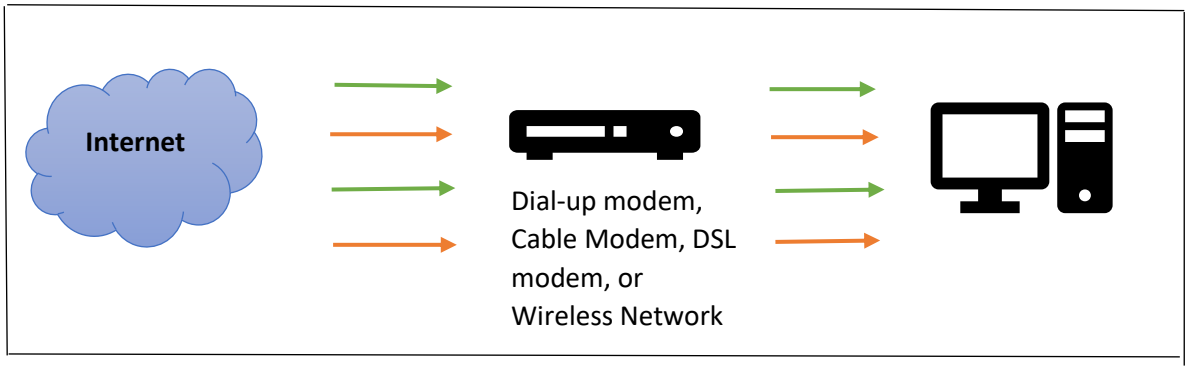


Fig 5.2.1: A FIREWALL

5.3 MALWARE SCANNER

Malware scan is the process of deep scanning the computer to prevent malware infection. It is accomplished using an anti-malware software. This process involves multiple tools and techniques to identify malware. Every time a file enters the computer the malware scanning process starts. The ani malware analyzes the file and collects the file code. Note, malware contains a unique code or signature that is used to identify it.

6.ROLE OF SOCIAL MEIDA

As social media has grown by leaps and bonus, it has brought various benefit simultaneously, and it has posed serious social media cyber security concerns. It also acts a vulnerable platform to be exploited by hackers. Social media plays a huge role in cyber security and could be checked if it has originated from a trusted and a reliable source and that they are not altered. Users share their personal information on social media, which can cause privacy breaches.
We need to be smart using the internet and avoid visiting untrusted website re never to be clicked; instead, type in the browser's URL address

7.CONCLUSION

This paper focus on cyber security need in the present situation because cyber-crime is increasingly growing a national an economic level cyber-crime is major implication at the industries and institutes, as well as public and private sectors. Cyber-crime continues to diverge down different paths with each new year that passes so does the security of the information the latest and destructive technologies, along with the new cyber tools and threats that come to light each day are challenging for the organization as well as for common peoples, there are new intelligence software and platform come into existence that try to protect the device and organizations private data. There is no perfect solution for cyber-crimes but we should try to minimize them with some of the techniques mention above in this paper we try to collect some techniques for securing information.

8. ACKNOWLEDGMENT

I would like to thankful to my department of computer science & Engineering to support and for providing research environment tools to accomplish this work.

9.REFERENCE

1) ITU Cyber Security Work Program to Assist Development Countries, 2009
2) Computer Security Practices in Non Profit Organizations – A Net Action Report by Audrie Krause
3) ITU Cyber Security Work Program to Assist Development Countries, 2008

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified ⁜ Impact Factor 7.39 ⁜ Vol. 11, Issue 5, May 2022
DOI: 10.17148/IJARCCE.2022.115143

4) Kellermans, "Technology Risk Checklist, Cybercrime and Security", IIB-2
5) Cyber Security: Considerations and Techniques for Network-Based Protection version 2.0
6) A Sophos Article 04. 12v1.dNA, eight trends changing network security by James Lynne
7) Md Lia kat Ali Ku tub Thakur Beatrice Autobytel Challenges of Cyber Security and the Emerging Trends BSCI'19, July 8, 2019, Auckland, New Zealand