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 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 5, May 2023

DOI: 10.17148/IJARCCE.2023.125223

REVIEW ON CYBER SECURITY

Harshali R. Tapase[1], Vijay. M. Rakhade[2], Lowlesh N. Yadav[3]

Final Year Student, Computer Science Engg., Shri Sai College of Engineering & Technology, Bhadrawati, India[1]

Professor, Computer Science Engg., Shri Sai College of Engineering & Technology, Bhadrawati, India [2]

Professor, Computer Science Engineering, Shri Sai College of Engineering & Technology, Bhadrawati, India[3]

Abstract: Cybersecurity plays an essential part in the field of Information Technology. We'll be assaying a variety of Cyber-attacks and different security styles. Securing information has come one of the biggest challenges in the present day. Whenever we think about cyber security, the first thing that comes to mind is 'cybercrime', which is adding immensely daily. Various Governments and companies are taking numerous measures to help this cybercrime. Besides different styles, cyber security is still a huge concern to numerous. This paper concentrated on the challenges cyber security faces on the rearmost technologies. It also focuses on the rearmost cyber security ways, ethics, and trends changing the face of cyber security.

Keywords: cyber security, cybercrime, online

I. INTRODUCTION

Today man can send and receive a new form of data may be an email or an audio or video just by the click of a button but did he ever think about how he is securely data-id being transmitted or sent to another person safely without any leakage of information the answer lies in cyber security. Today internet is the fastest-growing infrastructure in everyday life. Moment internet is a swift-growing structure in everyday life. But due to this emerging technology, we are unable to safeguard our private information in a very effective way and hence these days Cybercrimes are increasing day by day. Today more than 60% of total commercial transactions are done online, so this field requires a high quality of security for transparent and best transitions. hence cyber security has become the latest issue. The scope of cyber security is not just limited to securing information in the IT industry but also the various other fields like cyberspace.

II. CYBERCRIME

Cybercrime is a term for any illegal exertion that uses a computer as its primary means of commissioning theft. The U.S. department of justice expands the description of cybercrime to include any illegal exertion that uses computers for the storehouse of substantiation. The growing list of cybercrimes includes crimes that have been made possible by computers, similar as network intrusion and the dispersion of computer contagions, as well as computer-grounded variations of crimes, similar as identity theft, stalking, bullying, and terrorism which have come as a major problem to people and Nations. The consumer must appreciate and observe introductory information security ethics like opting for strong watchwords, actuality being cautious of accessories in dispatch, and having backup data. Learn redundant introductory cyber security values.

III. PAGE STYLE

1. Virus-

When executed, this type of malicious software replicates itself by modifying other computer programs. Computer viruses cause economic damage due to system failure, corrupting data, increasing maintenance costs, etc.

DOI: 10.17148/IJARCCE.2023.125223

2. Worms-

A computer worm is a standalone malware computer program that replicates itself to spread to another computer. numerous worms are designed only to spread and don't essay to change the system they pass through.

3. Malware-

Malware is a term short for malicious software, used to destroy computer operations, gather very sensitive information, or gain access to private computer systems. malware is defined by its vicious intent, acting against the conditions of the computer stoner, and doesn't include software that causes unintentional detriment due to some insufficiency. The term malware is occasionally used for bad malware and unintentionally dangerous software.

CYBER SECURITY TECHNIQUES:

1. Access control and password security-

The concept of user name and password has been a fundamental way of protecting our information and they may be one of the first measures regarding cyber security.

2. Authentication of data-

DOI: 10.17148/IJARCCE.2023.125223

The documents that we receive must always be authenticated before downloading that is it should be checked if it has originated from a trusted and reliable source and that they are not altered. Authenticating these documents is usually done by the anti-virus software present on the devices. Good anti-virus software is also essential for protecting the device from viruses.

3. Malware scanners-

This is software that usually scans all the lines and documents present in the system for vicious code or dangerous viruses. viruses, worms, and Trojan horses are examples of vicious software that are frequently grouped and referred to as Malware.

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. All dispatches entering or leaving the internet pass through the firewall present, which examines each communication and blocks those that don't meet the specified security criteria. hence Firewalls play an essential part in detecting Malware.

Internet Security products:

1. Antivirus-

Antivirus software and internet security programs can protect a Programmable device from attack by detecting and eliminating viruses. Antivirus software was used in the early years of the internet but now with the development, several free security applications are available on the internet.

2. Password Managers-

The password manager is a software application that is used to store and organize passwords. Password managers usually Store passwords encrypted, requiring the person to create a master password; a single, ideally a very strong password that allows the user access to their entire password database.

3. Security Tokens-

Some online sites offer the user the ability to use the 6-number code which aimlessly changes after every 30-60 seconds on a security token. The keys on the token have erected computations and manipulated figures grounded on the current time erected into the device. This means that after every thirty seconds there is only a certain sequence of numbers possible that would will it be correct to access the online account.

Advantage-

1. It will safeguard your company.
2. Please keep your personal information private.
3. Enable users to work in a relaxed environment.
4. It also maintains efficiency.
5. Various jobs are mechanized as a result of this.
6. Organize data and information more effectively.
7. The information and files as recommendations and suggestions are essential for the productivity of the business.

Disadvantage-

1. The high cost of cyber security.
2. The complicated nature of cyber security.
3. The need for constant monitoring.
4. The lifelong process is the nature of the field.
5. Slows down the system even more than before.
6. Workplace stress.
7. Short supply of resources.

DOI: 10.17148/IJARCCE.2023.125223

IV. CONCLUSION

This paper is trying to tell about the various cyber-attack and the various security method that can be used to prevent a device from getting attacked. Also, it helps to overcome a server loophole in their computer operation.

REFERENCES

1. A STUDY OF CYBER SECURITY CHALLENGES AND ITS EMERGING TRENDS ON LATEST TECHNOLOGIES G. NIKHITA REDDY, G.J. UGANDER REDDY.
2. RESEARCH PAPER ON CYBER SECURITY Mrs. Ashwini Sheth, Mr. Sachin Bhosale, Mr. Farish Kurupkar, CONTEMPORARY RESEARCH IN INDIA (ISSN 2231-2137): SPECIAL ISSUE: APRIL, 2021.
3. A Review Paper on Cyber Security, Saloni Khurana, International Journal of Engineering Research & Technology (IJERT) ISSN: 2278-0181 Published by, www.ijert.org IMPACT – 2017
4. Cyber Security: Understanding Cyber Crimes- Sunit Belapure Nina Godbole.
5. IEEE Security and Privacy Magazine – IEEE-CS “Safety Critical Systems – Next Generation “July/ Aug 2013.
6. https://en.wikipedia.org/wiki/Phishing
7. https://en.wikipedia.org/wiki/Internet_security#Phishing
8. https://en.wikipedia.org/wiki/Malware