International Journal of Advances in Scientific Research and Engineering (IJASRE)

E-ISSN : 2454-8006

DOI: 10.31695/IJASRE.2023.9.2.7

Volume 9, Issue 2
February - 2023

Cyber Security: Challenges and Preventive Measures

Sneha Bedadhala[1], Chandra M. M. Kotteti[1], Matthew N. O. Sadiku[2]

[1]School of Computer Science and Information Systems
Northwest Missouri State University
Maryville, MO 64468

[2]Roy G. Perry College of Engineering
Prairie View A&M University
Prairie View, TX, USA

ABSTRACT

Cyber Securityplays a vital role in information technology. In recent days, the major issue faced by most private companies and government organizations is cyber-attacks,which can causesignificant financial harm. Everything today has become electronic and protecting the data from cyber-attacks has become the biggest challenge. There are diverse ways to prevent cyber security attacks. The primaryfocus of this article is to present a variety of cyber security attacks and discusssome preventive measures on how to overcome thechallenges posed by those attacks.

Keywords: Cyber Security, Cyber-attacks, Confidentiality, Information Technology (IT).

INTRODUCTION TO CYBER SECURITY

Cyber Security is concerned with challenges related to the security of electronic datathat includesmaintaining privacy, accessibility, and integrity. Privacy refers to the act of keeping information from being disclosed to unreliable systems or people. Integrity refers to the absence of any unauthorized deletion or change. Finally, accessibility refers to the ability of a system to process, store, and deliver information to be used whenever necessary and by those who need it. The main goal of the research is to have a piece of proper knowledge about cyber security to prevent attacks that are primarily caused by information technology [1]. The term "cyber security" refers to the entire body of technology and procedures used to protect computer systems and electronic data. We are unable to protect our personal data,which has also emerged as a current concern. There should be some best ways to protect the data, and devices from unauthorized users accessing it and causing damage to the resources [2].

2. LITERATURE REVIEW

As per[3] there is a need to enroll in a training program that educates all employees across all departments on cyber security. The implementation of the training program for cyber security must be given high importancetoprotecting the company's data. First and foremost thing is that the company needs to figure out what the employees need to be trained on and detailed security awareness programs should be conducted within the organization. All the workforce should be responsible for maintaining data integrity after signing the agreements. They should make sure of using unauthorized malware software.

The review in[4], includes the concepts of preventing cyber security using machine learning. There are many challenges faced due to cyber security and proper measures are taken based on Artificial Intelligence (AI). AI and Machine Learning are the best ways to reduce the impact of cybersecurity by detecting the threats caused to organizations.

According to[5], most cyber-attacks were due to mistakes made by humans and reports are in favor of proving that human error is responsible for the damage to the company. To combat these dangers, a company should promote a culture of risk awareness at work, starting with an emphasis on cyber security.The crucial part of cyber security is security data from any person. The organization's primary role is to verify user identification and secure the data by giving access to authorized users.

3. CYBER SECURITY ATTACKS

- Denial-of-service attacks are the most common cyber-attack on hardware, software, or other network resources that prohibits authorized users from using the resources and services they are entitled touse, which results in the stop of interaction between other systems and the internet as well.
- A logic bomb is a cyber-attack of malicious logic that waits for the correct situation to strike the software and perform harmful activities.
- Sniffer is a program that intercepts network traffic using a sniffer packet and scans each packet in the data stream for certain data.[1].
- Trojan horses frequently resemble beneficial programs that users are willing to run while concealing hazardous code. It leads to the corruption of the files and the virus is loaded into the memory. Viruses can only spread through human interaction, unlike worms.
- Abuse tools are used to attack the business and process features of the software application.
- Virus is a common cyber security attack that affects the devices through a code that results in infecting files and other computer areas.
- Frequent counting represents the count of the cyber-attacks that are taking place throughout the day. It keeps track of all the data breaches done in the organization or any industry.
- Spyware is software installed in the device which collects all the data and exposes it to third-party hackers.

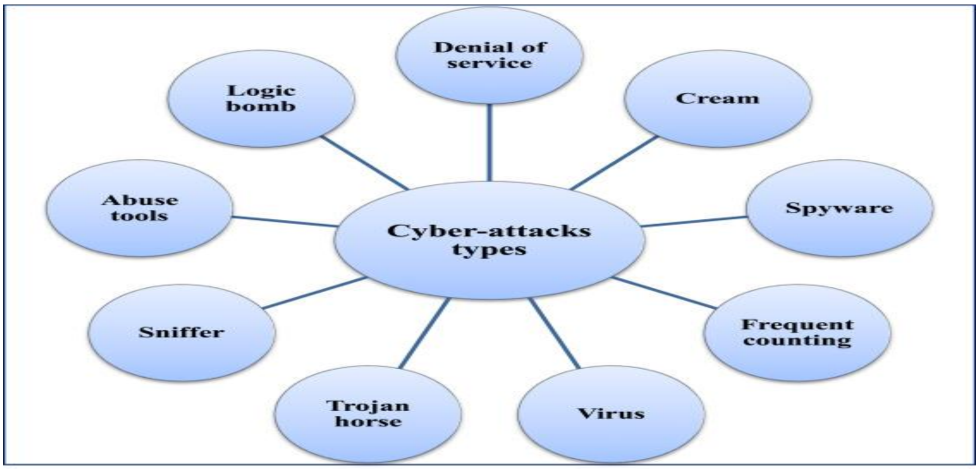

Fig. 1 Typesof cyber-attack

4. TYPES OF CYBER-SECURITY

Cyber-security has different methods to prevent data, and networks from internal or external threats.Cyber Security Analysts make sure that permission should be given or not for the people who are working in an organization to access computers, servers, intranets, and networks. There are many areas of cyber securitythat deal with different security concerns as shown in Fig. 2 for better data protection.

DOI: 10.31695/IJASRE.2023.9.2.7

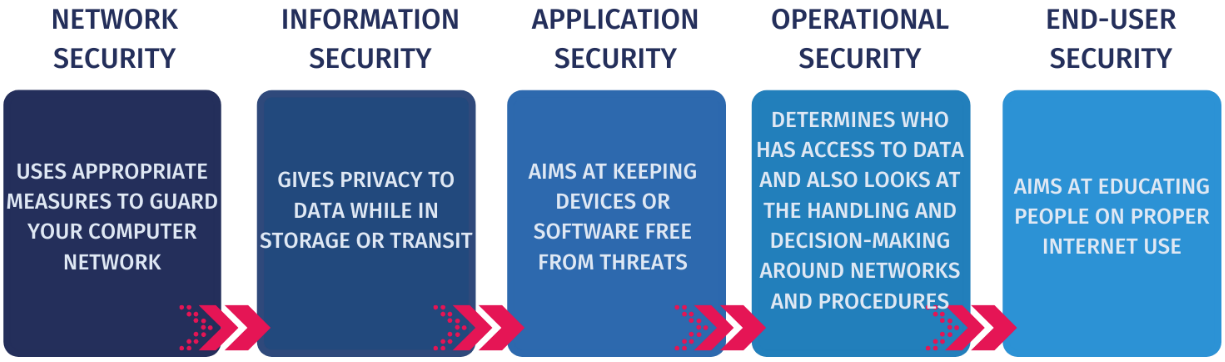
NETWORK SECURITY
USES APPROPRIATE MEASURES TO GUARD YOUR COMPUTER NETWORK
INFORMATION SECURITY
GIVES PRIVACY TO DATA WHILE IN STORAGE OR TRANSIT
APPLICATION SECURITY
AIMS AT KEEPING DEVICES OR SOFTWARE FREE FROM THREATS
OPERATIONAL SECURITY
DETERMINES WHO HAS ACCESS TO DATA AND ALSO LOOKS AT THE HANDLING AND DECISION-MAKING AROUND NETWORKS AND PROCEDURES
END-USER SECURITY
AIMS AT EDUCATING PEOPLE ON PROPER INTERNET USE

Fig. 2 Types of Cyber Security

- Network Security: Network security is nothing but providing security to computer networks by preventing them from viruses and hackers using both hardware and software technologies. All the possible actions are taken to protect the data from integrity.

- Application security: Application security is providing security to the application code and data against cyber threats. All possible measures are used to the secure application from being attacked.

- Information security: Information security prevents accessing information from unauthorized users. Users are not allowed to disclose the information and prevent unwanted activity.

- Operational security: Operational security is securing data from the wrong hands by determining who has access to it and checking whether he/she is an authorized person to use the data.

- End-User Security: End-User Security is all about educating or giving proper insight to the users about the security attacks related to cyberspace.Trainingrelated to security will lead to a decrease in cyber security attacks. This helps to explore user identificationmore and helpswork-related security identity[6].

4.1 Preventive Measures:

- Implement fundamental cyber security training: Conducting workshops helps staff members use only approved software and maintain secure passwords. It's also a good idea to put into effect common sense procedures related to employee safety and access to technology[7]. It can be accomplished by taking a few straightforward actions, such as prohibiting employees from accessing their systems from home duringnon-working days or implementing a verification process.

- Detect and prepare: The main duty of the cyber security analyst is to detect and monitor vulnerabilities. It results in avoiding harm and allowing for a smooth return to business[8].

- Invest in VPN technology since you have no control over the external network, regardless of the severe measures the main responsibility of the organizations is to prevent the company’s data.They need to make the devices secure and can be used only in the office premises through organizations’ Wi-Fi. The employee who is working at home must connect to the organization’s VPN for more security.

- 2-Factor Authentication: Multi-factor authentication is the process of providing security for the applications or any data by providing the features like a phone call, SMS, OTP, email verification, and others. This helps the users to make their login secure and protect their data from hackers.

5. Conclusion

DOI: 10.31695/IJASRE.2023.9.2.7

The internet is havinga significant impact on people's lives in the modern world, where cyber-security experts must deal with a variety of cyber threats in situations that are almost always real-time. Several challenges are coming up every day to provide better security for organizations' infrastructure. However, they need to know how to use their platform well and resolve the issues. In this article, we presented a quick overview of the topic of cyber security, how it is impacting society and some of the preventive measures.

References

[1] M. I. Al-Ghamdi, "Effects of knowledge of cyber security on prevention of attacks," *Materials Today: Proceedings.*

[2] B. Alhayani, S. T. Abbas, D. Z. Khutar and H. J. Mohammed, "Best ways computation intelligent of face cyber attacks," *Materials Today: Proceedings.*

[3] T. Caldwell, "Making security awareness training work," *Computer Fraud & Security*, vol. 2016, pp. 8--14.

[4] A. A. Jamal, A.-A. M. Majid, A. Konev, T. Kosachenko and A. Shelupanov, "A review on security analysis of cyber physical systems using Machine learning," *Materials Today: Proceedings.*

[5] B. Dash and M. F. Ansari, "An Effective Cybersecurity Awareness Training Model: First Defense of an Organizational Security Strategy".

[6] O. Ogbanufe, "Enhancing end-user roles in information security: Exploring the setting, situation, and identity," *Computers & Securityx*, vol. 108, p. 102340.

[7] S. Hart, A. Margheri, F. Paci and V. Sassone, "Riskio: A serious game for cyber security awareness and education," *Computer Fraud & Security*, vol. 95, p. 101827.

[8] S. Furnell, H. Heyburn, A. Whitehead and J. N. Shah, "Understanding the full cost of cyber security breaches," *Computer Fraud & Security*, vol. 2020, pp. 6--12.

About The Authors

Sneha Bedadhala is a graduate student at Northwest Missouri State University, Maryville, MO. She is pursuinga major in Applied Computer Science.She has worked as a Cyber Security Analyst and keptinsight into cyberattacks taking place in the real world.Her research interests include Machine Learning and Cyber Security on cloud-based applications.

Chandra M. M. Kottetiis an assistant professor in the School of Computer Science and Information Systems at Northwest Missouri State University, Maryville, MO. His current research interests include machine learning, deep learning, data science, and computer science.

Matthew N. O. Sadiku is a professor emeritus in the Department of Electrical and Computer Engineering at Prairie View A&M University, Prairie View, Texas. He is the author of several books and papers. His areas of research interest include computational electromagnetics and computer networks. He is a fellow of IEEE.

C. A. Email: snehareddy2529@gmail.com

DOI: 10.31695/IJASRE.2023.9.2.7