IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 2, August 2024

A Study of Cyber Security Challenges and Its Emerging Trends on Latest Technologies

Chavan Dhanashri, Chavan Aishwarya, Chavan Sanika, Chavan Ruchita, Prof. Kumbhoje M.R.
Department of Commerce and Research Center BBA(CA)
Shri Shiv Chhatrapati College, Junnar, Maharashtra, India

Abstract: *Cyber Security plays an important role in the field of information technology .Securing the information have become one of the biggest challenges in the present day. Whenever we think about the cyber security the first thing that comes to our mind is cyber crimes which are increasing immensely day by day. Various Governments and companies are taking many measures in order to prevent these cyber crimes. Besides various measures cyber security is still a very big concern to many. This paper mainly focuses on challenges faced by cyber security on the latest technologies .It also focuses on latest about the cyber security techniques, ethics and the trends changing the face of cyber security*

Keywords: Cloud providers, Cybercriminals, *Threats,* Mobile security

I. INTRODUCTION

Today Internet is the fastest growing infrastructure in everyday life. In today's technical environment many latest technologies are changing the face of the mankind. But due to these emerging technologies 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 percent of total commercial transactions are done online, so this field required a high quality of security for transparent and best transactions. Hence cyber security has become a latest issue. The scope of cyber security is not just limited to securing the information in IT industry but also to various other fields like cyber space etc. Even the latest technologies like cloud computing, mobile computing, Ecommerce, net banking etc also needs high level of security. Since these technologies hold some important information regarding a person their security has become a must thing. Enhancing cyber security and protecting critical information infrastructures are essential to each nation's security and economic wellbeing. The fight against cybercrime needs a comprehensive and a safer approach. Given that technical measures alone cannot prevent any crime, it is critical that law enforcement agencies are allowed to investigate and prosecute cybercrime effectively. Today many nations and governments are imposing strict laws on cyber securities in order to prevent the loss of some important information. Every individual must also be trained on this cyber security and save themselves from these increasing cyber crimes.

II. CYBER CRIME

Cyber crime is a term for any illegal activity that uses a computer as its primary means of commission and theft. The U.S. Department of Justice expands the definition of cyber crime to include any illegal activity that uses a computer for the storage of evidence. The growing list of cyber crimes includes crimes that have been made possible by computers, such as network intrusions and the dissemination of computer viruses, as well as computer-based variations of existing crimes, such as identity theft, stalking, bullying and terrorism which have become as major problem to people and nations. Usually in common man's language cyber crime may be defined as crime committed using a computer and the internet to steel a person's identity or sell contraband or stalk victims or disrupt operations with malevolent programs.

III. CYBER SECURITY

Cyber security is the practice of protecting systems, networks, and programs from digital attacks. These cyber attacks are usually aimed at accessing, changing, or destroying sensitive information; extorting money from users via ransomware; or interrupting normal business processes.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 2, August 2024

Implementing effective cyber security measures is particularly challenging today because there are more devices than people, and attackers are becoming more innovative.

IV. DEFINITIONS

"Cyber Security is the body of technologies, processes, and practices designed to protect networks, devices, programs, and data from attack, theft, damage, modification or unauthorized access."

"Cyber Security is the set of principles and practices designed to protect our computing resources and online information against threats."

V. TRENDS CHANGING CYBER SECURITY

1. Response and Resilience: Building effective incident response and resilience strategies has become paramount. Organizations must focus on preventing attacks and detecting, mitigating, and recovering from breaches. This includes regular security assessments, employee training, and robust incident response plans.
2. Global Collaboration: Given the transnational nature of digital threats, international collaboration has become crucial. Governments, law enforcement agencies, and cyber security organizations worldwide are working together to share threat intelligence, track down cybercriminals, and mitigate threats on a global scale.
3. Mobile Devices: A Growing Target for Cyber Attacks The proliferation of mobile devices has made them lucrative targets for cybercriminals, with a notable increase in malware and attacks targeting mobile banking and personal data. The extensive use of smart phones for various activities, including financial transactions and communication, amplifies the risks associated with potential breaches. Mobile security becomes a focal point as cyber security threats evolve, with anticipated trends indicating a rise in smart phone-specific viruses and malware.
4. Cloud Security Challenges and Solutions: As organizations rely on cloud services, ensuring robust security measures becomes paramount for data storage and operations. While cloud providers implement robust security protocols, vulnerabilities may still arise due to user-end errors, malicious software, or phishing attacks. Continuous monitoring and updates are essential to mitigate risks and safeguard confidential data stored in the cloud.

VI. CONCLUSION

Computer security is a vast topic that is becoming more important because the world is becoming highly interconnected, with networks being used to carry out critical transactions. Cybercrime continues to diverge down different paths with each New Year that passes and so does the security of the information. The latest and disruptive technologies, along with the new cyber tools and threats that come to light each day, are challenging organizations with not only how they secure their infrastructure, but how they require new platforms and intelligence to do so. There is no perfect solution for cyber-crimes but we should try our level best to minimize them in order to have a safe and secure future in cyber space.

REFERENCES

[1]. A Sophos Article 04.12v1.dNA, eight trends changing network security by James Lyne.
[2]. Cyber Security: Understanding Cyber CrimesSunit Belapur Nina Godbole.
[3]. A Look back on Cyber Security 2012 by Luis corrons – Panda Labs