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: 7.301
Volume 3, Issue 5, May 2023

Overview of Cyber Security

Akshit Gupta and Dheeraj
Student, B. Tech, Department of Computer Science and Engineering
Dronacharya College of Engineering, Gurgaon, India

Abstract: *Cybersecurity has become one of the most critical issues of our time, with cyber attacks becoming more frequent and sophisticated. This paper provides an overview of the threats that organizations face in the cyber world, the techniques used by cyber criminals to attack systems, and the best practices that organizations can implement to protect themselves. The paper discusses the importance of cybersecurity, the challenges that organizations face in implementing effective cybersecurity measures, and the role of individuals in preventing cyber attacks.*

Keywords: Threats, Techniques, Best Practices

I. INTRODUCTION

In today's digital age, organizations are increasingly reliant on technology to operate their businesses. While technology has enabled unprecedented levels of productivity, efficiency, and innovation, it has also created new vulnerabilities that can be exploited by cyber criminals. Cyber attacks can result in significant financial losses, damage to a company's reputation, and compromise of sensitive data. In this paper, we provide an overview of cyber security, including the threats that organizations face, the techniques used by cyber criminals, and the best practices that organizations can implement to protect themselves.

Threats:
The threats that organizations face in the cyber world are constantly evolving. Malware, ransomware, phishing attacks, and social engineering are just a few of the tactics that cyber criminals use to exploit vulnerabilities in systems. In addition to these threats, organizations must also be aware of insider threats, where employees or contractors with access to sensitive information may intentionally or unintentionally compromise data.

Techniques:
Cyber criminals use a variety of techniques to carry out attacks. Malware, such as viruses, trojans, and worms, can infect systems and steal sensitive information. Ransomware can encrypt files and demand payment in exchange for the decryption key. Phishing attacks use social engineering to trick individuals into divulging sensitive information, such as passwords or credit card numbers. Social engineering tactics, such as pretexting, baiting, and quid pro quo, can also be used to manipulate individuals into providing sensitive information.

Best Practices:
Organizations can implement several best practices to protect themselves against cyber attacks. These include implementing a layered security approach, educating employees on best practices for security, conducting regular security audits, and using encryption and other security measures to protect sensitive data. Additionally, organizations should have an incident response plan in place to quickly and effectively respond to cyber attacks if they do occur.

II. CONCLUSION

In conclusion, cyber security is a critical issue that all organizations must address to protect themselves against the ever-evolving threats that exist in the digital world. By implementing best practices and educating employees on the importance of cyber security, organizations can reduce their risk of becoming victims of cyber attacks. It is important to remember that cyber security is a continuous process that requires ongoing attention and investment to stay ahead of the latest threats.