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: 6.252
Volume 3, Issue 6, January 2023

An Overview on Cyber Security

Prof. Darshan Patil and Abhishek Subhash Jha
Asst. Professor and Research Scholar
St. Rock's College of Commerce and Science, Borivali (W), Mumbai, India

Abstract: *The provided text emphasizes the critical role of cyber security in safeguarding networks and devices against external threats, highlighting the core principles of confidentiality, integrity, and availability (CIA). It underscores the importance of authentication mechanisms, such as usernames and passwords, in enhancing security. The text outlines various types of cybercrimes, including computer-assisted crimes, crimes targeting computers, and crimes where computers play an incidental role. It describes common cyber-attack tactics employed by cybercriminals and discusses the educational offerings of Samplilearn, particularly their Advanced Executive Program in Cyber security, designed to train and develop the next generation of cyber security professionals.*

Keywords: Cyber, security, Confidentiality, Integrity, Availability, Authentication, Cybercrimes

I. INTRODUCTION

Cyber security is a vital process aimed at safeguarding networks and devices from external threats. Many businesses employ cyber security professionals to secure confidential information, ensure employee productivity, and boost customer trust in their products and services.

The cornerstone of cyber security lies in upholding the industry-standard principles of confidentiality, integrity, and availability (CIA). Confidentiality ensures that data can only be accessed by authorized parties, integrity ensures that information can only be manipulated by authorized users, and availability mandates that systems and data must be accessible as per agreed-upon parameters.

A pivotal element of cyber security involves the implementation of authentication mechanisms. For instance, a username identifies an account that a user seeks to access, while a password serves as a means to verify the user's identity. Types of Cybercrimes Cybercrime encompasses any unauthorized activity involving computers, devices, or networks. These crimes are broadly categorized into computer- assisted crimes, crimes where the computer is the target, and crimes where the computer is incidental to the crime rather than the primary focus.

Cybercriminals often seek to profit from their actions using various tactics, including Denial of Service (DOS) attacks, where a hacker overwhelms a server's resources, making it inaccessible to legitimate users; malware attacks, where victims are affected by harmful software rendering their devices unusable; man-in-the-middle attacks, where a hacker intercepts data packets by positioning themselves between a victim's machine and a router; and phishing attacks, where a hacker sends deceptive emails to trick users into revealing personal information.

Other cyber-attacks include cross-site scripting attacks, password attacks, eavesdropping attacks (which can also be physical), SQL-injection attacks, and birthday attacks based on algorithm functions.

Cyber security Education Simplilearn goes beyond introductory cyber security courses in India by offering a comprehensive Advanced Executive Program in Cyber security, designed to nurture the next generation of cyber security experts.

Cyber security courses encompass training in CompTIA Security+ 501 and Certified Ethical Hacker (CEH), equipping professionals to become adept security testing experts; Certified Information System Security Professional (CISSP) training, which prepares students to become chief information security officers (requiring a minimum of five years of IT security experience); Certified Information System Auditor (CISA) training, focusing on auditing and verifying systems and policies; Certified Information Security Manager (CISM) training, enabling students to manage an organization's daily security through projects; Certified in Risk and Information Systems Control (CRISC) training, which concentrates on assessing risk levels within business processes; and Certified Cloud Security Professional (CSSP) training, providing an architectural overview of cloud technology and security.

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: 6.252
Volume 3, Issue 6, January 2023

All these courses culminate in the Advanced Executive Program in Cyber security, where students learn to design and develop policies and structures to fortify businesses' security infrastructure. If you aspire to become a cyber-security expert, enroll in Simplilearn's courses today to elevate your career.

II. REVIEW OF LITERATURE

A Study Of Cyber Security Challenges And Its Emerging Trends On Latest Technologies, G.Nikhita Reddy, G.J.Ugander Reddy, (2014), stated that 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.

A Literature Review of Cyber Security Pallavi Murghai Goel, 2019, examined that the meanings of both the security of information and ICT. The paper then argued that cyber security is distinct from information security, despite sometimes being used as an equivalent concept for information security. Information security is information defense, which is an advantage, against potential harm resulting from various threats and vulnerabilities. At the other hand, cyber security is not only the defense of cyberspace itself, but also the safety of those operating in cyberspace, and all of their properties that can be accessed via cyberspace. This paper argues that while cyber security and information protection are significantly similar, these two terms are not exactly comparable. In addition, the paper argues that cyber security reaches beyond conventional information security boundaries to include not only the protection of information resources, but also that of other properties, including the individual himself. In information protection, reference to the human factor is generally linked to human's role(s) in the process of protection. In cyber security this aspect has a further element, namely, humans as possible targets of cyber-attacks or even engaging unknowingly in a cyber-assault.

2.1 OBJECTIVES OF THE RESEARCH

- To understand and comprehensive overview of cyber security.
- To encompassing its critical role in safeguarding networks and devices from external threats. The research aims to emphasize the fundamental principles of confidentiality, integrity, and availability (CIA) that serve as the cornerstone of cyber security.

III. RESEARCH METHODOLOGY

The research is based on secondary data. The research data is collected by secondary sources by various books, articles and from internet.

IV. FINDINGS

The text effectively conveys the importance of cybersecurity and outlines various aspects related to cybercrimes and cybersecurity education. Here are some suggestions to enhance and refine the text.

Provide a brief context on the increasing significance of cyber security in today's digital landscape and the ever-evolving nature of cyber threats.

- Principles of CIA: Expand on each principle of Confidentiality, Integrity, and Availability, providing real-world examples to illustrate their importance in cyber security.
- Authentication Mechanisms: Elaborate on various authentication methods beyond just usernames and passwords, including biometrics, two-factor authentication (2FA), and multi-factor authentication (MFA).
- Types of Cybercrimes: Provide a succinct description of each type of cybercrime mentioned, along with statistics or case studies to showcase their impact on individuals and organizations.
- Cyber security Education: Highlight the benefits of pursuing a career in cyber security and how it is a rapidly growing field. Include success stories or testimonials from professionals who have completed cyber security courses.
- Course Offerings by Simplilearn: Briefly describe the key components and unique aspects of each training program offered by Simplilearn, focusing on the practical skills and knowledge participants gain.

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: 6.252
Volume 3, Issue 6, January 2023

By incorporating these suggestions, the text can provide a more comprehensive and engaging overview of cyber security, cybercrimes, and the educational opportunities available at Simplilearn.

V. CONCLUSION

In conclusion, cyber security stands as a critical imperative in modern times, aimed at defending networks and devices against an array of external threats. Businesses recognize the significance of cyber security professionals in securing sensitive information, maintaining productivity, and establishing trust with their clientele. The bedrock of cyber security rests upon the pillars of confidentiality, integrity, and availability (CIA), ensuring data accessibility to authorized entities, preventing unauthorized manipulation, and guaranteeing consistent system availability. Authentication mechanisms, like usernames and passwords, form a pivotal aspect of cyber security, providing a means to verify the identity of users seeking access. Understanding the different types of cybercrimes, ranging from computer-assisted crimes to deliberate targeting of computer systems, sheds light on the evolving tactics employed by cybercriminals to exploit vulnerabilities and gain illicit profits.

Simplilearn, with its Advanced Executive Program in Cyber security, extends beyond introductory cyber security courses, equipping aspiring professionals with the knowledge and skills necessary to combat cyber threats effectively. Covering a spectrum of cyber security courses, from CompTIA Security+ 501 to Certified Cloud Security Professional (CSSP), the program prepares individuals to fortify organizations' security infrastructure and contribute to a safer digital ecosystem. For those aspiring to excel in the realm of cyber security and make a substantial impact, enrolling in Simplilearn's courses represents a proactive step towards elevating their careers and becoming proficient cyber security experts. With the ever-evolving threat landscape, the importance of robust cyber security education and training cannot be overstated.

REFERENCES

[1]. A Study Of Cyber Security Challenges And Its Emerging Trends On Latest Technologies, G.Nikhita Reddy, G. J. Ugander Reddy, (2014),https://www.researchgate.net/publication/260126665.