International Journal of Scientific Research in Science and Technology
Print ISSN: 2395-6011 | Online ISSN: 2395-602X (www.ijsrst.com)
doi : https://doi.org/10.32628/IJSRST229170

Cyber Security : Strategy to Security Challenges A Review

Shruti Rajesh Nistane*, Radhika Rajesh Sharma
CSE, Jawaharlal Darda Institute of Engineering and Technology, Yavatmal, Maharashtra, India

Article Info
Volume 9, Issue 1
Page Number : 316-319

Publication Issue
January-February-2022

Article History
Accepted : 20 Feb 2022
Published : 28 Feb 2022

ABSTRACT

During recent years,the wireless communication and technologies have given rise to many cyber crimes and exploited the cyber security. Cybersecurity is the protection and prevention of internet-connected systems like hardware, software and data from cyberthreats and harms.Cyber security is important for the protection of confidentiality, integrity and availability of information assets. Perhaps the biggest challenge of cyber security is the continuous and immense growth in technology. The paper proposes challenges and issues related to cyber security. Some major challenges are phishing attacks, ransomware attack, IoT attacks and many more.

This paper proposes a framework describing cyber terrorism. So there is need to create awareness about cyber security so that there will be safe and secure environment for users.

Keywords: Confidentiality, Ransomware Attack, Cyber Threat, Integrity, Availability.

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. [1] Earlier, there was a system to send any information via letters, telegrams, etc. This system was quite time consuming and was not reliable. Later on, the development took place by invention of telephone, which helped to communicate from large distances and now there is an era of wireless technology. While doing this information exchange, it is mandatory that your information is to be safe while going through many processes. This implies the main purpose of cyber security. Cyber security is a broad term that has evolved over time with no clear consensus on its exact meaning. [2]

The world is experiencing rapid growth in cyberspace today [3]. Such an extraordinary growth in informationaccess gives opportunities to those with malicious intentions. It is the need of the hour [3] and the act of protecting the systems and technologies from unusual activities. Cyber security means maintaining the Integrity, Confidentiality, and Availability (ICA) of computing assets belonging to an organization or connecting to another organization's network. Due to the evolution and increase of cyber threats, many researchers believed and urged to educate the new generation about the concepts of

cyber-security [4]. Cyber-crimes occur due to negligence in cyber-security and awareness among the clients [5-6]. As stated in the recent research [7], the US has introduced the threat intelligence frameworks. This framework works on the principle of gathering information from various sources which have been carefully examined by human security experts. Besides, researcher also taking aid of machine learning techniques to analyze threats which in advanced way respond to attack incidents[8-9].

Cyber security gives the assurance and guarantees to internet users their communication way/internet is secure and protected against any attack of unauthorized third person.

II. CYBER SECURITY

Cyber security is the set of rules, body of technologies, processes and procedures to protect the electronic data, networks, computers, and programs from any attack and unauthorized access. Cyber security must satisfy three points:

1) Measure amount of data for the protection of information technology.

2) The Level of protection as an outcome from application of those taken measures.

3) The field associated with the professional endeavor. These three aspects of cyber security play a vital role to prevent and secure a personal data of every user of internet, business, and government [10].

Those data are essential because they can be hacked by other person for illegal activities. Various powers oversee the lofty ascent in hostile cyber intrusions and unapproved network breaks. The blast of new advancements and development of societal reliance on allinclusive interconnected innovation, joined with the robotization and commoditization of cyberattack tools, digital aggressor modernity, and low passage hindrances into the cybercrime market 10 are no uncertainty among the key ones [11].

CHALLENGES ON CYBER SECURITY IN INDIA

1) Cyber Terrorism:

There is one more term associated with this topic "Cyber Security", i.e., "cyber terrorism". Cyber terrorism is a way or a path or a mechanism through which an enemy is trying to know all the secrets of any nation and posing the threat to nation"s policy. 'Cyber terrorism is the convergence of terrorism and cyber space. It is generally understood to mean unlawful attacks and threats of attacks against computers, networks, and information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives[12].

Elements of Cyber Terrorism	• Politically-motivated cyber attacks that lead to death or bodily injury; • Cyber attacks that cause fear and/or physical harm through cyber attack techniques; • Serious attacks against critical information infrastructures such as financial, energy, transportation and government operations; • Attacks that disrupt non-essential services are not considered cyber terrorism; and • Attacks that are not primarily focused on monetary gain.

2)Threat to ICT infrastructure:

Means to exploit, distort, disrupt, and destroy information resources range from hacker tools to devices such as electromagnetic weapons; directed energy weapons; HPM (High Power Microwave) or HERF (High Energy Radio Frequency) guns; and electromagnetic pulse (EMP) cannons. The attack against an information infrastructure can be carried out with both physical implements (hammer, backhoe, bomb, HERF, HPM) and cyber-based hacking tools. The same is true for the target: It can be cyber,

consisting for example of information or applications on a network, or physical, such as computers or a telecommunications cable. [13]

3)National cyber security :

There is no way to underestimate the hacker, because the method by which the information is stolen by illegal means is totally out of imagination, as we are ignorant about the ways of stealing information. The changing phase of cyber attacks as well as ever-increasing sophistication of attack methods have complicated the efforts of collecting valuable intelligence information for effective proactive, preventive and protective measures. [14]

4)Human Error or Failure:

A] Phishing:- A form of social engineering in which the attackers provides what appears to be a legal communication, but it contains hinden or embedded code that redirect the reply tp 3rd party side, in an effort to extract personal or confidential information.

B] Ransomware Attacks. C] IOT Threats

III. CONCLUSION

Following comclusions can be drawn from above description :-

1.Internet has become a basic part of life in all over world. There are many advantages and disadvantages. The critical advantage is misuse of internet by criminal persons via unauthorized access and sources. People urges secure and protected platform who use internet. Cyber security gives the facility to internet users access/use the secure and protected source and way. Intranet has a private network used in government organizations and especially in military. It is more secure as compared to local internet but some drawbacks are occurred in this network. Then onion routing and intelligent agents control/protect the all over system by any threats and attacks. The security is the fundamental issue in the versatile specially appointed system [15]

2. The goal of a cyber security is management program is to identify the risks, understand their likelihood and impact on the business, and then put in place security controls that mitigate the risks to a level acceptable to the organization.[16]

3 Cyber security is becoming more and more important as world is highly interconnected with different networks.[17]

4. Protect wireless devices: Personal firewalls can protect individual devices from attacks launched via the “air connection” or from the internet. [18]

IV. REFERENCES

[1]. G.Nikhita Reddy1 , G.J. Ugander Reddy2 , “A study of cyber security challenges and its emergning trends on latest technologies”, 1- 6.

[2]. Some perspectives on cyber security: 2012”, 16 November 2012, 2 – 22.

[3]. BhavnaArora.:Exploring and analyzing Internet crimes and their behaviours. Perspectives in Science. 8(7). 540-542.(2016). DOI: https://doi.org/10.1016/j.pisc.2016.06.014

[4]. Barry M. Lunt, Dale C. Rowe, Joseph J. Ekstrom.: The Role of Cyber-Security in Information Technology Education. In Proceedings of the 2011 Conference on Information Technology Education. ACM, New York, NY, USA 113-122, (2011)

[5]. Bruce Schneier. 2018. Crypto- Gram. https://www.schneier.com/crypto-gram/archives/2018/0615.html#1. AccessedAugust 18, 2018

[6]. EirikAlbrechtsen.:Qualitative Study of Users' View on Information Security. Computers & Security. 26(4).276-289.(2007).DOI: https://doi.org/10.1016/j.cose.2006.11.004.

[7]. ScottE.Jasper.:US Cyber Threat Intelligence Sharing Frameworks. International Journal of Intelligence and Counter Intelligence. 30(1).53-65.(2017).DOI: https://doi.org/10.1080/08850607.2016.1230701.

[8]. Abdallah, A. E., Mahbub, K., Palomar, E., Wagner, T. D.:A Novel Trust Taxonomy for Shared Cyber Threat Intelligence. Security and Communication Networks.2018, Article 9634507. DOI:https:/doi.org/10.1155/2018/9634507.

[9]. 9Emmanuel, S., Thomas, T., Vijayaraghavan, A.P. : Machine Learning and Cybersecurity. Machine Learning Approaches in Cyber Security Analytics. 37-47. 2020. Springer, Singapore. DOI: https://doi.org/10.1007/978-981-15-1706-8_3

[10]. Deibert, R. (2012). Distributed Security as Cyber Strategy: Outlining a Comprehensive Approach for Canada in Cyberspace. Journal of military and strategic studies, 14.

[11]. Weber, R. H., & Studer, E. (2016). Cybersecurity in the Internet of Things: Legal aspects. Computer Law \& Security Review, 32, 715- 728.

[12]. SS Raghav, “cyber security in india's counter terrorism strategy”, 2-5.

[13]. Dr Gulshan Rai, “National Cyber Security Policy”, draft volume 1.0, 6-21, 26 Mar 2011.

[14]. Evgeny Lebanidze Cigital, “NRECA / Cooperative Research Network Smart Grid Demonstration Project Guide to Developing a Cyber Security and Risk Mitigation Plan”, 17-125.

[15]. Li, W., & Joshi, A. (2008). Security issues in mobile ad hoc networks-a survey. Department of Computer Science and Electrical Engineering, University of Maryland, Baltimore County, 1-23.

[16]. G.Nikhita Reddy 1 . G.J. Ugander Reddy2 . "A study of cyber security challenges and its emergning trends on latest technologies", 1-6.

[17]. "Why Cyber Security Is Important", State of Wyoming, Office Of the Chief Information Officer, 2001 Capitol Ave, Rm 237, Cheyenne, WY 82002, 2-2.

[18]. K Yadav, “Conclusions and Future Scope of the Work”, 2012, 3-4.

Cite this article as :

Shruti Rajesh Nistane, Radhika Rajesh Sharma, "Cyber Security : Strategy to Security Challenges A Review", International Journal of Scientific Research in Science and Technology (IJSRST), Online ISSN : 2395-602X, Print ISSN : 2395-6011, Volume 9 Issue 1, pp. 316-319, January-February 2022. Available at doi : https://doi.org/10.32628/IJSRST229170
Journal URL : https://ijsrst.com/IJSRST229170