Cyber Security: Applications in Digital World

Dr.G. Rajitha Devi
Asst.Prof. in Computer Science
Email:rajithareddygurram@gmail.com

Abstract:

Cyber Security is the approach that deals with safe guarding confidential data, computer networks, computer system and software operations from cyber-attacks. A cyber-attack can be described as an atrocious operation which points out the networks of the computer, frameworks of the computer networks and information. This utilizes miscellaneous methods to loot and modify information systems. Cyber security is one of the prominent fields in computer applications like military, medical, financial and also in government and corporate. Cyber Security provides security for the users. In this article, we will discuss some of the cyber security attacks.

Keywords: *Cyber-attacks, Digital services, Information warfare, Nuclear power,*

INTRODUCTION:

There are multiple layers of protection in an outstanding cyber security approach that has scattered across the programs, networks, computers, or data that one plan to secure. In a composition, the technology, people and processes all must accompany one another to set up a powerful defence from cyber-attacks. Indian digital services firm subex reported in EWS18 on August 10, 2019 that India was one among the most attacked nations in IOT space and it recorded a 22 percent attack on IOT deployments in our country. Transportation sectors, financial services and smart cities force the sectoral ranking in the order of attacks said the "State of internet of Things". The study by Bangalore-headquartered telecom solutions revealed that among 15 Indian cities from which data was collected; Bengaluru, Mumbai and New Delhi are inviting the maximum number of cyber-attacks. In this article types of attacks were discussed. In this fast-growing computer age, where our lives cannot be imagined without our electronic devices to perform almost every task in routine life, the security of the information stored in these devices is dubious. The only way to safeguard our private and personal information is by taking proper measures against cybercrime. The top key cyber threats are:

1. "Companies in the crosshairs of information warfare
2. IoT devices broaden state espionage operations
3. The weaponization of adware networks
4. Deep fakes in the wild- AI in information warfare".

 ISBN: 978-93-88808-80-4

Employment of machine learning, installation ransom ware software and the Acknowledgment of the importance of cyber security by several business leaders of many organizations helps us reduce these threats.

Types of Threats

There are a few threats of Information security as confirmed by

(i) Malware

It is malicious software that stops the functioning of the entire system. It is done by the help of some harmful program.

(ii) Social Engineering

The name suggests us that it is the change of behavior of people to indulge in wrong actions with data. The types include Phishing, Baiting, Vishing etc.

(iii) Ransom ware

It is another category of malware from crypto virology that terrorizes the public data and manipulates it or blocks it without their knowledge.

Major domain

The following are the areas of computer security

a. Network Security

It protects the network from being misused by any unauthorised person. Many tools are used to build a network security still alerts go missing.

b. Cloud Security

Cloud is used by almost all the organizations whether big or large. Since all the important data transfers and storage are done there, it must be protected properly. Cloud providers use new tools to safeguard their data.

c. Application Security

Web application security has become the weakest side. The web pages are morphed and used in a wrong way. But latest tools that are emerging help the people to guard their pages and other applications from falling in wrong hands.

d. Infrastructure

It is highly essential to have physical systems that can avoid any wrong access and wrong usage of the system. The upcoming systems are having good infrastructure that is stable enough to handle any situation.

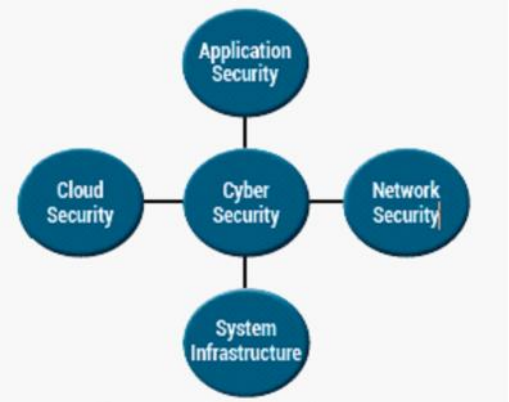

Figure 2: Cyber Security Areas

Applications and Challenges:

Cyber security has wide applications in different sectors of society. Individuals, industries and businesses rely upon cyber security experts to protect their systems from cyber attacks. Financial institutions and banking sector have always been targets for cyber attacks due to multiple reasons. Hackers try to manipulate the market and make profits from it. They usually target websites, applications or servers to fetch sensitive credentials and misuse them. Power grids and nuclear power plants' vulnerabilities may be easily exploited even if they are not connected to the Internet as demonstrated by Stuxnet worm .The aviation sector heavily relies on complex radio communication systems which, if attacked, could cause a worldwide disruption of radio communications which may pose many lives in danger. Personal computers and smart phones store data of individuals which is of great use for hackers who may use this data for fraud financial transactions and may sell in the black market for further misuse. Hackers would bypass multiple sensors like microphones, cameras, GPS navigators, gyroscopes to collect personal health information. These sensors are remotely controlled using WiFi, cellular network or Bluetooth. The home automation devices like voice assistants can also be exploited to obtain sensitive information. These personal use devices are mostly used by vendors selling them to obtain user data in order to understand user behavior for future improvements. This vulnerability may also be exploited that information very easily either by accessing those devices or by fetching the information being sent over the network to the vendors in between. These devices vary from smart phones, smart watches, home assistants to smart vehicles and smart house locks. Along with the personal-use devices, most common targets to fetch sensitive data are the cloud servers, which store data of a particular user for multiple applications using those servers. Many times, hackers have exploited the vulnerabilities of various companies storing user data on the cloud to get the sensitive information. In October 2019, a security researcher hacked into OYO's database to get booking IDs, phone numbers, date of booking and location for multiple users. The health sector has also been the target of cyber attacks in the past. Many times potentially harmful vulnerabilities have

ISBN: 978-93-88808-80-4

been demonstrated in the medical equipments, which are connected over the Internet. DoS and DDoS attacks have been observed on the equipments leading to equipment failure causing disruption in patient care and posing life threats to patients. Hospital computers have been attacked multiple times by ransom ware and other multiple malware either to get the data or to get the ransom. These cyber attacks have caused huge financial loss not only to financial institutions, but also to various other industries. The actual loss is very difficult to be estimated.

CONCLUSION:

The cyber-attacks can be prevented using few ways by identifying the threats, cybercrimes concern and heed, spy on employees, utilization of two faced confirmation and investigating on a regular basis for suspicious activity. Mitigation measures may differ but security remains the same. So, updating databases and devices plays a major role in safe guarding one's data. Thus, this article provides an overall understanding about cyber security attacks and few prevention measures. With the rise and significant developments in the technology, especially the cyber world, users are getting seamless experience to multiple facilities at their doorstep. This cyber world connects people across the globe. But, this also leaves the users open to cyber attacks. If any cyber attack happens, then the ultimate victim is the user itself. User's data safety should be the first priority of the companies. Therefore, various cyber security methods need to be developed or improved for safety of users. System testers should be hired to analyze the systems and remove vulnerabilities from them before making them available to users.

REFERENCES:

[1] https://www.geeksforgeeks.org/session-hijacking/

[2] https : //www. researchgat e .net/publication/285112521_IP_Spoofing

[3] https://www.webopedia.com/TERM/K/keylogger.html

[4] https://searchsecurity.techtarget.com/definition/dictionary-attack

[5] ht t p s : //www.techopedi a .com/definition/18091/brute-force-attacki

[6] What is Cyber security?
https://www.cisco.com/c/en_in/products/security/what-is-cybersecurity.html, Accessed on 16th October 2019.

[7] Cybersecurity, https://searchsecurity.t e c h t a r g e t . c o m / d e f i n i t i o n /cybersecurity, Accessed on 12th October 2019.[3] Backdoor Attack, https://www.imperva.com/learn/application-secur i ty/backdoor-shell-attack/, Accessed on 7th October 2019.

[8] Denial-of-Service Attack, https://searchsecurity.techtarget.com/definition/denial-of-service Accessedon 4th October 2019.