International Journal of Reliable Information and Assurance
Vol.7, No.2 (2019), pp.27-34
http://dx.doi.org/10.21742/ijria.2019.7.2.05

A Detailed Review on Focus Areas of Cyber Security

N. Thirupathi Rao[1] and Debnath Bhattacharyya[2]

Dept. of Computer Science and EngineeringVignan's Institute of Information Technology (A), Visakhapatnam 530049, AP, India
[1]nakkathiru@gmail.com, [2]debnathb@gmail.com

Abstract

Security is one of the most important factor or point to be considered for everyone in their life. Providing security and breaking the security are two important points to be noted for everyone who can be using the gadgets in these days. The other important factor or the point to be considered was the cyber security. The attacks or the collection go data unethically without the knowledge of the user's being stolen. The cases or the issues being under this trap are being increased from time to time and day to day in those days. The data to be stolen will be used for various reasons. Some may be using for money collection and some are using it for anti-social elements and unethical issues. Hence, in the current article an attempt has been made to provide a detailed idea of the types of attacks and types of issues and types of malwares that can be attacked and also some suggestions were provided. The important issues to be focused in the case of cyber security issues are given a thought and the details are given a light on it. The readers of this article can get the basic knowledge about the cyber security issues and threats and the steps to be followed such that to escape from these sorts of attacks. Also a focus was given on various aspects such that to escape from these types of security attacks.

Keywords: *Cyber security, Nodes, Attacks, Hackers, Firewalls, Network, Segmentation, Wireless networks, Wi-Fi, Malware, Phishing*

1. Introduction

Cyber security is one of the recent growing research area that can be sued for the betterment of the internet and applications that can be used through internet [1][2][3]. The major concerned areas where the cyber security that can be used for providing security and safety to the areas like providing security to the internet-based connection type of systems, providing security to the hardware components of the machines, systems, internet-based applications and the software and data being used in various applications for the protection of the systems from attacks from various locations at various attacks. In the current day of the applications that was being used in nowadays are almost all applications are being utilized through internet. All the applications are being using the internet connectivity, it is the major headache was almost all the applications are internet connectivity based applications and the performance by those applications are also internet connectivity based models. Hence all these applications and methods are easy vulnerable for more attacks and can be hacked by various types of people at various locations [2][4][5]. The physical systems and their maintenance and the security tot the data being stored and being used from those machines and servers is providing security is a big

Article history:
Received (June 13, 2019), Review Result (July 25, 2019), Accepted (September 24, 2019)

Print ISSN: 2288-8950, eISSN: 2207-5143 IJRIA

task for the people. Providing access to the users who are authenticate persons and the persons who are unauthenticated persons to be identified and the access should be given to those who are eligible such that the utilization of the machines to be used properly.

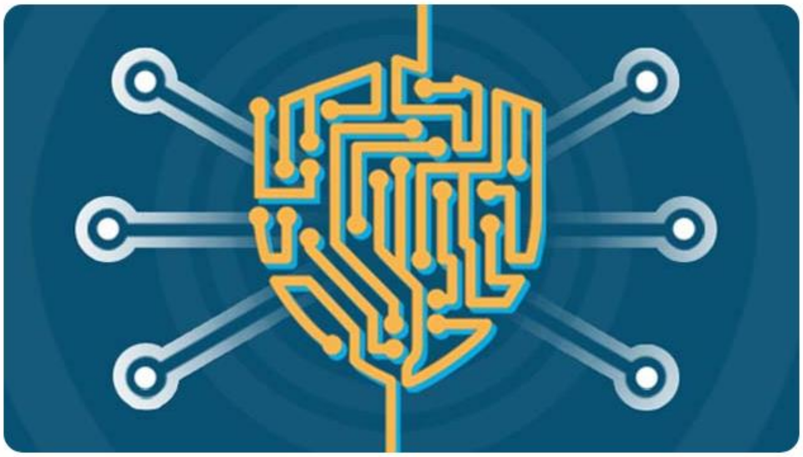

Figure 1. Cyber security model [2]

The major advantage and the major applications and the tasks that the users are getting from the area of this cyber attacks and other related cyber models are the protecting the network and providing security to the networks from cyber attacks [5][6]. In general, the organizations having some confidential and useful data that should not be breached or could be attacked by some other people should have a good cyber people who can protect the system from its attacks and the data can be provided securely from other sorts of attacks.

2. Various modes of cyber security attacks

As the technology is growing day by day, the inventions of new technologies and their applications had been growing day to day and increasing in number from time to time. Several new technologies had been evolving day to day, the new security threats and new security trends have been developing day by day [7][8][9]. Providing security to the devices with these sorts of new trends are making a new and big challenges from time to time to protect the networks and its components from the ever increasing cyber attacks and cyber threats [10]. Some of the important and some type of modes of attacks and their mode of operations are explained in detail as follows,

Malware: It is a line of code being used in a program to affect the components of a program or to damage the content of code in a program like the computer viruses, Trojan horse problems, worms and other spyware models.

Phishing: It is one of most important and most highly used cyber attack s models that are available in the area of fraudulent modes. In the current mode, some emails are sent the users with some interesting data such that the users opens the mail and the harmful content that was entered in the system files and the data stored in the machines will be stored and if that data was important to be hacked and blackmailed. Then based on the demands, the users can clear their system data or on the other hand, the users will leave the data as unwanted data.

Ransomware: The other important type of the attack that a attacker make the other users to worry much. In the current mode of attack, the other attackers will lock some files of the system and make the user cannot access such files from the system even though the user is being using such systems. The relieving from such type of systems is very difficult to escape and can process the data to be unlocked.

Social Attacks and social engineering: The other types of attacks that once the users of the systems needs to worried about were the social attacks or the social engineering attacks. The users can catch or can block some items of the documents or the data that was kept in the social network websites under someone's profiles in Facebook, twitter or some other famous social network websites. In order to release such data, the users may be requested or blackmailed to provide some money otherwise the data will be leaked to some other users or the other types of the users at various locations with various assumptions and various aspirations.

Advantages of Cyber Attacks: By utilizing the features and techniques of cyber security models and other methods will rise a set of advantages also [11]. Some of them can be noted as follows,

- Providing security to the private data and storage of data
- Protecting the websites and the data in website from unauthorized users.
- Protecting the data of the end users.
- Increasing the facility and providing the security to improve the recovery of data from various locations.
- Protecting the business of the customers and owners of the companies and shopping malls and other websites being hosted for various applications.

3. Important focus areas of cyber security

When discussing about the various issues related with the cyber security and its applications will be a good and needed requirement for any users [12]. One should have a clear idea or the clear picture of what are important points to be noted and important factors to be discussed for better understanding and for better processing of the applications providing the required security and in some special cases for more security as per the requirements [13]. When we are studying and interested to know the various aspects of these cyber models, some of the important areas to be considered important and focused are as follows,

3.1. Securely configured and encrypted devices

Whenever a user or a normal person or normal user purchases any electronic gadget that can be utilized with the combination of internet connectivity much care should be taken while using them. The devices should always be run with some secured software's and original operating system software's such that the files and devices cannot be hacked and easily targeted by the hackers [14]. I the people are using the unsecured devices, the data that was being used in the devices are not safe and it can be accessed by any type of person from anywhere of the internet. The devices should always be protective by suign the original software's and applications should always be used from the trusted parties only, not from the untrusted parties. Some of the precautions can be taken while using them are like,

The mobile devices or the gadgets should always be used with proper lock such that the device cannot be opened to any other person without proper credentials. As a result, even if the device was lost, the data cannot be accessed by any other person.

The hard disk of any laptop or any desktop system to be whole encrypted such that the device cannot be accessed or no person can be accessed by any other person for the betterment of the more protection to the users.

All the computers and the laptops and even the mobile phones should have an antivirus such that the unwanted files and unauthorized access to the users and the other users cannot be granted to any other persons such that the security to be made more difficult for others to attack.

3.2. Network components should configure securely

Whenever the users or we are having a network of our within the campus or within the office, the provision of providing security to such network is more important. As we will send and receive the most important concepts and data in such LAN network, if any intruder enters here, the data will be easily hacked and can be used for some other purposes [15]. Hence, providing security to our own networks at our homes or the at offices is also an important task to be considered. The users need to have separate and network and all the components to be used in such networks will have the protection of unauthorized access of entering into the network and at the same time the access of the data in the network. As a result, the users need to have a trusted devices and more secured devices in the networks whenever we are establishing a private network at our premises of our home or at our office premises.

3.3. Logical access controls

Providing security to the users in the network is one of the most important and challenging task to process. When a number of users in the company had given the access to utilize the services from the network with the data stored in servers and from other users too. It is always required to monitor them. Checking and cutting the permission to the users is also not a good ides of termination of access every time. Every employee in the organization needs to have the access that the databases. Hence, the logical application of thought and provision of security was important here. The users will be given unique identification and codes for their identification in the network. Checking of the users from time to time to monitor the utilization of the customers who were not registered with the company, also to monitor the access by providing the passwords to the users with which they cannot be breached by any others and also these passwords cannot be done or noted by any other outside person from outside the network [16]. The passwords should always be more complex and very difficult to estimate them. The combination of alphabets, numbers and special characters may give some important and more complex combination of passwords for the users such that they cannot be broken that much faster and easier. An email alert can be developed and placed in the software such that to identify the persons who are trying to access the wrong passwords or attempting with different types of new passwords from a same location or same ip address and also to identify the same person trying to login with different wrong passwords. All these points and factors to be noted in a detailed manner and can be used for the better usage of the network and for better working of the private network that had developed for our purpose or for our own office purpose.

3.4. Physical access controls

Controlling of access to the persons or the other users to the locations where the mass storage of data servers are located in the office areas or at various locations of the campuses or at various servers at various locations is more important. Once the location of data was known to the common people, the visiting of the people to such places may be more due to the increasing of the thought of looking how these data was stored and hoe that data can be used. Hence, keeping the information regarding such places hiding was one of the best options of providing normal security [14][15][16]. The data in those servers can be protected more securely and if any unauthorized persons enter there, the data can be easily tampered or stolen. Hence, more security needs to be there for such places. The security can be restricting the persons without any proper identification. The persons will be given passwords, eye retina password, fingerprint password and other types of passwords can protect the unauthorized person entry to such places. Security cameras can be placed in such locations such that the persons whoever enter into that area can be tracked. The physical access to such places can be closed and only for those authorized persons can be granted permission to enter at various intervals of time for more security.

3.5. Online and email protection

In recent days, most of the attacks on cyber-based were taking place through email only. The data that will be embedded in the body of the email and the subject will be kept as some interesting and the people who don't these sort of ideas will open the mail and the content in the body of the mail will be entered in to the system and all files in the system will be corrupted and the data can be accessed by the all other persons. Once this thing happened, the hackers can be daily accessing the person mail details, his personal details and also all the data that he is receiving from all the sources [16]. Hence, it is always better for the public to not to open the mails which were not known to us or which will be looked like the phishing emails. The utilization of browsers also plays a key role in utilizing the browser for accessing the internet. The latest developed browsers are somehow good browsers that they are continuing with some good software in them and also to protect the users from phishing emails.

The browsers also having some extensions that may not be opened by the browsers in recent days and also the Google Gmail is also providing some options like the trash where the new and never opened or never used websites or the mails cannot be opened directly or cannot be shown to the users directly in the mails inbox and will be shown at the trash data mails. In some cases, the mails that were shifted to the trash will be always considered to be the new mails and are most of the cases not related to the users whoever is using the current mails. Hence, it is always better for the users not to open the mails which were not related our profession, our interests or our education or our job or our shopping related issues.

3.6. Backup and data recovery

The other important factor or the point to be considered and kept in mind when we are working on the systems with large databases and other important data points. The data to be used for these points are very important especially for those companies which were working on the analysis of data and reaching to the public for various purposes. The data stored in social networking websites and public related organizations working with the data of the public is also important. In order to escape from these sorts of attackers and the loss of huge important data, it is always better to take some backup of data from time to time. Not only is the collection of data from time to time, but also keeping such data from unauthorized personae utilizations also important [9][10]. Hence, it is always suggested to store the same data copies at various locations simultaneously such that data loss at one location may be recovered from other locations.

The utilization of data and storing it at various locations of the servers is always a better choice. Taking the count of data space form remote servers from cloud applications and storing them at various locations can reduce the hassle-free for the users. Hence, the storage of data at various locations at various remote sources will give a better utilization and better protection to the data. If due to some other issues, if the data was lost at one point of location, the data from the other point of locations can be accessed and can be utilized by other sources at various times at various locations.

3.7. Wireless security

The other way of receiving the threats of unauthorized access of data and creating unnecessary issues was the utilization of the wireless connectivity to the customers or the visitors who were entering as guests as wireless connectivity like the Wi-Fi. The persons can access the connection and also can access the data from the internal servers through this facility too. Hence, it is always suggested to separate the users in tot two categories. The internal staff and other staff related to the particular office or particular company and the other visitors or the guests in to two separate lists and separate network. The provision of others using Wi-Fi network was separated and the list of customers can use be separated and the company staff can use one network and the other people or the visitors can use the other network which was separated and cannot be connected with any other important servers or any other important devices in the inside company’s servers [4][5].

3.8. Network segmentation

In order to provide the network of an institution or a company is always a challenging task. Several researchers had proposed several methods to follows such that to avoid such attacks on the networks of the companies or the institutes. The other important model or the idea that was suggested in order to provide a full security to the networks was the segmentation of the network. In the process of keeping an entire network in to a single group and identifying the errors or mistakes in the network and also difficult to identify the place or the node where the intruder had entered and the data was being stolen or creating some unethical issues in the network [6][7][8].

In order to overcome such issues, the splitting of the big data network into small pieces of the network and each single piece of network some little number of nodes such that the network can be easily managed and easily identified the number of nodes and the data being accessed by the nodes present in the each single small networks and also easy to track the users whoever connected with these small set of networks such that to process these small networks. Moreover, the best move was to identifying of the intruders and the data being stolen also can be identified easily and the users also identified. If any issues will happen in the network point or in a small segmented network, immediately the managers or the administrators or the network admin can easily identify the problems in the particular small network segment and can be easily controlled the access or in some other times the access can be cut easily.

4. Conclusion

The problems with the cyber security and its related areas are growing day by day in the society. The number of people being cheated or being made useless and being stolen of data is being increasing day to day in the society. The number of people being cheated are increasing a lot and the precautions can be taken or followed such that to save themselves. Hence, in the current article an attempt has been made to provide detailed issues to be focused on cyber security while we are using some mobile phones or laptops or some other electronic gadgets. The more precautions to be taken while we are using the mobile phones due to the reason that most of the personnel data is being stored in the mobile phones in recent days. By reading or studying the current article, he users of these electronic gadgets can get the better overview of the usage of these devices while having a thought and idea on cyber attacks.

References

[1] PROTECH, https://www.psgi.net/news/posts/10-focus-areas-for-cyber-security, **(2019)**

[2] CISCO, Cybersecurity, https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html, **(2019)**

[3] Yu Jun, Kuang Zhenzhong, Zhang Baopeng, Zhang Wei, and Lin Dan "Leveraging content sensitiveness and user trustworthiness to recommend fine-grained privacy settings for social image sharing," IEEE Transactions on Information Forensics and Security, 2018, vol.13, no.5, pp.1317-1332, **(2018)** DOI: 10.1109/TIFS.2017.2787986

[4] Yu Jun, Tao Dapeng, Li Jonathan, and Cheng Jun "Semantic preserving distance metric learning and applications," Information Sciences, vol.281, pp.674-686, **(2014)** DOI: 10.1016/j.ins.2014.01.025

[5] Yu Jun, Yang Xiaokang, Gao Fei, and Tao Dacheng, "Deep multimodal distance metric learning using click constraints for image ranking," IEEE Transactions on Cybernetics, vol.47, no.12, pp.4014-4024, **(2017)** DOI: 10.1109/TCYB.2016.2591583

[6] Yu Jun, Zhang Baopeng, Kuang Zhengzhong, Lin Dan, and Fan Jianping, "iPrivacy: Image privacy protection by identifying sensitive objects via deep multi-task learning," IEEE Transactions on Information Forensics and Security, vol.12, no.5, pp.1005-1016, **(2017)** DOI: 10.1109/TIFS.2016.2636090

[7] Jia Gangyong, Han Guangjie, Jiang Jinfang, and Li Aohan, "Dynamic time-slice scaling for addressing OS problems incurred by main memory DVFS in intelligent system," Mobile Networks & Applications, vol.20, no.2, pp.157-168, **(2015)** DOI: 10.1007/s11036-015-0587-2

[8] Jia Gangyong, Han Guangjie, Wang Hao, and Wang Feng, "Cost aware cache replacement policy in shared last-level cache for hybrid memory-based fog computing," Enterprise Information Systems, vol.12, no.4, pp.435-451, **(2018)** DOI: 10.1080/17517575.2017.1295321

[9] Jiang Congfeng, Duan Liangcheng, Liu Chunlei, Wan Jian, and Zhou LI. "VRAA: Virtualized resource auction and allocation based on incentive and penalty," Cluster Computing-The Journal of Networks Software Tools and Applications, vol.16, no.4, pp.639-650, **(2013)** DOI:10.1007/s10586-012-0235-6

[10] Jin Wang, Xiujian Gu, Wei Liu, Arun Kumar Sangaiah, and Hye-Jin Kim, "An empower Hamilton loop based data collection algorithm with mobile agent for WSNs," Human-centric Computing and Information Sciences, vol.9, no.18, December, **(2019)** DOI:10.1186/s13673-019-0179-4

[11] Jin Wang, Yu Gao, Kai Wang , Arun Kumar Sangaiah, and Se-Jung Lim, "An affinity propagation based self-adaptive clustering method for wireless sensor networks," Sensors, vol.19, no.11, pp.2579, **(2019)** DOI:10.3390/s19112579

[12] Ruxia Sun, Lingfeng Shi, Chunyong Yin, and Jin Wang, "An improved method in deep packet inspection based on regular expression," Journal of Supercomputing, vol.75, no.6, pp.3317-3333, **(2019)**

[13] Chunyong Yin, Jinwen Xi, Ruxia Sun, and Jin Wang, "Location privacy protection based on differential privacy strategy for big data in industrial Internet of Things," IEEE Transactions on Industrial Informatics, Aug 2018, vol.14, no.8, pp.3628-3636, **(2018)** DOI: 10.1109/TII.2017.2773646

[14] Yuyu Yin, Yueshen Xu, Wenting Xu, Min Gao, Lifeng Yu, and Yujie Pei, "Collaborative service selection via ensemble learning in mixed mobile network environments," Entropy, vol.19, no.7, pp.358, **(2017)**

[15] Yuyu Yin, Wenting Xu, Yueshen Xu, He Li, and LifengYu, "Collaborative QoS prediction for mobile service with data filtering and slopeone model," Mobile Information Systems, vol.2017, article no.7356213, pp.1-14, **(2017)** DOI: 10.1155/2017/7356213

[16] Jia Gangyong, Han Guangjie, Jiang Jinfang, and Li Aohan, "Dynamic time-slice scaling for addressing OS problems incurred by main memory DVFS in intelligent system," Mobile Networks & Applications, vol.20, no.2, pp.157-168, **(2015)** DOI: 10.1007/s11036-015-0587-2

This page is empty by intention.