Scholarly Research Journal for Humanity Science & English Language,
Online ISSN 2348-3083, SJ IMPACT FACTOR 2019: 6.251, www.srjis.com
PEER REVIEWED & REFEREED JOURNAL, FEB-MAR, 2021, VOL-9/44

CYBER SECURITY AND CYBER THREATS

Devansh Bansal

Department of Computer Science and Engineering, Chandigarh Engineering College Landran, India. Email Id: bansal.devansh87@gmail.com

Paper Received On: 25 MAR 2021

Peer Reviewed On: 30 MAR 2021

Published On: 1 APRIL 2021

Content Originality & Unique: 85%

Abstract

Cyber security in the IT world refers to the protection of data which could be present either on personal devices or the cloud from being leaked or shared that could lead to financial loss to the individual or an organisation. With the technology advancement the number of attacks on the organisations have increased drastically which has made the study of cybersecurity quite important nowadays. The data which is present on the internet is quite vulnerable which often results in the information being compromised. Various challenges are faced by the IT industries in order to protect the data of the employees and the data of the organisation. Challenges are in the form of data security, automotive security, internet security, mobile security and biometric authentication. A brief elaboration on each is discussed below in the paper. Cyber attacks are done basically for two reasons, the former being to gain money by laundering the information and the later is for the revenge for an individual. Hackers are the professionals who perform the attacks. Some common cyber threats are adware, spyware, phishing, etc. whose description is given below in the 'Cyber-attacks' section. Moreover, this paper states some practices that will be helpful to reduce data breaches or other cyber threats. If these practices are followed then data can be prevented from exploitation.

***Keywords** : Cyber Security, Cyber threat, Ransomware*

I. INTRODUCTION

The Internet has revolutionised the world which has made the accessibility of information really easy and from any anywhere. But this has resulted in the new area of study which is basically protection of this data which is present on our devices and over the internet. The study is known as Cyber Security. The term itself states its meaning which is the security of cyber networks. Cyber attacks have increased manifolds which mainly aims to steal information from the hosts using various techniques. Everything is automated in present world which makes cyber security the latest issue.

All the compliance policies of the system should be met in order to minimize the data loss. We all know the importance of data for any organisation and the breach of sensitive information could incur financial losses to a organisation. Thus, the importance of protection of this data is self explanatory.

II. CHALLENGES OF CYBER SECURITY

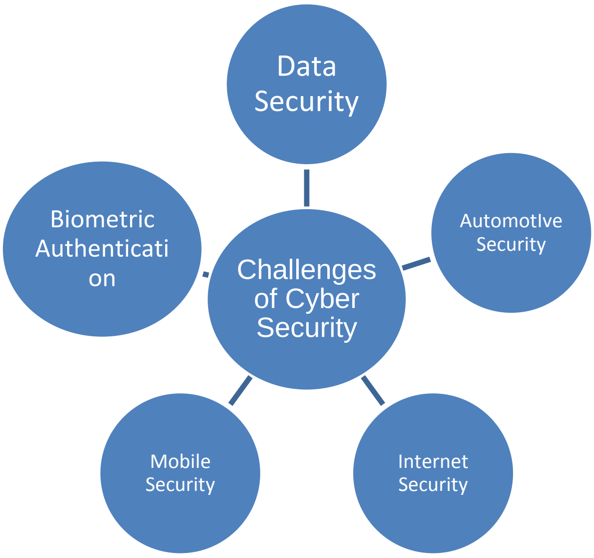

Fig1: Depicts challenges to Cybersecurity

.[1] Today more than 80% of total commercial transactions are done online, So a bigger challenge is faced by professionals in order to secure sensitive information from being leaked.

Data Security: The increasing abuse of computers and growing threat to personal privacy through data banks have triggered much interest in the technical safeguards for data. The main purpose for data security is to safeguard the data from unauthorized access.[2]Organisations around the globe spend hefty amounts to protect the data. Data encryption and Data Loss prevention policies are applied on the systems to prevent the data loss.

Automotive Security: Recent advancements has led to inculcation of technology into the automobile sector. Modern cars are made with microprocessors, electronic control units and designed using software codes. The ECU's are thus vulnerable and they act as a target for hackers which leads to the vehicle being compromised. The attacks in the particular area target the functions of the vehicle like the breaking system and the steering system of the same and could also steel the GPS information which could tell about the whereabouts of the individuals. Harder protocols needs to be enforced by the manufacturer to encounter this type of challenge.

Internet Security: Internet Security is often thought to be related only to internet but on the contrary it represents a broader aspect including browser security and network security as a whole.[3] The art and science of cryptography and its role in providing confidentiality, integrity, and authentication is also a part of Internet security. It is regarded as the main source of virus in the systems as the malicious softwares from the internet can be used to gain access of system.

Ransomware is a threat in which [4] person has to pay ransom to decrypt the files that were decrypted by the hacker. This threat is the main issue faced by organisations. Firewalls and antivirus software's can be deployed into the environments as to protect them from hackers. The antivirus software need to be updated as it is updated with the signatures on a regular basis.

Mobile Security: The world of mobiles and telecommunications has had a great growth in the market.[5] Mobile devices are the new and the latest target of the hackers. Mobile security refers to the protection of our smartphones and tablets. Nowadays mobiles have almost replaced the laptops, all the functions can easily be performed by this device. Thus, the protection of smartphones is becoming really important as it contains all the business related information of an individual. Malicious links that are present on the social networking sites pose a great threat to the mobiles as they are a source of virus. User awareness can play a major role in protecting the device from such links.

Biometric Authentication: This was developed as a security measure but is seen as a critical problem. Biometric authentication means to identify an invidual by the biological traits. Although biometric authentication is quite secure but it has certain cons too.

The setup cost is high and if the system is compromised a new setup has to be deployed immediately. Biometrics work on the principal of partial information in order to authenticate the user which results in false positives.

III. CYBER THREATS

A Cyber threat is regarded as a malicious act to seek or destroy the data which is important to an organisation. Data breaches and virus attacks are the most common cyber threats.

We shall now discuss the various types of cyber threats that could be present in our environment and pose a problem for the same:

A. **Malware:** It is a code that is written by professionals that is present in software's, it is basically design to

damage computer, server or the entire network. Malware is quite a generic term for various viruses. It contains:

- **Spyware:** It is a software that will be [6] installed on the system to keep a check or spy the activities and finally the data is shared to the person who will be willing to pay for it. It does not harm the computer but leaks the activities performed by the individual.
- **Adware:** They are the programs that affect the working of a person by delivering unwanted advertisements while working [11]. This in turns consumes high bandwidth of the connection and thus slows down the system. It is basically meant to slow down the work which was being carried out.
- **Worms:** They are the malicious program that are designed to cause damage to data and files on the computer. It is basically a self-replicating program that keeps on self-replicating and eats the entire disk memory. The worms will not stop copying itself until and unless the entire space on the disk is filled.
- **Trojan Horses**: A Trojan horse is a smart kind of virus, it looks like a legitimate software (any utility program) but is actually a malicious software. It looks completely harmless on the outside but is capable of taking the entire access of the system.

B. **Denial of Service (DOS) Attack:** A Denial of Service attack is used to target the users by making the resource completely unavailable by flooding the traffic on the particular website. This basically results in the website completely inaccessible to the user. A attack on wide level in which not only a single user nut multiple user across different locations are targeted is a Distributed Denial of Service Attack.

Although no sensitive information is leaked in the attack but it can cause a great deal of time and money to the particular user[10].

C. **Phishing and Pharming:** In Phishing, the attacker poses as a legitimate looking website which tricks the user into giving out sensitive information that could lead to data breach or an online transaction. Phishing is basically fooling the target user to give out sensitive information with the help of authentic looking website.

Pharming is a way in which the users are redirected to bogus website with the help of a legitimate looking URL. Through pharming attack, the attacked points out to an illegitimate website via legitimate looking URL.

D. **Ransomware:** Ransomware is a malicious program that can encrypt the files that are present on the computer. It further displays a message to pay the ransom in order to decrypt the files and the mode of payment is usually in the form of cryptocurrency. This particular malware refers to the money making scheme and the program could be installed into the system with the help of malicious links that look legitimate.

After the ransom is paid the data is decrypted by the key which is provided by the hackers.

Ransom attacks have increased to a great extent and money has been extorted from the users.

[5]Fig: This figure completely explains that user has to pay ransom for decryption

IV. Cyber Security Techniques

A. **Encryption:** It is a way of encoding the data which can be decoded only by a key[9]. In such a case even if the data is being leaked it is rendered useless as it cannot be decoded. It is a protective measure that is being used in many organisations

B. **Setting up Firewalls**: Firewalls acts as barrier between the computer and the Internet. They are basically designed to prevent the unauthorized access to or from a private network which in turn protects us from malware. [7]The rules for the firewalls must be configured according to needs of the organisation. The firewalls should be updated in order to be completely effective.

C. **Access Control**: It is assigning user their roles and the data which is accessible for each role. It thus helps in maintaining a hierarchy and the visibility of data. Authentication is a way to verify the credentials of a person which means that the person is who he claims to be. Authorisation is a way in which it is decided whether that particular person has the clearance for that particular data.

D. **Keeping the Systems and Software upto Date:** Often cyber attacks takes place in an organisation due to the outdated versions of software or the operating system. Usually the loopholes which are present in the previous versions are updated in the current one which leaves no chance with the hackers to invade the system.

E. **Enforce a Strong Password Policy:** Strong passwords are very important and play an important role in protecting the employee information. Password must be updated at regular intervals. Multi factor authorization should be practised. To ensure a strong password a password policy must be set by the organisation.

F. **Installing Antivirus**: Antivirus is to detect and delete the malware that could be present into our system. The [8]Antivirus programs are regularly updated with signatures that helps them to detect the potential virus and thus clean the system. Regular full system scans can help us keep the devices protected from viruses.

V. CONCLUSION

Due to the advancements in the field of IT and the automated process the working of machines is on the rise which makes Cyber Security a very important aspect. Numerous cyber attacks are being carried out daily to compromise data thus making the practices of security very essential. No absolute measure or a solution has been designed yet to counter all the attacks but still as preventive measure the above practices should be followed in order to minimize the damage.

References

Atul M. Tonge , Suraj S. Kasture , Surbhi R. Chaudhari, "Cyber security: challenges for society-literature review"

L. M. Kaufman, "Data Security in the World of Cloud Computing," in IEEE Security & Privacy, *vol. 7, no. 4, pp. 61-64, July-Aug. 2009, doi: 10.1109/MSP.2009.87.*

G. A. Marin, "Network security basics," in IEEE Security & Privacy, *vol. 3, no. 6, pp. 68-72, Nov.-Dec. 2005, doi: 10.1109/MSP.2005.153*

Savita Mohurle , Manisha Patil , "A brief study of Wannacry Threat: Ransomware Attack 2017", in International Journal of Advanced Research in Computer Science, Volume 8, No. 5, May-June 2017

N. Leavitt, "Mobile Security: Finally a Serious Problem?," in Computer, *vol. 44, no. 6, pp. 11-14, June 2011, doi: 10.1109/MC.2011.184.*

[6] Kirda, E., Kruegel, C., Banks, G., Vigna, G. and Kemmerer, R., 2006, August. Behavior-based Spyware Detection. In Usenix Security Symposium (p. 694).

E. S. Al-Shaer and H. H. Hamed, "Modeling and Management of Firewall Policies," in IEEE Transactions on Network and Service Management, *vol. 1, no. 1, pp. 2-10, April 2004, doi: 10.1109/TNSM.2004.4623689.*

A. Badhusha, S. Buhari, S. Junaidu and M. Saleem, "Automatic signature files update in antivirus software using active packets," Proceedings ACS/IEEE International Conference on Computer Systems and Applications, *Beirut, Lebanon, 2001, pp. 457-460, doi: 10.1109/AICCSA.2001.934043.*

Boneh, D., Sahai, A., & Waters, B. (2011, March). Functional encryption: Definitions and challenges. In Theory of Cryptography Conference (pp. 253-273). Springer, Berlin, Heidelberg.

Mahjabin, Tasnuva, et al. "A survey of distributed denial-of-service attack, prevention, and mitigation techniques." International Journal of Distributed Sensor Networks 13.12 (2017): 1550147717741463.

J. Gao, L. Li, P. Kong, T. F. Bissyandé and J. Klein, "Should You Consider Adware as Malware in Your Study?," 2019 IEEE 26th International Conference on Software Analysis, Evolution and Reengineering (SANER), *Hangzhou, China, 2019, pp. 604-608, doi: 10.1109/SANER.2019.8668010.*