CGC International Journal of Contemporary Technology and Research
ISSN: 2582-0486 (online) Vol.-3, Issue-1 DOI: 10.46860/cgcijctr.2020.12.26.154

A Study of Cyber Security and Cyber Threats

Khushpreet Kaur*
Department of Computer Science and Engineering,
Chandigarh Engineering College Landran, India
Email Id: *khushilochb@gmail.com

Abstract: **Cybersecurity has a vital role in Information Technology. The cybersecurity security involves the security on data/information stored in various devices present on different networks. However, it is very difficult to secure information in today's world because of the increasing number of devices like computer systems, mobile phones, televisions, etc. for technological development. The data can be in many forms like data of employees in the organization, an individual's data present on a social media website, the data stored in mobile devices or on the cloud. This data is stored mostly on networks including the company's websites, servers, the cloud which is the main reason for data to be hacked. Numerous cyber threats are increasing day by day and to ensure cybersecurity and privacy of internet users various challenges have been faced by IT industries. Those challenges include data security, mobile security, network security, Application Security, Biometric authentication. The elaboration of these cybersecurity challenges and cyberattacks will be discussed in this paper. Cyber attacks are not only harmful to organizations, but it is also dangerous for individuals. Those attacks are the attacks done by cyber attackers for their advantage or to harm individuals for their revenge. Some common cyber threats are phishing, ransomware attack, malware, etc. whose description is given below in the 'Types of cyber-attacks' section. Moreover, this paper includes cybersecurity techniques that will be helpful to reduce data breaches, identity theft, or other cyber threats. Awareness of those cyber techniques will help both individuals and organizations to protect their information from various types of cyberattacks.**

Indexed Terms- **Cybersecurity, Phishing, antivirus, cyber threats, malware (*Keywords*)**

I. INTRODUCTION

Cybersecurity plays a significant role in Information Technology. It consists of two keywords that are cyber and security. The word cyber means technology of networks and machines which consists of information while security means protection of that information present in systems or on the internet. In other words, the activity of safeguarding devices, networks, and applications from automated threats in cybersecurity. Typically, these cyberattacks are targeted at acquiring, manipulating, or damaging confidential information, extorting user's money; or disrupting regular business processes. It is especially difficult today to enforce successful cybersecurity policies because there are more machines than individuals, and attackers are getting more creative,

Cybersecurity is necessary because cyberattacks are dangerous for everyone whether organizations, individuals, employees, or consumers. Cybersecurity is important because a huge amount of data is used by a number of organizations in various ways like for storing and processing. The various cyber attacks which are a threat to computer users are identity theft, spoofing and cyber stalking.[7] In cyber world, it is difficult to capture the cyber criminals than in the physical world which is the main reason of increase in cyber crimes.[1] Unauthorized access to that kind of data that has been used by corporations may have detrimental implications.

II. CHALLENGES OF CYBER SECURITY

To ensure security and safety over networks, the organisations face various challenges which are listed below. It is not only a challenge for organisation but also to individuals, political groups and terrorist organisations[2].

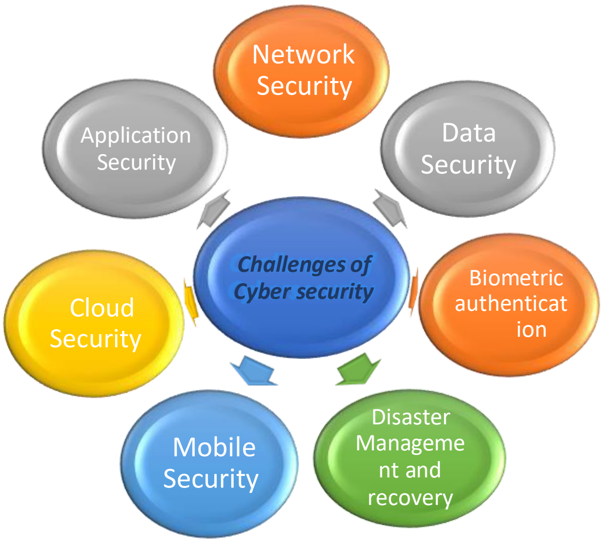

FIG 1: Challenges of Cybersecurity

A. Network Security: A network's security protects a business against unauthorized access and privacy violations. Better security over a network can also detect and destroy internal device threats as well. Some compromises and trade-offs are often necessary for the successful implementation of network security.[3] For Example, Extra logins help ensure data security of business from unauthorized access, but they also slow down the productivity of the company. One of network security's big concerns is that it uses a lot of company resources. A huge amount of data is generated by network security tools because of which there are chances that security threats can be ignored or be slipped. Machine learning is also used by IT teams for the automatic detection of security threats so that human errors can be reduced. However, it cannot be a perfect system

B. Application Security: Most of those best recent hackers think the weakest point in targeting an enterprise is web application security[6]. Because of the proliferation of new partnerships with software companies that are not yet fully vetted and protected, it is impossible to keep up with them. Security for apps begins with great code, which is often difficult to find. Penetration checking and fuzzing are the two other security activities any organization can start adopting now after achieving safe coding practices.

C. Data Security: In every sector, a huge amount of data is stored for various purposes like employee data which includes confidential information, transaction details, etc. Security should be provided to these types of data so that hackers cannot misuse it. Data loss prevention consists of designing policies and procedures for the handling and prevention of data loss and, in the case of a cybersecurity breach, implementing recovery policies. This includes setting data access network permissions and regulations.

D. Biometric authentication: As a revolutionary cyber protection approach, biometric authentication is gaining more and more attention. Although some people see biometrics as a modern and successful way to incre[ase corporate protection, others see it as a critical problem. There are several forms of biometrics-based authentications: common fingertip scans to identify a more innovative speech, iris, or face. Many people assume that it is almost difficult to compromise biometric systems- the data should not be guessed and every individual is unique. Therefore, it seems to be a stronger option for single-factor authentication and a perfect complement to a scheme for multi-factor authentication. Biometric devices have their limitations, however. A big concern is that much like a user's username and password, biometric information can still be stolen or accessed. However, the user cannot change the scans of their iris or have a new face, unlike a password. This poses new problems in the future for cybersecurity experts.

E. *Cloud Security*: Many companies arenot yet ready to place their information on the cloud and prefer to be reserved until it is assured that a cloud is a secure place to put the information. The reason is that those organizations store information on their own private networks where their data is secure as compared to the cloud because the data is placed on public networks in cloud storage which can lead to a cyber-threat. Some issues that lead to cloud attacks are insecure APIs, Cloud misconfigurations, and loss of data by human error or through natural disasters[4].

F. *Mobile Security*: We can communicate with everybody in every part of the world today. Yet security is a very major problem for these mobile networks. Firewalls and other authentication mechanisms are becoming porous these days when individuals use gadgets such as laptops, computers, PCs, etc. all of which again require additional securities other than those found in the software used[11]. We must almost always worry about these mobile network's protection issues. Mobile security must be taken care of because these mobile networks are being particularly attacked in the cyber world.

G. *Disaster Management and Recovery*: Disaster recovery and enterprise continuity which is also one of the challenges of cybersecurity describe how an enterprise reacts to an occurrence in cybercrime or some other circumstances that allow processes or data to be destroyed. The policies of data recovery are required to gain the access to the records and activities in case of disaster incidents because these policies of the organizations determine the recovery process of data.

III. TYPES OF CYBER THREATS

There are two types of attackers in the cyber world: Internal and External. Internal attacker is the one having authorized access to the data however external attacker is someone who is unauthorized user.[9] Different types of security threats which are harmful to organizations are given below:

A. *Phishing*: It is an attack in which the focus of attackers is to steal information like passwords or credit card details[5]. This can be done via sending links in email or through text messages from the person who can the user think of as a trustworthy person and fools the user to open that link. It can cause disclosure of sensitive information; malware installation or system freeze for a ransomware attack. It is the sort of cyber attack that is most widespread. This violation may have devastating consequences. For an individual, this means identity fraud, theft of money, or illegal transactions[10]. There are two types of phishing attacks: spear-phishing and whale phishing. These attacks mainly differ in the targeted users where spear phishing is the email attack on a particular individual in the organization while in whale attack the targeted user is of a high profile like the company's CEO or CFO.

A ***Ransomware***: It is a kind of security threat in which the operating system access is blocked by attackers and bitcoins are requested for accessing the system. Locky, Petya, WannaCry, and CryptoLocker are some of the most dangerous ransomware threats. [8] These threats can be installed in the system by installing infected application or software, by clicking on untrusted URL links, by downloading or opening a malicious attachment in the spam email, or by visiting a malicious website.

B ***Ransomware:*** It is a kind of security threat in which the operating system access is blocked by attackers and bitcoins are requested for accessing the system. Locky, Petya, WannaCry, and CryptoLocker are some of the most dangerous ransomware threats. These threats can be installed in the system by installing infected application or software, by clicking on untrusted URL links, by downloading or opening a malicious attachment in the spam email, or by visiting a malicious website.

C ***Denial Of Service (DOS) Attack***: It is the attack in which the network gets shut down and becomes inaccessible.[1]In this denial of service attack the device is flooded with requests until the device becomes incapable to handle the regular traffic.[8]

D ***Malware:*** It is a software or a piece of code thatis developed by the attackers. There are various ways a virus can attack like while software or application installations, using infected storage devices, or by clicking on the URL link in spam emails, etc. The different types of malware attacks include computer viruses, Trojan horses, worms, spyware.

a. *Computer viruses and worms*: Virus is a program that can be transmitted via a network or from machine to machine without the awareness of user and can cause malicious attacks [8]. It can corrupt the confidential data of the companies [8]. The organization's files can also be deleted,and hard disks can be formatted through virus attack.

However, worms attack the machines or networks that are self-controlled. These are mainly spread through the attachments in the emails and gets triggered when it is opened [9].

b. *Trojan horses*: It is named after the ancient Greek Trojan Horse; the Trojan is a form of malware that enters an intended system that looks like one thing, such as a basic piece of software, but then inserts the malicious code inside the host machine once[10]. Trojans are known to be one of the most threatening forms of malware because they are mostly meant to steal financial data.

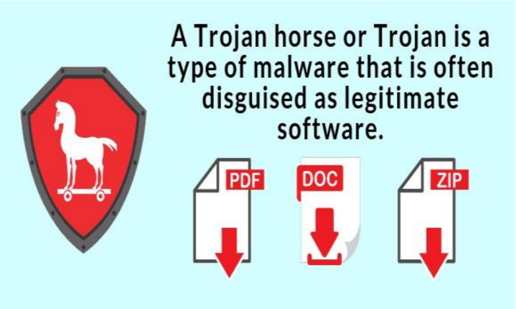
A Trojan horse or Trojan is a type of malware that is often disguised as legitimate software.
PDF
DOC
ZIP

FIG 2: How Trojan horse looks [12]

c. *Spyware*: Spyware is a form of software installed to capture user data, their devices, or their browsing habits[9]. All browsing records are sent to the attackers without the awareness of the user. Other malicious applications can also be downloaded from the internet and installed by spyware.

IV. CYBER SECURITY TECHNIQUES

A. *By encrypting data*: Data encryption gives your business an advantage when the knowledge falls into the wrong hands because even if a hacker sniffs it out, it becomes worthless so it's not that easy to crack through the encryption currently on the market these days.

B. *By authentication of data*: Before downloading, the files we obtain must always be authenticated whether they have come from a reputable and reliable source and also, they are not modified[12]. The anti-virus software present in the systems typically performs authentication of these records.

C. *Continuously backing-up data*: This will help to safeguard against ransomware that blocks computer files before monetary demands are met by the attacker [13]. In this case, backing up of data will be helpful if your machines or servers are locked and you do not have to pay for access to your files.

D. *Using a firewall for protection over the network*: It is necessary to prevent unauthorized traffic from accessing the network by using a firewall, as malware may spread by means other than email. With the use of a firewall, all the messages are reviewed and those which are not meeting the specific security requirements are removed[12]. For users who use company machines away from corporate network security, such as home PCs or laptops, you can add a personal firewall to assure that the device is secure.

E. *Installing Anti-virus software and keeping it up to date*: The use of antivirus software is to detect, delete or disable malicious software, viruses or worms. [12] There is an automatic upgrade option for many antivirus programs which is helpful in downloading new viruses so that the new viruses can be checked as soon as identified. On any device, anti-virus software is a necessary and fundamental requirement[12].

V. CONCLUSION

Cybersecurity is a topic that is more and more important because of emerging technologies with a number of devices. As there are numerous cyberattacks cybersecurity is a must for each and everyone who is using cyberspace. However, the perfect solution does not exist for cybercrimes, but we can try the above- mentioned solutions to minimize cyber attacks in order to make cyberspace a safe and secure place

REFERENCES

[1] Zhang, Y., Xiao, Y., Ghaboosi, K., Zhang, J., & Deng, H,"A survey of cyber crimes", Security and Communication Networks: https://doi.org/10.1002/sec.331,pp-422–437, 2011

[2] S. Z. Sajal, I. Jahan and K. E. Nygard, "A Survey on Cyber Security Threats and Challenges in Modem Society," 2019 IEEE International Conference on Electro Information Technology (EIT): doi: 10.1109/EIT.2019.8833829., pp. 525-528, USA, 2019

[3] X. Li and H. Zhao, "Network security situation assessment based on HMM-MPGA," in Proceedings of 2016 2nd International Conference on Information Management (ICIM),pp. 57-63, London, UK, May 2016

[4] Katmore, I., Cyber Security Challenges: EDUCBA,https://www.educba.com/cyber-security-challenges/, (2020, September 29)

[5] HR, M., MV, A., S, G. et al, "Development of anti-phishing browser based on random forest and rule of extraction framework"Cybersecur 3, 20 (2020). https://doi.org/10.1186/s42400-020-00059-1

[6] Lin, Herbert & Spector, Alfred & Neumann, Peter & Goodman, Seymour, Toward a safer and more secure cyberspace,Commun. ACM. 50. 128. 10.1145/1290958.1290991, 2007

[7] Sunil, G &Aluvala, Srinivas & Reddy, S &Dadi, Ramesh & Varun, Revuri, "VARIOUS FORMS OF CYBERCRIME AND ROLE OF SOCIAL MEDIA IN

CYBER SECURITY" pp.- 2709-2715, 2020

[8] A. Singh and M. S. Bora, "Cyber Threats and Security for Wireless Devices," SSRN Electronic Journal, 2013, doi: 10.2139/ssrn.3419703.

[9] M. A. Javaid, "Top Threats to Cloud Computing Security," SSRN Electronic Journal, 2013, doi: 10.2139/ssrn.2325234.

[10] Dobran, B, 17 Types of Cyber Attacks To Protect Against in 2020, PhoenixNAP Global IT Services,https://phoenixnap.com/blog/cyber-security-attack-types, 2020, December 8

[11] Gade, Nikhita Reddy & Reddy, Ugander,"A Study Of Cyber Security Challenges And Its Emerging Trends On Latest Technologies", 2014

[12] .R. A. Clarke and R. K. Knake, The fifth domain : defending our country, our companies, and ourselves in the age of cyber threats, New York: Penguin Press, 2019