International Journal of Engineering Applied Sciences and Technology, 2017
Vol. 2, Issue 6, ISSN No. 2455-2143, Pages 51-53
Published Online in IJEAST (http://www.ijeast.com)

ROLE OF CYBER-THREATS AND CYBERSECURITY IN THE DIGITAL ERA

Akshita Jaitly
Manipal University, Jaipur

Abstract: With an exponential increase in our dependency on technology, security becomes imperative. In this paper, we put forth the issues related tocybercrime, how to determine the security of our data and what motivates a cybercriminal. The main objective of this paper is to provide basic knowledge about the importance of cybersecurity and prevention/minimization of cyber-threats.

Keywords: Cybersecurity, Cybersecurity threats, Cybercriminals, Hackers, Spoofing, and Confidentiality.

I. INTRODUCTION

Originally, Internet was a small network between few computers which used to send and receive data. The network has grown a lot since then. Having affordable computers and portable electronic devices made sharing and receiving information a lot easier. People can now play games with anyone across the globe, shop, read newspapers and even exchange money or manage bank accounts. Other devices such as cars, smart televisions, refrigerators, elevators, power plant and may more have also started communicating with computers. Undoubtedly Internet has made our lives a lot easier, but this comes with a price to pay. In this huge communication network, one computer/ device might send a command to another asking it to delete all its data or share it with the sender. This is known as viruses and malware. Just like we don't keep the doors of our house open for anyone to enter we should protect information valuable to us.

With the increasing dependencies on technology, security becomes imperative. With the acronym CIA, we can understand how secure our data is [3].

i) Confidentiality makes us think about who has access to our data. Methods deployed to ensure confidentiality include data encryption, user IDs, and passwords. Other methods may include biometric verification, authentication token, and one-timepassword (OTP) which is widely used today.

ii) Integrity means who has the rights to modify our data. Is it for public use oris it for authorized users only? If authorized users, then what kind of authorization is need? These are the type of questions one should ask when talking about integrity. Maintaining the consistency, accuracy, and trustworthiness of data is known as integrity. Various measures are needed to make sure that data does not alter in transit; unauthorized users don't access it or make any changes. These measures include access control i.e. file permissions, network etc.

iii) Availability causes us to ask the question whether I have access to my data, can I access it from different devices and so on. It is best maintained by ensuring a timely and reliable functioning of the hardware.

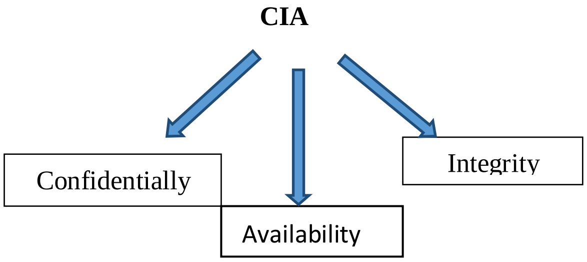

Fig1.1

Computer viruses and Trojan of today are designed to do everything from stealing data, billions of dollars to watching you on your webcam. Trojanviruses (or Trojan horses) look like a normal file or software. Used by hackers or cybercriminals to gain access to one's system and insert more malware. Unlike viruses, Trojan does not have the ability to replicate but provides remote access of computer's data to its creator.With this access, a hacker can delete, modify, update or copy any file to or from the computer system giving them access to confidential information like bank account or credit carddetails.[1]For example, if one of your files contains an itinerary for your next holiday, they would have knowledge of your whereabouts.

Financial gain is the top motivator for cybercriminals while others may engage in such activities for fame. Fame-seeking hackers target big banks or government agencies. Furthermore, juvenile thoughts like revenge or flaunting could lead to seriousdamage. Stalking, child exploitation, stealing sensitive information from government agencies/websites, business rivalry lead to hacking opponent company's databases, to name a few.

The word cyber means technology and security means protection, therefore the act of protecting technology may be known as cybersecurity i.e. to protect networks, computers, programs and data from attack, damage or unauthorized surveillance [11]

II. CYBERSECURITY THREATS AND PREVENTIVE MEASURES INVASION OF PRIVACY

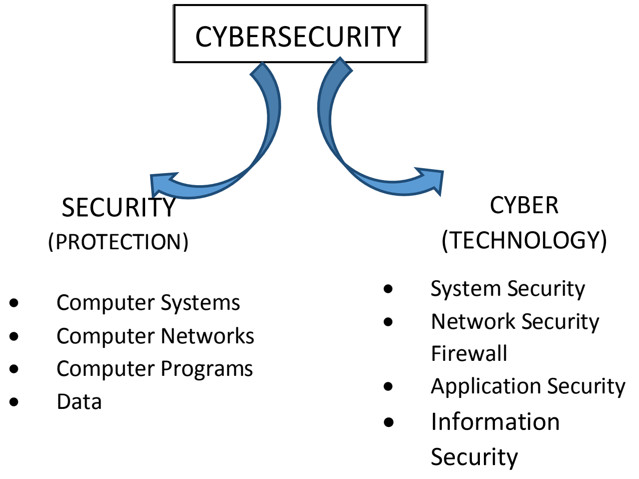

Fig 2.1 Segments of cybersecurity

Every search you make on google is being recorded and stored. This is how it provides you with suggestions on the basics of yourhistory. As well as keeping a record of searches and voice, google also keeps a record of your location. Google's location history allows you to see your location at a particular date and time. It has its advantages, but if someone hacks into your account or Google's server they will have access to these locations. Microsoft, Apple, Gmail, Yahoo, Hotmail, all of them reserve the right to read their users' emails. All the emails received and sent are scanned for some keywords which are useful to track terrorist or illegal activities. Disabling location services would prevent Googleor Apple from keeping a tab on it. Also using software which helps you browse the net anonymously by hiding your IPaddress and your identity by bouncing off your internet connection of three different servers and protecting you. One such software is tour.

III. SPOOFING ATTACKS

Spoofing is a kind of attack where an individual or a group of individuals impersonates to be of some authority in order spread viruses or have access to some valuable information. There are several different kinds of spoofing attacks that malicious parties can use. Most common ones include e-mail spoofing, IP address spoofing and ARP spoofing which send files containing malware to infect target system while SMS spoofing is an emerging attack. By taking a few simple measures one can save themselves from these spoofing attacks. Some prevention methods include packet filteringusing spoofing detection software and only downloading files from trusted websites or senders [4].

IV. PHISHING ATTACKS

Cyber-criminals often use a phishing attack to gain access to information like usernames, passwords, and credit card details. Mostly they achieve this through sending emails and using keywords like- verify, update, validate or click here to login to your account. Some of the common phishing attacks are-

(a)Deceptive Phishing is generally used to get someone's bank details and reaches out to people in the form of an email which may be threatening or require their urgent attention, scaring them to follow up the link and give in details on the fake website. To distinguish a fake webpage from a real one to look at the page URL, one should also look for grammar mistakes and spelling errors throughout the mail.

(b)Spear Phishing has the same goal as deceptive phishing, but the approach differs. The mail is customized by adding target's name, age, phone number, company they work for etc. For protection against this kind of scam, you should be careful about what all personal information you make available on social networking sites.

(c) Another type of phishing called CEO Phishing steals money by impersonating an authority figure which requests some wire transfers from others in a company. This is very common in businesses where the employees are not aware of cybersecurity threats and what measures to take, so they fall into the trap and put themselves and their business at risk. Preventive measures should be taken by the company itself by giving its employees including top executives, proper security awareness training.

(d) Pharming- method in which a pharmer targets a DNS (Domain Name Server) server and changes the IP address associated with it and redirects the user to a fraudulent website, even though they entered the correct website address. To keep away from such attacks, everyone should only enter their login details on HTTPS- secured websites and use antivirus software [7].

V. DENIAL OF SERVICE (DOS) ATTACK

If for instance you type in the URL on the web browser and are waiting for your request to be processed.an attacker overloads the site's server and since a server can only process a limited number of requests, your request won't be processed. This is called denial of service attack where an attacker "floods" the server with requests preventing others from using it. In a similar manner, your email can also be flooded with spam containinglarge size messages resulting in you reaching the data your data limit in your account. This prevents you from receiving any legitimate emails. Installing antivirus and firewalls may help in reducing such attacks. But there is no effective way of preventing the attack [6, 9].

VI. FUTURE SCOPE

The need for protection against various cyber-threats is only going to increase in the coming years as the advancement of technology is taking place at a rapid pace.Cybersecurity will be a necessity to our day activities and play a more prominent role in businesses.

The biggest challenge that cybersecurity organizations might be facing is the shortage of cyber talent. While there may be a lot of graduates to fill the positions, but the level of skill required is missing. Many experts believe that starting specialized training early in college might help resolve this problem for future.

Most developed nations will soon accept the fact thatcyber-attacks and digital spying are the top threat to the country's security. Since terrorists also try to take advantage of the vulnerabilities of a system/software to fulfill their intentions, making security a major issue of concern.

VII. CONCLUSION

In the starting the paper discusses the CIA model for used for evaluation of how secure our data is. I believe that this is an effective method for anyone who is not a cybersecurity expert to easily know how vulnerable they are to a cyberattack. Also, taking simple preventive measures like identifying and deleting spam emails, finding the difference between a fake and an authentic website could help reduce loss of data/privacy.

Businesses and governments should pay good attention to how secure their network and communication is by employing cybersecurity experts. Prevention from cyberattacks such as phishing, spoofing or DOS should be the top priority for government agencies, as data breach would could affect nation's security.

VIII. REFERENCES

1. https://us.norton.com/internetsecurity-malware-what-is-a-trojan.html
2. V. Suganya, A Review on Phishing Attacks and Various Anti Phishing Techniques, available at https://www.ijcaonline.org/research/volume139/number1/suganya-2016-ijca-909084.pdf
3. Eric A. Fischer-Cybersecurity Issues and Challenges: In Brief
4. Neil DuPaul- Spoofing Attack: IP, DNS & ARP
5. DaQuan Stevens, Esteban Proano, Salem Alzaabi-Hardware and Software Security
6. Mindi McDowell-Understanding Denial-of-Service Attacks, available at https://www.us-cert.gov/ncas/tips/ST04-015
7. https://www.tripwire.com/state-of-security/security-awareness/6-common-phishing-attacks-and-how-to-protect-against-them/
8. James Lyne: Everyday cybercrime -- and what you can do about it, https://www.youtube.com/watch?v=fSErHToV8IU
9. Ankit Fadia, Cyber Security-The key to realizing the dream of a truly Digital India
10. Reuben Paul- what is cyber security?, https://www.youtube.com/watch?v=vvsfM5Dixow
11. Cybersecurity, https://www.youtube.com/watch?v=sdpxddDzXfE