IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 3, Issue 1, February 2023
Impact Factor: 7.301

Data Security:Challenges in Cyber World

Dr. Quazi Farheen A
Assistant Professor, Department of Computer Science & Information Technology
Yeshwant Mahavidayalya, Nanded, Maharashtra, India

Abstract: *In today's era Internet technology becomes very extensive to exchange information through online. Different Government and private sectors mostly depends on Information Technology. The essential thing in internet world is the data. This data or information have to be protected from any harm, error and damage. The first step in protecting yourself is to recognize the risks and become familiar with some of the terminology associated with them. There are various option to protect from the cyber crimes. The data can be protected using various techniques such as Anti-viruses, anti-malware, spy ware, encryption, access control, physical security, keep backup of data regularly, and good security habit.*

Keywords: Data security, Literature Review, Phishing, Types of attacks, Preventions

I. INTRODUCTION

In today's world, personal information is of vital importance. Security is breached by unauthorized persons. In this case, Data security is important in vision of government as well as private sectors. In information intensive organizations secured management of information has become an important issue. Organizations have to actively use security technologies and extant researches in information security have to be focused on the use technologies.

II. LITERATURE REVIEW

Phishing is a form of social engineering. Phishing attacks use email or malicious web sites to solicit personal, often financial, information. Attackers may send email seemingly from a reputable credit card company or financial institution that requests account information, often suggesting that there is a problem. When users respond with the requested information, attackers can use it to gain access to the accounts.

Malicious code, sometimes called malware, is a broad category that includes any code that could be used to attack your computer. Malicious code can have the characteristics like It might require you to actually do something before it infects your computer. This action could be opening an email attachment or going to a particular web page. Some forms propagate without user intervention and typically start by exploiting software vulnerability. Once the victim computer has been infected, the malicious code will attempt to find and infect other computers. This code can also propagate via email, websites, or network-based software. Some malicious code claims to be one thing while in fact doing something different behind the scenes. For example, a program that claims it will speed up your computer may actually be sending confidential information to a remote intruder. Viruses and worms are examples of malicious code. In most cases, vulnerabilities are caused by programming errors in software. Attackers might be able to take advantage of these errors to infect your computer, so it is important to apply updates or patches that address known vulnerabilities [2].

In a denial-of-service (DoS) attack, an attacker attempts to prevent legitimate users from accessing information or services. By targeting your computer and its network connection, or the computers and network of the sites you are trying to use, an attacker may be able to prevent you from accessing email, web sites, online accounts (banking, etc.), or other services that rely on the affected computer. The most common and obvious type of DoS attack occurs when an attacker "floods" a network with information. When you type a URL for a particular web site into your browser, you are sending a request to that site's computer server to view the page. The server can only process a certain number of requests at once, so if an attacker overloads the server with requests, it can't process your request. This is a "denial of service" because you can't access that site[6].

An attacker can use spam email messages to launch a similar attack on your email account. Whether you have an email account one available through a free service such as Yahoo, you are assigned a specific quota, which limits the amount of data you can have in your account at any given time. By sending many, or large, email messages to the account, an attacker can consume your quota, preventing you from receiving legitimate messages.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 3, Issue 1, February 2023
Impact Factor: 7.301

III. EXISTING SYSTEMS

Responding to Attack : How do you avoid being part of the problem: so there are no effective ways to prevent being the victim of a DoS or DDoS attack, but there are steps you can take to reduce the likelihood that an attacker will use your computer to attack other computers: Install and maintain anti-virus software .Install a firewall, and configure it to restrict traffic coming into and leaving your computer. Follow good security practices for distributing your email address Applying email filters may help you manage unwanted traffic. - How do you know if an attack is happening: Not every attack is denial-of-service attack. There may be technical problems with a particular network, or system administrators may be performing maintenance. However, the following symptoms *could* indicate a DoS or DDoS attack: unusually slow network performance (opening files or accessing web sites) unavailability of a particular web site inability to access any web site dramatic increase in the amount of spam you receive in your account. What do you do if you think you are experiencing an attack:Even if you do correctly identify a DoS or DDoS attack, it is unlikely that you will be able to determine the actual target or source of the attack. Contact the appropriate technical professionals for assistance. If you notice that you cannot access your own files or reach any external web sites from your work computer, contact your network administrators What do you do if you think you are a victim: If you believe you might have revealed sensitive information about your organization, report it to the appropriate people within the organization, including network administrators. They can be alert for any suspicious or unusual activity. If you believe your financial accounts may be compromised, contact your financial institution immediately and close any accounts that may have been compromised. Watch for any unexplainable charges to your account. Consider reporting the attack to the police, and file a report with the Federal Trade Commission.

IV. CONCLUSION

By using Proper methods and good security habits we can make safe our personal information by minimizing the access other people have to your information. You may be able to easily identify people who could, legitimately or not, gain *physical* access to your computer—family members, roommates, co-workers, members of a cleaning crew, and maybe others. Identifying the people who could gain *remote* access to your computer becomes much more difficult. As long as you have a computer and connect it to a network, you are vulnerable to someone or something else accessing or corrupting your information; however, you can develop habits that make it more difficult. Lock your computer when you are away from it. Even if you only step away from your computer for a few minutes, it's enough time for someone else to destroy or corrupt your information. Locking your computer prevents another person from being able to simply sit down at your computer and access all of your information. Disconnect your computer from the Internet when you aren't using it. The developments of technologies such as DSL and cable modems have made it possible for users to be online all the time, but this convenience comes with risks. The likelihood that attackers or viruses scanning the network for available computers will target your computer becomes much higher if your computer is always connected. Depending on what method you use to connect to the Internet, disconnecting may mean disabling a wireless connection, turning off your computer or modem, or disconnecting cables. When you are connected, make sure that you have a firewall enabled.

Government should not assert authority in ways that would make private sector assumption of security responsibility impossible in the future as technology advances or conditions changes. Security is breached by unauthorized persons. Data security is important in vision of government as well.

V. ACKNOWLEDGMENT

Finally, I present my gratitude towards my institute, ‘Yeshwant Mahavidayalya. Nanded and my all colleagues for helping me with every aspect to complete this paper. It wouldn’t have been possible without their support.

REFERENCES

[1]. The Hacker Playbook 3: Practical Guide To Penetration Testing - Peter Kim
[2]. Social Engineering: The Science Of Human Hacking - Christopher Hadnagy June 25, 2018 by Wiley
[3]. The Art Of Invisibility - Kevin Mitnick
[4]. Hacking for Beginners: A Step By Step Guide For You To Learn the Basics of Cybersecurity And

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 3, Issue 1, February 2023
Impact Factor: 7.301

Hacking - Ramon Nastase

[5]. Blue Team Handbook: Incident Response Edition - Don Murdoch August 3, 2014 by Create Space Independent Publishing Platform

[6]. The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography - Simon Singh August 29, 2000 by Anchor.