International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2020 IJSRCSEIT | Volume 6 | Issue 2 | ISSN : 2456-3307
DOI : https://doi.org/10.32628/CSEIT206251

Issues and Challenges for Preventing Cyber-Attacks

Arvind Kishanrao Rathod*, Bhushan Shivaji Kulkarni
Department of Computer Engineering, Government Polytechnic, Jintur, Maharashtra, India

ABSTRACT

The main objective of cyber security is to prevent various types of attacks on individual user system or organizations system or network by implementing some preventive measures such as by enforcing security policies, providing security awareness among the peoples by organizing frequent trainings or workshop to avoid social engineering attacks. Also implementing some tools such as intrusion detection system, firewall, antiviruses in individual system on organizations network and avoid from data corruption or alteration attacks by attackers via internet or some other means.

Keywords: Digital Forgery, Viruses, Worms, Rootkits, Keyloggers, Watering Hole, Vishing

I. INTRODUCTION

From last two decades all the offline businesses becomes online business called e-business. Notebooks and light pens replace the cashbook and pens. Large quantity businesspersons' are doing the online transactions over the internet. The e business reduces the time, money, work force, paper etc. within the fraction of seconds information is exchanged among various accounts online. Today all peoples are able to perform the online activities such as transmission of information, video, audio via emails or some other online ways without knowing that information is safely transmitted or not.

However, along with these positive things some negative things such as digital forgery, e-crimes and many more digital crimes evolved rapidly. In addition, many criminals are doing such attacks. If any online attack becomes successful then it will become the reward for the attacker.

Now a day we know that internet is a place where attacker can easily get any readymade tool for making online attack. Some attackers are so smart that they can develop their own tool or program for online attack.

One advantage for attacker is that they can do this online attack from anywhere any place. Attackers are becoming more technocratic and daily they are applying new tricks for online fraud or crime. Hence, it is becoming difficult to identify them.

So it becomes necessary to provide cyber security for all types of online activities such as developing and enforcing cyber security policies, providing trainings to all online users, imposing technologies for preventing e-crimes etc.

II. OBJECTIVE OF STUDY

a) To understand the need of cyber security
b) To understand different types of threats to cyber security.
c) To study the various available tools for preventing threats and e crimes.

CSEIT206251 | Accepted : 21 March 2020 | Published : 30 March 2020 | March-April-2020 [6 (2) : 212-215]

III.THREATS TO SECURITY

A. **Malicious Programs** -There are various types of malicious programs that affect the security of user's data, information. These malicious programs includes-

a) Viruses – A Virus is a malicious program, which attaches itself to the legitimate user program. Attacker to infect the legal program creates it. The viruses can perform the activity that the attacker wants to do with legal user data. They can modify, delete the original data or prevent the legal user from access of it.

b) Worms – Worms are also malicious programs like viruses but they cannot modify or delete the legal users data but they can replicate themselves and consumes the system resources such as memory, storage space etc. and brings the system in halt condition so that further the legal user cannot access the system more.

c) Backdoors – A backdoor are the programs that may be created by attacker or legal software developer. Attacker to avoid the legal authentication process and grant the access to the system for doing malicious activities even if the organization or legal user fixes the original vulnerability creates these.

d) Rootkits – A rootkits are the malicious program that takes the command and control of entire computer without knowing the legal user. They have ability to remotely execute the programs and change the system configuration. They also helps attacker to create backdoor in to the system by changing the system files.

e) Keyloggers – Keyloggers are the insidious malicious programs that may be installed on users system while browsing the illegal websites or downloading illegal internet contents. Depending upon the type of keylogger, they can record everything that the legal user types such as passwords, ids and many more things and send this information to the attackers system. In addition, they can record which website that legal user visited.

f) Spywares – Spywares are the malicious software or programs that without permission of legal user get the access of system, monitor the system and steal the sensitive information, system data of legal user. They are hidden and very difficult to detect.

B. Social Engineering Attacks – Authorized users are convinced by the attackers using all social engineering techniques to provide the confidential information of the system data or organization in these techniques. There are many ways of social engineering attacks such as phishing, watering hole, vishing etc.

i) Phishing – In this attack attacker creates fake messages, emails, or webpages similar to legal one and sends these to the targeted users. Legal users in return blindly provide all the information to the attacker via these messages or emails or on duplicate web addresses.

ii) Watering Hole – In this type of attack the attacker injects the malicious code in the public web pages that the user frequently visits and collects all the information of the legal user.

iii) Vishing – In this type of attack the attacker uses the phone and attaches a toll free number to it and recreates the company's interactive voice response system and makes the spoofing calls so that the legal user by trusting on it feed all legal information to the attacker.

Along with these attacks, the attacker can also perform Denial of Service (DOS) or Distributed Denial of service attack (DDOS), SYN-ACK flooding attack. In DOS or DDOS attack, targeted system is overwhelmed with large number of messages by the attackers system after that targeted system is not able to handle this traffic and it becomes to a stage of hang.

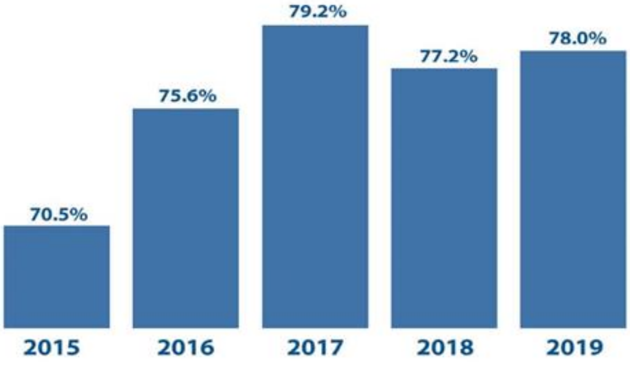

Figure 1: Frequency of successful attacks by year.

This figure is taken from Imperva 2019 Cyber threat Defense Report that says, "Almost two-thirds of IT security professionals believe a successful cyber-attack is imminent in 2019"

IV. EFFECTIVE MEASUREMENTS TO PREVENT THE ONLINE CYBER ATTACKS.

To prevent the online cyber-attacks there are some preventive measures to be taken by the organizations, users of the system.

a) Maintaining Strong User Permissions and Access Control. – Organization should prepare the strong policy for maintaining strong user permissions and access permission. Strong administrator accounts can be minimized. User should be forcefully allowed to change their passwords regularly. Week password identifying programs must be installed so that user cannot keep default passwords. By this way, the brute force attack can be prevented.

b) Operating System Hardening – systems vulnerability scan, port scan can be performed regularly so that all vulnerabilities can be patched by installing the latest service packs and open ports can be blocked. With this, the attacker cannot make the backdoor entry and manages the system.

c) Application Hardening – Application installed in the system can be updated to latest versions so that the attackers cannot manage them.

d) Perform Penetration Testing – Penetration testing can be performed periodically once in month so that the vulnerabilities in the system can be checked.

e) Security Awareness - An active security awareness program is most effective method to oppose potential social engineering attacks. Depending the level of threat peoples should be properly trained on social engineering. Constantly remind the users about possible avenues of attacks.

f) Digital Certificate – Digital Certificates are used for sharing public keys which are used for encryption and authentication; they are used for securing secure socket layer connection between web browser and web server. Used to solve the problems of tampering and impersonation.

g) Secure Socket Layer – SSL is a commonly used internet protocol for managing the security of a message between web browser and web server. It provides two layer of security services – Authentication and confidentiality logically SSL provides a pipe between web browser and web server. It uses public and private key encryption technique from RSA that also includes the use of a digital certificate.

SSL can performs this by using its following given protocols such as SSL record protocol, Handshake protocol, Change-cipher spec protocol, Alert protocol.

V. CONCLUSION

The area of online cyber security is more vast and from last few years the peoples are becoming dependents on computers and networks, so they are more intrested in the security of these computers and networks. With more use of computers and networks on daily basics to conduct everything like making purchaces, data, money transfer etc. the security of computer and network becomes paramount importance so that the information that is exchanged becomes private and secure. There are also many techniques available for online cyber security.

VI.REFERENCES

[1] G.Nikhita Reddy And G.J.Ugander Reddy, “A study of cyber security challenges and its emerging trends on latest technologies” in Research Gate, Article · February 2014.

[2] Santosh Kumar Maurya and Nagendra Pratap Bharti, “Cyber Security; Issue and Challenges in E-Commerce”, in Indian Journal of Research, Volume: 5, Issue: 1, January 2016.

[3] Jitendra Jain and Dr. Parashu Ram Pal, “A Recent Study over Cyber Security and its Elements”, in International Journal of Advanced Research in Computer Science, Volume 8, No. 3, March – April 2017.

[4] 2018 security threat report by Www.protiviti.com.

[5] ACS cyber security Threats, challenges and opportunities guide 2018.

[6] https: // www.comparitech.com / vpn/ cyber security - cyber - crime - statistics -facts-trends /.

Cite this article as :

Arvind Kishanrao Rathod, Bhushan Shivaji Kulkarni, "Issues and Challenges for Preventing Cyber - Attacks", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 6 Issue 2, pp. 212-215, March-April 2020. Available at doi : https://doi.org/10.32628/CSEIT206251
Journal URL : http://ijsrcseit.com/CSEIT206251