Volume 4, Issue 3, March 2014 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Security Threats

Er.Simar Preet Singh
Assistant Professor
Computer Science & Engineering Department
DAV University, Jallandhar, Punjab (INDIA)

Er.Renuka Gujral
Research Scholar
Computer Science & Engineering Department
DAV University, Jallandhar, Punjab (INDIA)

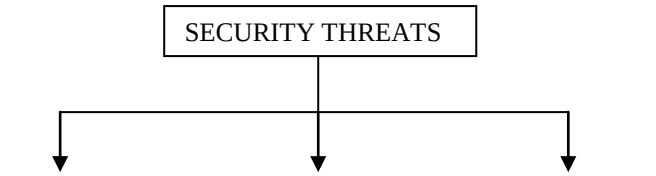
Abstract— every organization wants to secure the computer system and its confidential information from the unauthorized users. It focuses on the background of the computer security which includes protecting information from theft, attacks from hackers, intruders. The security means the process or mechanism by which the important information is protected from unauthorized access, copyright, unauthorized disclosure and some physical threats. This paper focus on some of the fundamental security threats those points towards the computer security, safety and reliability by taking such prevention measures. Many of the past incidents have caused intentionally and have reacted maliciously today. Firstly, we examine the characteristics of the security vulnerabilities and threats, and recall some previous incidents by discussing this article. This paper focuses on the prevention against the security threats [4].

Keywords— Security threats, classification of security threats, prevention, detection, reaction, steps to prevent

I. INTRODUCTION

Security threats with the general threats associated with the computer system .Threat is a possible danger that reduces the security and causes possible harms to system as well as data [2]. Security vulnerability is a weakness in a system design which can exploit the system. For Example: if you leave the house opened with no lock-it is called vulnerability. The intruder tends to open the lock-is a security threat and when the intruder opened the lock –that is called security attack [1] [2]. The Threat can be people threats, natural threats and physical threats. The people threat can loss up to 50-60% annual dollar .Natural threat can be of 20% annual dollar loss .Physical threat can be of 5-10% annual dollar loss [2].

II. CLASSIFICATION OF SECURITY



a) Insider
b) Outsider

Figure1: Classification of Security Threats

A. People threats

People threat can be insider or outsider which is performed by the human itself [8] [3].

a) Insider Threats:

The most dangerous threat to security is insider threat because the whole data or information is known to company's employees in the organization and their losses are in high rate. The possible consequences of insider attack can loss of confidentiality, loss of integrity, loss of availability [3].

- Unauthorized disclosure: the unauthorized disclosure means the revealing of information that is not sanctioned by above authority .its consequences can be degradation, interruption, and abridgement of rights.
- Unauthorized use: the unauthorized use is the use of the company resources without having any permission. Its consequences can be copyright, violation for the use of unlicensed software.
- Theft: Theft includes the stealing of information from company facilities. Its consequences can be loss of important information, program that contains on hard disk or any storage media [4].
- Modification and Alteration of data: This is an unauthorized changing of data which can be motivated by any person for favoritism, for personal gain or misguided the employee. It is possible consequences include poor quality of output results, loss of integrity and benefit to another company [1].

b)Outsider Threats: Outsider threats are generally the unauthorized user which is from outside the company.it can be Hacker, cracker and intruder.

- Hacker threats: The hacker is the person tries to hack the computer system. The possible consequences are threat to computer securityi.e.eavesdropping, hijack username password, steal of money [2].
- Cracker threat: The cracker is the person who cracks the password of accounts i.e. Gmail, Facebook, and yahoo to exploit the security weakness. Its possible consequences are spoofing, social engineering (revealing of password), and loss of confidentiality.
- Intruder threat: Intruder is the person who tries to gain the unauthorized access which damages and disturbed the data on that system. Its consequences include loss of availability and integrity.

B. Natural Threats

The natural threats are the threats which occur naturally by atmospheric disturbances. It can be failure of electrical power, hardware stops working, fire and smoke, and other threats [8] [6].

- Failure of electrical power: it is the failure of power system or disturbance in the continuity of power supply which cans results into shutdown of the system stops the current processing, minor loss of data, and interruption of services.
- Hardware Failure: in this, any component fails to perform the task or particular disk crash. Its results can be the loss of processing time, loss of software capability.
- Fire and smoke: fire in wide amount as it destructs the entire building. Smoke can harm the CPU fan due to overheating. The possible consequences are stops the continuity of work, loss of system for long period of time.
- Other threats: air conditioning (liquid leakage), humidity, earthquake, floods.

C. Software Threats

The software threats can be of virus, Trojan, worms, spyware.

a) *Virus*: The virus appeared in 1981,the first seen "in the wild"(i.e. in the public domain) and Elk Cloner is second computer virus was found is a Apple II operating system spread by floppy disk. The virus is a class of program written to perform a specific function. Virus is spread through application programs on computer as well as installed application programs on disk drives and through email attachment. The virus performs its function in two forms. Firstly, it copies itself another programs whenever going to execute the instruction commanded. This damages the both system hardware and software. Secondly, it may waits for defined time and date. It became difficult to rebuild the system software and data because viruses are rapidly developed to other programs. The possible consequences such as system corrupt, loss of data, system crash, hard disk failure. There are four types of virus:

1. Program virus: It spreads from one program to other program.
2. Boot Sector: It spreads from the infected floppy disk used, infects the hard drive
3. Macro: It spreads from such Microsoft Word, Excel and outlook, when we opened the infected file.
4. Email attachment: When an infected email is opened.

b) *Trojan Horses:* The software code packed inside the useful application. When this program runs, the camouflaged virus executes and it starts deleting the files and damages the whole system. It spread through the email attachment, music files, and games. Suppose a user wants to download a movie or a music file. An example of Trojan horse is like an animated picture of Christmas SantaClaus, displaying a message "Merry Christmas", but behind it extra code is executed which deletes all the files, or might be giving your account passwords, your credit cards numbers and its password to a stranger.

c) *Worms*: It is the program that self-replicates or copies itself repeatedly into the RAM memory. It also copies itself into the disk drives so it can go into the RAM again. [5][1]Worms use more than one method to copies itself. Worm mostly arises through the email, when you open the email attached, the worm attacks on the windows outlook and other such address books and selects the names randomly and the worm sends the copies of itself to the names into the address books. Some examples of worms are such emails attached with the subject line as "HERE YOU HAVE","JUST FOR YOU", It was the first email worm created in 1982. The other email worm such as "Melissa" or "I LOVE YOU" which has an attachment with name "LOVE-LETTER-FOR-YOU.TXT.vbs"[9] .In 2008 the Conflicker worm spreads which is one of largest infected worm ever.

d) *Spyware:* Spyware is the software that secretly installed on computer system without having the knowledge of user. [5][1] It secretly monitors user activities, commands and takes the control of user over the personal PC. It records the internet surfing habits, key strokes and private information. Its danger level and prevalence is very high. Consequences of spyware are that it can collect and gather personal information of user such as regular website visited credit cards detail, usernames and passwords. The most common spyware does the following:

i. Display unwanted advertisement
ii. Change web browser settings
iii. Perform unwanted actions by an intruders
iv. Download and install unwanted programs or files.
v. Record the data and transmitting into the third party
vi. Shutdown PC or program.

It is first appeared in 1999, as a component in free downloadable games. Remote Administration tools (RAT) is the most dangerous spyware threat.

III. HOW TO SECURE THE SYSTEM

There are the basic three methods to secure the system:

i. *Prevention:* The prevention can be done by taking measures to prevent your information being damaged, altered or stolen. Prevention measures are to lock the server room door to set up the high-level security polic

ii. *Detection:* The detection measures allow you to detect when and how the information has damaged, altered or stolen and who has damaged the cause.

iii. *Reaction:* The measures should be taken that helps you in recovering the whole information, even if the information is lost or damaged.

IV. STEPS TO PREVENT FROM THESE THREATS

As the internet is used throughout the day, it has also increased the risk of data loss and integrity to the confidential data:

A. Browsing Safely

a) Avoid clicking on everything:

There are many banner ads and popups on the internet that are made to have a click on it. So that, on a click you will be get infected with some kind of threat [7] [11].

i. You should make sure that the browser is configured as such it first asks you before running files or downloading.

b) Beware of misleading popups:

Most of the popups are basically designed as same as antivirus software. This popups tricks the user that their antivirus software has found some infection, and when the user click on the popups, the infected virus is actually installed on the Pc.

i. Instead of clicking on the link, Close the popup window and open the antivirus program on your window.

ii. Don't try to click on 'X' to close the window as this will leads to more popups. To prevent from this use task manager.

iii. Avoid clicking on the advertised popups those warn that only their software can fix problem.

iv. Ensure that browser should block popups.

c) Clear your cache:

Clear your popup regularly for not reappearing popups again and again.

d) Consider a different browser:

New browser should be used such as Firefox, Chrome, and Opera as they are more secure.

i. Browser should be up to date to which prevents from unauthorized attacks.

e) Don't access to the illegal sites:

As virus is illegal, they most occurred on the illegal sites. Avoid the sites that let you download the copyright content or other illegal communities.

B. Handling Downloaded Files

a) Select the needed downloads:

Download only the selective and the needed program according to the requirement. Avoid unnecessary clicks on the links.

b) Download from the trusted sites only:

It is advisable that if you try to download then download it only from the developed sites. Risks can be reduced from the trusted sites.

c) Beware from the fake extension:

Windows hides common file extension and exploits the file by doubling with such dangerous extension.

i. If you don't see the extension of your file which is downloaded it means it is the malicious file that contains malicious software.

For extension visibility, open windows explorer, click on view tab/menu and select options. Go to view tab in the Folder options window, and uncheck the" hide extension for known file types" box.

d) Scan the downloaded files:

Make habit of scanning the downloaded files with the help of antivirus software.

i. Always scan the ZIP files as they often contain multiple files.

ii. There are email programs that scan your emails, but still you should scan email files manually with your antivirus software.

iii. Don't open the untrusted file.

A virus or worm does not spread until you open the downloaded file. If you do not trust on the file then delete this file.

iv. Read the license agreement: While installing the software, you should not blindly accept it especially from the companies that you have never heard before.

C. Dealing with E-mails

a) Don't download the attachments from the source you don't know [11]. Email attachments are the most common way to get the malware spread.

i. If you don't know the sender, then you should not download any attachment from that mail.

b) Disable images preview

There are many applications which automatically download the images, which are more vulnerable as these images contain the malicious code.

c) Beware of business related emails.

As the phishing technique is used, this copies the style of the email from the company, and it the fake site with the regular URL of the company.

D. Protecting Yourself

a) Install the antivirus program:

The free antivirus software should be installed that protects the computer from various virus infections [1] [11].

i. You should have one antivirus programs installed at a time to avoid conflicts.

ii. Make sure the antivirus must be updated.

iii. Scan the computer at least weekly

b) Install the anti-spyware program:

Spyware hijacks your computer so to prevent from they install the antivirus software. Most programs include the Malware bytes, Spybot S&D, Hitman pro and Adware cleaner.

c) Enable a firewall:

Firewall protects the network ports in the internet communications that allow the data to send back and forth [4].

d) Keep the windows updated

The virus and malicious software exploits the window software. The windows should be updated automatically, in order to ensure that you're always protected.

e) Beware careful of USB drives:

The virus transmission is takes place while inserting the USB drives to the public computers. File sharing should be done by online or emails to send files.

f) *Beware about the remote access:*

In the most connected world the remote access and the remote sharing of resources is widely used.

i. If you need the remote connection, ensurethat the protection software is up-to-date.

g) Keep the backup for recovery

Backup should be scheduled and prevent from being damage or any loss done by virus or if the any disaster strikes. Back up can be created locally or remotely.

V. CONCLUSION

Security is needed to small and medium sized business though it can prevent from viruses, cybercrimes, Trojan and worms. Cybercrime is increases criminal attempts to danger the computer system. This paper aims to tell about the security threats facing their organization. There is a need to increase the use of such automated tools to indicate the occurrence of security attacks. Auditing and intelligent reporting are the methods to support security and threat management in a large scale for the past, current and the future. Such security solutions are needed to integrate the threat data from various security and network products [10]. The government must provide the better security policies for their products and to address them safely and reliability with much more consistency [10]. This document discussed about the possible security threats that can occur and certain measures to be taken to prevent from the loss of integrity, loss of confidentiality and the loss of availability. Consistent implementation to the security plan reduces the threats and increases the overall security of an organization data.

REFERENCES

[1]. A Handbook of information security, threats, vulnerabilities, prevention, detection and management VOL3 by HosseinBidgoli

[2]. Gollmann, Dieter. *Computer Security.* John Wiley and Sons

[3]. Bassham, Lawrence E., and W. Timothy Polk. *Threat Assessment of Malicious Code and Human Threats.* National Institute of Standards and Technology Computer Security Division.

[4]. Garfinkel, S., and G. Spafford. Practical UNIX Security. Sebastopol, CA: O'Riley& Associates

[5]. Trojans, worm and spyware: A computer Professional's guide to malicious code by Michael Erbschloe

[6]. Multimedia content representation classification and security by Bilge Gunsel, Anil K Jain, BulentSankur (Eds)

[7]. Secure computing Rita C. summers.

[8]. Foundations of computer security by David Salomon.

[9]. Essential computer security everyone guides to e-mail, internet and wireless security.

[10] Neumann P.G. Computer threats in aviation: vulnerabilities, threats and Risks: http://www.csl.sri.com/users/neumann/air.htm

[11]. How to stop E-mail spam, Spyware, Malware, Computer viruses, and hackers by Bruce C.Brown.

