International Journal of Current Engineering and Technology
E-ISSN 2277 – 4106, P-ISSN 2347 – 5161

Available at http://inpressco.com/category/ijcet

General Article

Computer Security

Ritika

Government College for Women, Rohtak, India

Accepted 12 Feb 2017, Available online 25 Feb 2017, **Vol.7, No.1 (Feb 2017)**

Abstract

It is a method to protect your data from malicious user by applying various techniques. You do not want your important data to be floating around freely, to protect data we need data encryption, decryption, antivirus etc. Here we discuss various security domains. The only purpose of these techniques is to protect your data with respect to confidentiality and integrity.

Keywords*: Unauthorized, anti-viruses, anti-malware, security domains*

Introduction

Computer security is protecting your data it also includes data storage and access. It involves measures like antivirus, firewalls, activating and deactivating software's to protect data from risk. In computer context protection is against unauthorized access. Or you can say protecting your information with respect to confidentiality and integrity.

System security is defined as: "The ongoing and redundant implementation of protections for the confidentiality and integrity of information and system resources so that an unauthorized user has to spend an unacceptable amount of time or money or absorb too much risk in order to defeat it, with the ultimate goal that the system can be trusted with sensitive information."

Computer security is of two types' software and hardware.

1) **Software security**: - It includes server protection, system security from viruses, data security from theft and safe computer practices.
2) **Hardware security**: - security of physical devices like server mainframe, portable memory and storage devices.

Various computer measures for security are

1) **Confidentiality** – to protect data from unauthorized users.
2) **Integrity** – to be sure of that data is not altered in between.
3) **Authentication** – to be sure that only intended user has sent the information.

Additional measures which are considered as a part of computer security are as follows:

1) **Access control** –only authorized users are allowed to access the information.
2) **Non repudiation** – the original sender cannot deny that he did not send the particular information.
3) **Availability** – to ensure that system is available at the need of the hour.
4) **Privacy** – The owner decides which information is visible to which user.

A Functional View on Computer Security

Computer security can also by analyzed by function. It is divided into 5 distinctive functional areas:

1. **Risk avoidance** – this is security fundamental which includes many questions like does my organization engage in activities that are too risky or do we really need unrestricted internet connection.
2. **Prevention** – Prevention techniques are used from the start like anti-virus and antimalware.
3. **Detection** – when the prevention fails only thing left is detection. And you still prevent damage which includes log keeping and auditing activities.
4. **Recovery** – sometimes any natural calamity and you can restore from scratch.

*Corresponding author: **Ritika**

Security Domains for Computer Security

1) **Physical security** – you can control protection against natural disaster.
2) **Operational/procedural security** – covering everything from managerial policy to reporting hierarchies.
3) **Personnel security** – hiring personnel and training, monitoring etc.
4) **System security** – user's access and authentication controls, maintaining files, their integrity, backups, log keeping etc.
5) **Network security** – protecting network servers, firewalls, controlling access. However it is difficult to achieve.

Many cyber security threats are largely avoidable. Some measures that should be included

1) Use good passwords, dictionary words should be avoided and keep your password protected.
2) Protect your system with antiviruses and anti-spyware software.
3) Don't click on unknown links and don't download unknown files.
4) Look for https in the URL, because here "s" stands for secure.
5) Avoid using unencrypted email and unencrypted instant messaging.

Why is Computer Security Important?

It is used for protecting data from theft such as bank details, credit cards information, password etc. Information present in your system needs to be secured to protect your data from unauthorized users. An unauthorized user can use your email id, pictures etc. Intruders also use your computer to attack other computers or websites. Hackers might crash others computers to destroy important information. All these factors state that your information should remain safe and confidential.

1) It is used to enable people to carry out their jobs, education and research.
2) Protecting personal and sensitive information.

Its objective:

1) To learn good computing security practices.
2) Use these practices in daily life and encourage others to do so.
3) Notify others if you become aware of a suspected security incident.

Computer security threats

Types of Computer threats are:

1. **Trojan**: - it is a very complicated threat. It hides itself from antivirus detection and hide important data such that user account comes under seize. It can take your entire security system.
2. **Virus**: - It is a program which replicates itself to destroy your computer.
3. **Worms**: - it is a harmless threat which is designed only to spread within a network or even the internet. It eats up all you space because of its replication problems.
4. **Spyware**: - it is basically used to spy on computer of the user. It can easily track down your daily activities and attacker can use your information. If you are searching for holiday's package then spyware send you holidays packages to make you spend your money.
5. **Scare ware**: - it gives you information that you have infection on your computer but actually you don't have, the basic idea is to threaten you but those anti malware software which claims to remove those threats.
6. **Key logger**: - it uses every key stroke when you type on keyboard it captures your username and password. It is a sub function of Trojan.
7. **Adware**: - It is a threat in which advertisement starts popping out, it does not actually harm anything but it is quite annoying.
8. **Backdoor**: - in this method in which it allows to bypass the entire authentication service. It is usually installed before any virus or any infection.
9. **Wabbits**: - It is a self replicating threat. It does not usually harm your system. It is form of DOS attack.
10. **Exploit**: - It works on browser and plug-in. It is specifically programmed to attack vulnerability. Software patches are used to solve this problem.
11. **Chain Letters**: - these threats are those which you see for example if you don't forward this message bad luck will follow you or your account will be deleted.
12. **Virus Document**: - it is a threat which attaches itself to the PDF file; it is advised to scan the document before opening any file.

Conclusion

Computer security basically securing your data from malicious users it includes protecting your data from adding, deleting or modifying your data. It includes measures like confidentiality, integrity, authentication, non-repudiation, privacy in order to keep your system safe. It is of two types i.e. hardware and software. It is an important factor because now a day's every business is done online and data protection is at top most priority for example you use your online bank account you do many transactions you don't want to lose money while performing any operations.

Reference

http://forums.iobit.com/forum/iobit-security-software/iobit-security-softwares-general-discussions/other-security-discussions/15251-28-types-of-computer-security-threats-and-risks
http://www.wisegeek.com/what-are-the-different-types-of-computer-security.htm
http://www.albion.com/security/intro-4.html
http://www.webopedia.com/TERM/S/security.html
http://www.contrib.andrew.cmu.edu/~aishah/Sec.html
http://its.ucsc.edu/security/training/intro.html