International Journal of Enhanced Research in Management & Computer Applications, ISSN: 2319-7471
Vol. 4 Issue 4, April-2015, pp: (44-46), Impact Factor: 1.296, Available online at: www.erpublications.com

Computer Security

Neetika

Abstract: Computer security is a method of applying various techniques in order to protect your data from unauthorized users. You don't want anyone to have to your important data for this purpose you use data encryption, decryption and anti viruses, anti-malware, firewalls etc. Here we have discussed various threats, functional view of computer security, security domains. The only sole purpose of all these measures to secure your data with respect to confidentiality and integrity.

Keywords: unauthorized, anti-viruses, anti-malware, security domains.

Introduction

Computer security is protecting your system and all the data they store and access. It is basically protecting your computing system from unauthorized users without authorization. It the process of protecting your data from malicious users it involves measures like antivirus, firewalls, activating and deactivating software features like java scripts, active x, data encryption and passwords. Computing security means protecting your data from risk. In computer context protection 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 be sure of that data is not accessed by unauthorized users.
2) **Integrity** – to be sure of that data is not altered in between source or destination.
3) **Authentication** – to be sure of 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** – to be sure of that 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 operational at the need of the hour.
4) **Privacy** – The owner decides which information is visible to which user, who has access to that particular information, who maintains it, for what purpose it is used.

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. **Deterrence** – here the threat to information assets through fear.
3. **Prevention** – Prevention techniques are used from the start like anti-virus and anti malware.
4. **Detection** – when the prevention fails only thing left is detection. And you still prevent damage which includes log keeping and auditing activities.
5. **Recovery** – sometimes any natural calamity happens or at times system crashes, then the only choice you are left with is recovery option and you can restore from scratch.

Security Domains for Computer Security

1) **Physical security** – you can control the coming and going of people and materials and 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 proper applications and use all necessary security patches.
3) Protect your system with anti viruses and anti-spyware software.
4) Don’t click on unknown links and don’t download unknown files.
5) Look for https in the URL, because here “s” stands for secure.
6) Avoid using unencrypted email and unencrypted instant messaging.

Why is Computer Security Important?

It is basically used for preventing your data from theft such as back details, credit card information, password, work related information etc. It is important to protect your data. Information present in your system, it can be changed and modified by 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 you 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.
13. **Mouse trapping**: **-** it directs you to certain website instead of whatever you have typed in the URL, if you try to close the window and reopen it, still it will consider that website as your homepage until you remove it.
14. **Obfuscated Spam**: **-** It is a spam mail, it directly does not do anything but it makes you click on different websites.
15. **Pharming**: **-** it works like phishing. It is of two types one is DNS and other one is HOST file. For example when you type www.google.co.in on your computer even then it redirects you to other website.
16. **Crime ware**: **-** It takes control of your computer to commit a computer crime. It plants a Trojan or malware in order you to commit the crime.
17. **SQL Injection**: **-** it does not affect the users directly. It gains access to the database and retrieve all the valuable information stored in the database.

Conclusion

Computer security basically securing your data from unauthorized access which includes protecting your data from adding, deleting or modifying your data. Computer security includes various features like Confidentiality, Integrity, Authentication Access control, Non repudiation; Availability, Privacy and your system much consider all these features in order to keep your system safe and confidential. Computer security is of any types but basically only two types are considered here which are software and hardware. Computer security 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.

References

[1]. 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
[2]. http://www.wisegeek.com/what-are-the-different-types-of-computer-security.htm
[3]. http://www.albion.com/security/intro-4.html
[4]. http://www.webopedia.com/TERM/S/security.html
[5]. http://www.contrib.andrew.cmu.edu/~aishah/Sec.html
[6]. http://its.ucsc.edu/security/training/intro.html