International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

Design and Analysis of Information Security for SIS in Prospective of Application Software

Sharanappa Patil[1], Ramesh .K[2]

Assistant Professor, Department of Computer Science, L.V.D College, Raichur-584103, Karnataka, India

Associate Professor, Department of Computer, Science and Co-Ordinator, Department of Physics, Karnataka State Women's University, Bijapur, Karnataka, India

Abstract: ***Information security plays an important role in protecting the assets of an organization. As no single formula can guarantee 100% security, there is a need for a set of benchmarks or standards to help ensure an adequate level of security is attained, resources are used efficiently, and the best security practices are adopted. In this paper is concerned with issues relating to the management of information security in organizations, motivated by the need for cost-efficient information security.***

Keywords: Assets of organization, Security, Information Security, Management of Information Security.

1. Introduction

Computer security (also known as cyber security or IT security) is information security as applied to computing devices such as applied to computing device such as computers and smartphones as well as computer networks such as private and public networks including the internet.

The value of security to individuals to organizations and to societies was violently demonstrated by the Sep-2011 terrorist attacks information security is today considered a prioritized issue for top management and the board of directors in the vast majority of organizations. A recent global survey showed that the majority of the 1230 organizations responding even considered information security to be a CEO level priority.

While information security plays an important role in protecting the data and assets of an organization, we often hear news about security incidents, such as defacement of websites, server hacking and data leakage. Organizations need to be fully aware of the need to devote more resources to the protection of information assets, and information security must become a top concern in both government and business.

To address the situation, a number of governments and organizations have set up benchmarks, standards and in some cases, legal regulations on information security to help ensure an adequate level of security is maintained, resources are used in the right way, and the best security practices are adopted. Some industries, such as banking, are regulated, and the guidelines or best practices put together as part of those regulations often become a de facto standard among members of these industries [1].

2. Issues Related to the Information Security

Too much business security will increase the costs and reduce the potential revenue substantially and it can in due course put an end to the business. By observing this point in business. In the business the entrepreneur who makes decisions in an uncertain environment is the reward for bearing uninsurable risk. Conversely insufficient security might leave the business open for fatal mistakes, espionage, sabotage and crime. The goal of security management in organization should therefore be to identify and strive toward the optimal point between security and insecurity.

The optimal level of security in an organizations from a strict financial perspective, will be found in the situation were the cost of additional security countermeasures exactly equals the resulting reduction in damages arising from security breaches. This level means profit maximization for the organization. Too little security means that security breaches are reducing profits as a result of damages to assets, and too much security means that the costs of security countermeasures (including operational ineffectiveness and high-end security solutions) consumer profits. Hence businessmen should not strive towards higher and higher security without thinking about the consequences. Moreover security measures have other consequences than strictly monitory to be taken into account, e.g., social, legal and ethical.

3. Issues of Vulnerabilities in Securing a Computer System

To understand the techniques for securing a computer system, By taking the consideration give n in Wikipedia these are some important things to first understand the various types of "attacks" that can be made against it. These threats can typically be classified into one of these seven categories:

3.1Backdoors

A backdoor in a computer system, a cryptosystem or an algorithm, is a method of bypassing normal authentication, securing remote access to a computer, obtaining access to plaintext, and so on, while attempting to remain undetected. The backdoor may take the form of an installed program (e.g., Back Orifice), or could be a modification to an existing program or hardware device. A specific form of backdoor is

a rootkit, which replaces system binaries and/or hooks into the function calls of an operating system to hide the presence of other programs, users, services and open ports. It may also fake information about disk and memory usage.

3.2 Denial-of-service attack

Unlike other exploits, denials of service attacks are not used to gain unauthorized access or control of a system. They are instead designed to render it unusable. Attackers can deny service to individual victims, such as by deliberately entering a wrong password enough consecutive times to cause the victim account to be locked, or they may overload the capabilities of a machine or network and block all users at once.

3.3 Direct access attacks

Someone who has gained access to a computer can install different types of devices to compromise security, including system modifications, software worms, key loggers, and covert listening devices. The attacker can also easily download large quantities of data onto backup media, for instance CD-R/DVD-R, tape; or portable devices such as key drives, digital cameras or digital audio players. Another common technique is to boot an operating system contained on a CD-ROM or other bootable media and read the data from the hard drive(s) this way. The only way to defeat this is to encrypt the storage media and store the key separate from the system.

3.4 Eavesdropping

Eavesdropping is the act of surreptitiously listening to a private conversation, typically between hosts on a network. For instance, programs such as Carnivore and NarusInsight have been used by the FBI and NSA to eavesdrop on the systems of internet service providers. Even machines that operate as a closed system (i.e., with no contact to the outside world) can be eavesdropped upon via monitoring the faint electro-magnetic transmissions generated by the hardware such as TEMPEST.

3.5 Exploits

An exploit (from the same word in the French language, meaning "achievement", or "accomplishment") is a piece of software, a chunk of data, or sequence of commands that take advantage of a software "bug" or "glitch" in order to cause unintended or unanticipated behavior to occur on computer software, hardware, or something electronic (usually computerized). This frequently includes such things as gaining control of a computer system or allowing privilege escalation or a denial of service attack. The term "exploit" generally refers to small programs designed to take advantage of a software flaw that has been discovered, either remote or local. The code from the exploit program is frequently reused in Trojan horses and computer viruses. In some cases, vulnerability can lie in certain programs' processing of a specific file type, such as a non-executable media file. Some security web sites maintain lists of currently known unpatched vulnerabilities found in common programs (see "External links" below).

3.6 Indirect attacks

An indirect attack is an attack launched by a third-party computer. By using someone else's computer to launch an attack, it becomes far more difficult to track down the actual attacker. There have also been cases where attackers took advantage of public anonymizing systems, such as the tor onion router system.

3.7 Social engineering and human error

A computer system is no more secure than the human systems responsible for its operation. Malicious individuals have regularly penetrated well-designed, secure computer systems by taking advantage of the carelessness of trusted individuals, or by deliberately deceiving them, for example sending messages that they are the system administrator and asking for passwords. This deception is known as social engineering

4. System Information Security (SIS) in Perspective for Application Software and Computers.

There are numerous ways to protect information in computers, including utilizing security-aware design techniques, building on secure operating systems and installing hardware devices designed to protect the computer systems.

4.1 Security and systems design

Although there are many aspects to take into consideration when designing a computer system, security can prove to be very important. According to Symantec, in 2010, 94 percent of organizations polled expect to implement security improvements to their computer systems, with 42 percent claiming cyber security as their top risk.

At the same time, many organizations are improving security and many types of cyber criminals are finding ways to continue their activities. Almost every type of cyber attack is on the rise. In 2009 respondents to the CSI Computer Crime and Security Survey admitted that malware infections, denial-of-service attacks, password sniffing, and web site defacements were significantly higher than in the previous two years.

5. Security Measures for Securing the Information

A state of computer "security" is the conceptual ideal, attained by the use of the three processes: threat prevention, detection, and response. These processes are based on various policies and system components, which include the following:

User account access controls and cryptography can protect systems files and data, respectively.

Firewalls are by far the most common prevention systems from a network security perspective as they can (if properly configured) shield access to internal network services, and block certain kinds of attacks through packet filtering. Firewalls can be both hardware- or software-based.

Intrusion Detection Systems (IDSs) are designed to detect network attacks in progress and assist in post-attack forensics, while audit trails and logs serve a similar function for individual systems.

"Response" is necessarily defined by the assessed security requirements of an individual system and may cover the range from simple upgrade of protections to notification of legal authorities, counter-attacks, and the like. In some special cases, a complete destruction of the compromised system is favored, as it may happen that not all the compromised resources are detected.

Today, computer security comprises mainly "preventive" measures, like firewalls or an exit procedure. A firewall can be defined as a way of filtering network data between a host or a network and another network, such as the Internet, and can be implemented as software running on the machine, hooking into the network stack (or, in the case of most UNIX-based operating systems such as Linux, built into the operating system kernel) to provide real time filtering and blocking. Another implementation is a so-called physical firewall which consists of a separate machine filtering network traffic. Firewalls are common amongst machines that are permanently connected to the Internet.

However, relatively few organizations maintain computer systems with effective detection systems, and fewer still have organized response mechanisms in place. As result, as Reuters points out: “Companies for the first time report they are losing more through electronic theft of data than physical stealing of assets”. The primary obstacle to effective eradication of cyber crime could be traced to excessive reliance on firewalls and other automated "detection" systems. Yet it is basic evidence gathering by using packet capture appliances that puts criminals behind bars.

6. Future Scope of this Study

This is the never ending process of information security it has training for the professionals to secure the information to avoid the unauthorized access of the information of other persons, in current era of technology there are several new ways are coming to hack the information to protect the valuable and confidential information professionals should adopt and develop new kinds of protection methods. Professionals should monitor the security system to avoid and detect the security flaws and check whether the information is accessed by authorized persons only. This makes information security an indispensable part of all the business operations across different domains.

7. Conclusion

This paper given the details about information about the information security. The importance of the security, the issues related to the information security, techniques to preserve the information and including the possibilities of information theft with in how many ways the company information may going to steal with technical details also. And System Information Security perspectives and measure to protect the information also. By referring this paper readers/researchers they got some information about security related issues and that makes an understanding for the readers/researchers for their research work or knowledge purpose for normal readers.

8. Acknowledgement

First I would like to thank my research guide Mr. Ramesh K, for his eminent guidance towards my research work giving me valuable suggestions and supporting for all kinds of research work. Also I would like to thank to Mr. M. A. Kareem, Head of the Department of Department of Computer Science, and Dr. S. M. Khened, Principal and Associate Professor, L.V.D College Raichur, for providing me the facilities to complete this paper. I am thankful to all the staff members of our department for supporting me directly or indirectly for the completion of this research paper. I am thankful to my family and friends for helping me to complete this research paper.

References

[1] http://www.infosec.gov.hk/english/technical/files/overview.pdf.
[2] http://en.wikipedia.org/wiki/Computer_security#Vulnerabilities
[3] Baskerville. Investigating information systems with action research. Communications of the Association for Information Systems, 2(19), 1999.
[4] D.Bell and L.LaPadula. Secure Computer systems: Mathemetical foundations and model. Technical Report M74-244, MITRE Corporation, Bedford MA, USA, 1974.
[5] F.Bjorck. The economics of information systems security. London School of Economics, Department of Information Systems, 1996.
[6] Burrell and G.Morga. Sociological Paradigms and Organizational analysis. Heinemann, London, United Kingdom, 1979.
[7] McGregor. The human side of enterprise. McGraw-Hill, New York NY, USA, 1960.
[8] Cam-Winget, N., Housley, R., Wagner, D., & Walker, J. (2003). Security Flaws in 802.11 Data Link Protocols. Communications of the ACM, 46(5), 35-39.
[9] Cavusoglu, H., Mishra, B., & Raghunathan, S. (2004). A Model for Evaluating IT Security Investments. Communications of the ACM, 47(7), 87-92.
[10] Di Pietro, R., & Mancini, L.V. (2003). Security and Privacy Issues of Handheld and Wearable Wireless Devices. Communications of the ACM, 46(9), 75-79.
[11] Frolick, Mark N. (2003). A New Webmaster’s Guide to Firewalls and Security. Information Systems Management, 20(1), 29-34.

Author Profile

Sri. Sharanappa Patil is working as a Assistant Professor in Department of Computer Science, L.V.D College, Raichur, Karnataka since from 8years. And he has completed B.Sc degree from L.V.D College, Raichur, Karnataka in the year 1999. He finished the M.Sc Information Technology from Periyar University, Selam in 2010. Now he is persuing the Ph.D. He is interested in the research area of Software engineering, Networking and Digital Image Processing.

Sri. Ramesh.K is presently working as Associate Professor in The Department of Computer Science, since 26.09.2012 and Co-Ordinator for The Dept. of Physics of Karnataka State Women's University, Bijapur. His qualification is B.E, M.Tech, (Ph D) in Computer Science & Engineering. He has published six research papers in international journals in the areas of Networking and Algorithms. And he edited four books (Mobile Computing, Programming Foundation, Software engineering, System Simulation).