Free essay on information security concepts

Law, Security

ASSIGN BUSTER

(i) Persuasive E-Commerce

It describes the use of adaptive technologies based on models and profiles of users, to predict user behavior and subsequently design or issue interactive messages that would respond or create the user’s needs to gain a commercial end. The persuasive e-commerce choose varied means to initiate a change in behavior or attitude, through the identification of distinct strategies that may be implemented separately and then predict the most likely decision depending on the users’ choices (Kaptein & Eckles, 2011). Persuasion profiles/models are based on behavioral data, personality, time; demographic characteristics of the user to create interactive technologies that would subsequently predict the needs etc of the user, and help the business to optimize on the possible opportunities. A perfect example of persuasive e-commerce is Amazon. com’s recommender system, which are specifically designed to model the users’ needs based on the searchers that they perform on the website, along with their search histories to recommend books and other merchandize to the users who may just need them. Similar technologies are used by multiple sites, which attempt to predict the attitudes of website users, and help the e-commerce sites to boost the effectiveness of attitudes, which would ultimately translate to a commercial benefit for the websites (Kaptein & Eckles, 2011).

(ii) Client Server Architecture

It refers to a model of computing with distributed application, in which workloads or tasks are partitioned between resource/service providers (servers) and resource requesters (clients). It involves information and data exchange between client and server machines, where a server has resources and powerful processing capacity, which it shares with client machines. While clients and servers may reside on the same system, they are often on separate computer hardware, which communicate over a network, with clients initiating sessions of communication with servers (Nemati, 2008). Many computing functions on the internet, including e-mail exchange, data and web access are founded on the client server architecture, facilitated by protocols such as SMTP, HTTP and Telnet.

Users of online services such as e-banking from a web browser on a client machine to send requests to access, use or retrieve information, data or other resources stored or possessed by a server machine. Once the server receives a request, it processes it, using all the facilities available to it and sends back a response, stores or passes on the output to other machines on the network. This architecture is best suited for sharing of computing resources, since the server stores important resources, including processing power and memory space that may be shared by many client machines, allows central control and has powerful programs to allow effecting task queuing and security, hence efficiency.

(iii) Virtual Private Network

Refers to private, remote computer systems, connected to each other mainly through public infrastructures (including the internet), protected by strict security procedures, and tunneling protocols such as data encryption, password protection, role-based access and restricted users. A Virtual Private Network (VPN) could connect an organization’s head office computers to its branches through public networks (American Online and the National Cyber Security Alliance, 2004). The ATM networks used by banks are an example of

VPNs, which use public networks to connect private computing resources among client machines. There are two major types of VPNs i. e. site-to-site and remote-access VPNs. Site-to-site VPNs permit network interconnection among many users e. g. head office’s internal networks, the company network and the branch networks, while the remote access VPN allows computer users to access remote networks e. g. company employees logging into their company’s intranet. These networks heavily save on computing costs by reducing the need for dedicated lines among different networks with the available infrastructure to connect networks. The need for network users to be properly authenticated, coupled with security protocols as such data encryption, the VPNs are safe, and allow computer users to access limited resources remotely or from different networks without compromising the security of the central networks.

(iv) Security Breach

It is defined as the unauthorized access/acquisition of unencrypted computer data or information, which effectively compromises the confidentiality, integrity or security of the data/information maintained by a computer system or while in transmission. It describes a successful bypass or contravention of security procedures, policies and practices from outside an organization (Choi, Fershtman, & Gandal, 2007). Computer security is geared at ensuring data; information as well as the physical infrastructure are protected from theft, intentional and accidental destruction or damage, or corruption, without affecting the accessibility and productive use of the resources by authentic users.

It ensures stored data integrity, by preventing unauthorized alteration, deletion or processing in order to ensure that the results that are retrieved from the system are both accurate and reliable. As such, access to information or data by authorized individuals, and using the acceptable processes does not amount to a security breach, but any unauthorized access to, and in contravention of access protocols or procedures amounts to a security breach, whether or not the stored information or data is compromised, stolen or altered. In 2011, SONY’s gaming database of clients was hacked into, leading to the loss of sensitive information on its clients, amounting to a severe breach of security for the company and perhaps most crucially for the individual computer users who lost their information to potential criminal agents (Pham, 2011).

(v) Cookies

Also referred to as browser cookie, HTTP cookie or a web cookie is a data piece sent from a web application and stored on the client’s web browser, while the user browses the website. This data would be available to the user, if they browse the same website in subsequent times, allowing the user to save on data input or remember their previous activity (Bavisi, 2009). They are usually designed to allow websites to reliably keep track of their states or user activity, with the number and nature of clicks and signing in among other events.

Since the information originates from, and is stored on the client computer browser, it cannot carry or install malware and viruses on the host computer, despite the fact that third party cookies’ tracking cannot be successfully used in the compilation of long term browsing histories of the user, which effectively jeopardizes the privacy and confidentiality of the computer user.

Cookies do however; serve an important purpose in the modern day web browsing, if they are implemented correctly not least because they minimize data input and the time used, while at once boosting the user convenience (Choi, Fershtman, & Gandal, 2007). Saving of passwords to commonly visited services such as e-mails on one’s computer is an example of a cookie, which stores the username and password on the web browser, which can then be automatically entered into the system for easier access.

(vi) Trojan Horse

It is a malicious standalone program or computer file, which masquerades as a legitimate program/file, can replicate itself, spy or steal data and information, harm the host computer systems or simply result into reduced speed and other inconveniences. Derived from the mythical Greek tales not least because it seeks to appear as a legitimate programs, and unlike computer viruses, which try to inject into other programs, Trojan Horses are self contained programs, which rely on drive by downloads etc to attach themselves on the host machines, before they start running within the host machine. Botnets are perfect examples of Trojan horses, popular with computer hackers, who use self-contained programs installed under guise on host machines, to install a backdoor onto the host machines, which can be subsequently used to access or take control of it. Hackers can easily gain remote access of any computer on a computer network once Trojans are installed. Other uses of Trojan Horses include upload or download of files on the host computer, keystroke logging, computer crashing; theft of data and installation of third party malware (American Online and the National Cyber Security Alliance, 2004).

(vii) Biometric Control

Is a form of authentication, which uses unique, human biological characteristics to control access to computer systems, data or information. Biometric Access Control are based on physiological as well as behavioral characteristics to uniquely identify individuals. These include finger prints, DNA, voice or other human behavior such as typing rhythm and gait, which are slowly replacing or complementing token-based knowledge-based identification systems,

because of the increased reliability and uniqueness of these identifiers. There are varied chemical behavioral aspects that can be used to uniquely identify individuals, and the specific aspects that are chosen for biometric control depend on the practical conditions, the level of security required. Basically, the templates of a person’s biometric identifiers are stored in the computer database, and users seeking access to the system give the identifier e. g. speak to a microphone, sign on a pad or place their hands in a finger print reader, for their identifiers to be compared with the stored template. Biometric control is however more costly and best suited for physical security as compared to knowledge-based identification, which uses passwords and personal experiences in authentication.

(viii) Stenographic Systems

This is a method or system of hiding data, which originally comprised random bits, with vectors superimposed on top in order to allow different security levels of de-encryption, to give the information different levels of protection from unauthorized users. Effectively, files are not just encrypted or stored but the partitions are randomized. The files that are encrypted look like randomized vectors of the partition, and whenever files are kept on a partition, it becomes multiply difficult to decode the stored data, without the algorithms and methods that are specifically designed to decode such information and data. This technologies use memory space inefficiently, but they give important data protection (Bavisi, 2009).

American Online and the National Cyber Security Alliance,. (2004). AOL/NCSA Online Safety Study. New York: AOL/NCSA .

Bavisi, S. (2009). " 22" Computer and Information Security Handbook. London: Morgan Kaufmann Pubblications Elsevier Inc.

Choi, J. P., Fershtman, C., & Gandal, N. (2007). Network Security: Vulnerabilities and Disclosure Policy#. Tal Aviv: CERT/CC.

Kaptein, M., & Eckles, D. (2011). Selecting Efeefctive Means to any End: Futures and Ethics of Persuasion Profiling. Stanford University.

Nemati, H. R. (2008). Information security and ethics: concepts, methodologies, tools and applications, Volume 4. New York: Information Science Reference.

Pham, A. (2011, April 28). PlayStation Network security breach will cost Sony much more than money. Retrieved May 28, 2012, from www. latimes. com: http://articles. latimes. com/2011/apr/28/business/la-fi-0428-ct-sony-hack-20110428