Study on the Security and Trust Issues of E-commerce

Xiaosen Wen [1]

[1] Xijing University, Xi'an, Shaanxi, 710123

346591653@163.com

KEYWORDS: E-commerce; Security and Trust Items

ABSTRACT: Tremendous impact e-commerce development to human society makes a series of research in related fields to become a global hot spots. In recent years, the development of e-commerce has gradually slowed down, which is one of the main security problems that hinder its development. It can be predicted to be into the true meaning of e-commerce era, security must be addressed. This paper argues that the security of e-commerce is based on trust, the sole factor in consumer confidence in e-commerce security, not hinder, the law is to protect the security of e-commerce and trust, and make some recommended measures to enhance user confidence in e-commerce transactions, thus promoting e-commerce fast! healthy development.

I. Introduction

Security of electronic commerce has been emphasis on attention and safety experts, therefore safety technology development continued to be applied, such as: encryption, firewalls, security authentication protocols. Application of these technologies greatly contributed to the development of electronic commerce. With the development of technology, both in hardware or software on the development of e-commerce provides a good environment for development and security assurances. But there is not a valid e-commerce system security assessment system. While some e-commerce security technology have developed appropriate safety standards, but the system as a whole, it is not enough. Safety features include e-commerce system: effectiveness, confidentiality, integrity, reliability (non-repudiation), review capability. Thus a measure of security of e-commerce system will study from several aspects. E-commerce security, people tend to consider the technical aspects, but often overlooked security management, security management in fact more important than the technology. Develop and implement a good security policy more effective than security technology more durable. Technology development is very fast, and the means and methods of implementation of the system against the constantly changing, thus developing good security policy is especially important. The biggest mistake most companies make in terms of security is not able to establish a good strategy and implementation steps, there is no guarantee the implementation of these policies. Security issues are constantly changing, enterprises have installed a firewall, they no longer consider security issues. When the system security architecture changes, you should upgrade and reconfigure the security facilities. So as to effectively use the existing security system to ensure safe operation of e-commerce system. Most companies tend to be less attention to developing e-commerce system security policy, the security system is simply attributable to the technical aspects, this is a misunderstanding. Therefore it should be taken seriously.

II. E-commerce Security Content

An important feature of e-commerce technology is the use of IT technology to transmit and process business information. Thus, e-commerce security as a whole can be divided into two parts: computer network security and business transactions. Computer network security include: computer network security equipment, computer network system security, database security. Wherein the computer network itself against possible security problems exist in the implementation of programs to enhance network security, computer network to ensure its own security as the goal. Business transaction security is closely around the security issues arising when applying traditional business on the Internet, a computer network security on the basis of ensuring the smooth progress of e-commerce process. That e-business confidentiality, integrity, identification, non-counterfeit and non-repudiation. Computer network security and e-commerce transaction security are inseparable in fact, the two complement each other, are indispensable. No computer network security as a basis for a business transaction security is like castles in the air, out of the question. No business transaction security, even if the computer network itself and then security, e-commerce is still unable to meet the specific security requirements.

III. Content Elements of E-commerce Security

As e-commerce is in the Internet environment of business activities, the security of transactions, reliability and anonymity has been an issue of concern in most of the trading activities. Therefore, in order to ensure the security of e-commerce transactions across the smooth conduct of e-commerce security system must have the following elements: 1, the validity and authenticity of the validity and authenticity of the e-commerce system requires effective information, trading entity and authenticity were identified. E-commerce in electronic form to replace the paper, then how to ensure the authenticity and validity of this information in electronic form of the business is the premise of e-commerce. E-commerce as a form of trade, the validity and authenticity of their information will be directly related to the personal, corporate or national economic interests and reputation. Therefore, network failures, operational errors, application errors, hardware failures, software errors arising from the potential threat of computer viruses and to control and prevention, to ensure that the trade data at the determined time, the determined location is valid. 2, confidentiality and privacy of confidential request for information is not disclosed to unauthorized person or entity, is the right to privacy of personal information from being leaked. E-commerce as a means of trade, the information directly on behalf of individuals, companies or national trade secrets. Traditional paper business is by mail a letter or package sent through reliable channels of communication to achieve commercial messages to maintain confidentiality purposes. E-commerce is built on a more open network environment (especially the Internet are more open networks), to maintain trade secrets comprehensive application of e-commerce is an important guarantee. Therefore, to prevent illegal access to information and information during transmission illegally stolen. 3, the integrity of the data integrity of the data requirements for the protection of data against unauthorized additions, deletions, modifications, or alternative, while ensuring data consistency. Simplify e-commerce trade process, reducing human intervention, but also brought the parties to maintain trade business information integrity, unity problems. Due to an unexpected error or fraud data are entered, the parties may lead to differences in business information. In addition, loss of, duplication of information, or the information transmitted during the data transmission of the order difference information will lead to different parties to trade information. Information integrity

trading partners will affect trade transactions and business strategies of the parties, the parties maintain trade information integrity is the foundation of e-commerce applications. Therefore, to prevent the information freely creating, modifying and deleting, at the same time to prevent the loss of information and duplication of data transfer process and ensure that the information transmitted order unity. 4, non-repudiation and reliability requirements of e-commerce system to ensure the reliability of the legitimate users of information resources would not be unfair to refuse; Non-repudiation requirements of e-commerce system to establish effective accountability mechanisms, preventing entities deny their behavior . E-commerce may be directly related to the two sides of the business commercial transactions, to determine how to conduct business transactions are carried out exchanges Founder expectations of the business side of this issue is the key to ensure the smooth conduct of e-commerce. In traditional paper-trade, trading parties by handwritten signature or seal on the trading of contracts, leases or trade documents and other written documents to identify partners, to determine the reliability of contracts, leases, bills and prevent the occurrence of acts of repudiation. This is commonly known as "black and white." In the paperless e-commerce way, identify trade side by handwritten signatures and seals have been impossible. Therefore, to provide reliable identification of individuals, businesses or countries involved in the transaction during the transfer transaction information in order to ensure the sender to send the data can not deny. 5, according to the ability to review the confidentiality and integrity requirements, can take advantage of e-commerce transaction system log file to review the results of the data track.

IV. Facing the Threat of E-commerce System

Standards of customer service model has three components: the server system, network, and client systems. Past operating system running on the host server system are mainly: MVS, VM, VMS, Unix. Now Window NT and Windows 2000 have been applied. Network members include: internal commerce and extranets. The main customers are some of the PC system or some terminal equipment.

E-commerce system, the virus is the most common cause of threat attention. Because the client system insecure architecture (PC / Mac) that makes viral invasion is often successful. To destroy a system, as long as the system can enter some kind of a conventional system code and data without the need for additional special privileges. In previous Windows9x and MacOs8.x operating system, this problem is particularly prominent. Although Windows NT and Windows 2000 are still vulnerable to this attack, but it can limit the authority to activate the virus. Very popular viruses such as: I love you, cover letters and other Unix systems are not infected. Virus attack on the system to cause damage to certain privileges job. In general, multi-level system privileges (such as Unix, VM S) can effectively prevent the virus destroyed the entire system, even if the system infected with a virus, it is only destroy a user's files.

There are many hacking tools (such as: BACK orifice, net bus) remote control, inspection, monitoring of all information of the target user. They can use the target device (PC) as the legitimate user to send the same information to the network, so there is very deceptive, often able to get away without being detected. There are some commercial tools (eg: cucme, vncviewer) also has this feature. Hackers can free download Trojans from some sites, of course, it also has a good side, the system administrator to use these tools to remotely control a large number of workstations, and thus become a powerful tool for system administrators to manage large number of workstations. Its negative aspect is the purpose of some people use it for evil, such as: fraud, modify data, such as eavesdropping.

V. E-commerce System in Privacy Issues

Privacy is one of the fundamental human rights of people, it is accompanied by people of their own dignity, rights, and the emergence of the generation of value, it requires people in social life, in relationships, respect and protect the right to privacy. Including personal privacy and the rights of life is not disturbed and domination control over personal data, specific to the network and e-commerce privacy, privacy protection involves the collection of personal data (including corporate trade secrets), transmission, protection of privacy rights issues in all aspects of storage and processing utilization. Claim form to be divided from the prying eyes of the rights of privacy, the right not to be invaded, the right not to be disturbed, it is not illegal to collect the rights of use; from the content of the right points can have personal qualities privacy (name, identity, likeness, voice, etc.), personal data privacy, the privacy of personal behavior, the content of communications privacy and anonymity of the right to privacy. Where privacy from prying eyes, the rights of invading mainly reflected in the user's personal mailbox, online accounts, credit history on the security and confidentiality; privacy rights are not being interfered mainly reflected in the use of mail users, exchange information and engage in security trading activities Privacy on; the right not to be illegally harvesting is mainly reflected in the user's personal qualities, personal information, etc. not to be exploited on a non-licensed state.

VI. Conclusion

With the rapid development of network, communications and computer technology use, business activities have become a reality. E-commerce with its relatively low cost, simplified business processes. Beyond the enormous profits the constraints of time and the expected mode of operation, widely around the world concerned. However, with the development of electronic commerce, many industry insiders are keenly aware that security issues as a ghost as a shadow player, famous case is Citibank hacked to steal tens of millions of dollars. universally whom shocked, Citibank can not even imagine ensure the security of their network systems. users how assured his own bank account online, to overcome the fear of consumers, the development of e-commerce, it must create a good reputation, safe and secure trading environment.

REFERENCE:

[1]Dimitri Konstantas，Jean-Henry Morin，Agent-based CommercialDissemination of Electronic Information，Computer Networds，2000，32：753～765.

[2]Simon S Y Shim，Vishnu S Pendyala，Meera Sundaram，Business-to-BusinessE-Commerce Frameworks，Computer，2000，10：40～47.

[3]WeberS FA，Modified analytic hierarchy process for automatedManufacturing decision[J]，Interface,1993,23(4)：115～117.