Study on the Information Security based on E-Commerce

Yu-qiao MENG

Jilin Teachers Institute of Engineering and Technology,changchun,130052.China

Email:xuqiongwen@sina.com

Keywords: E-commerce; information security; technology strategy; management system

Abstract. With the progress of economic globalization and information technology, e-commerce also has made a fast development. Meanwhile, the information security in e-commerce industry is becoming more and more important. This paper described information security issues existing in e-commerce, and provided technology strategy and management system on how to enhance the e-commerce information security.

Introduction

E-commerce is a transaction type which conducts an electronic payment through telecommunication network for obtaining information products or real products. With the progress of internationalization, socialization, opening and personalization of network, the virtual market of e-commerce has become the economic focus of global attention. However, the security issues have become the bottleneck of e-commerce development. It will be able to promote a more smooth and healthy development after solving the issues of information security of e-commerce.

Information security in e-commerce

Network attack. Because the computer network operation system, communication protocols and database management system have put emphasis on the convenience of using during the structural design and code design, which may cause the system has security vulnerabilities in many aspects of remote access, access control and password management etc., the hackers may use these vulnerabilities to attack the network. The typical case is that some illegal personnel adopting illegal means to consume network bandwidth or system resources, so that legitimate users can not access network resources normally, and lead to network paralysis and could not provide normal network services.

Information security issues in the storage and transmission process. The network information security issues of e-commerce are mainly shown during the process of transmission, the commonly used illegal means are interception, tampering and deletion of information, illegal personnel intercept information confidential through the analysis of the characteristics of network information transmission, including intercept legitimate users' account and password in order to conduct illegal e-commerce transaction and obtain benefits.

Computer system security. The computer system is the basic equipment of conducting e-commerce transaction. Due to the physical damage itself, it will lead to data loss and information disclosure and some other issues. Meanwhile, the information of network is facing greater risks.

Computer virus attack. The speed of virus spreading is becoming more and more faster due to the high development of network, it has more and more ways to spread as well as cause greater damage. It may cause the paralysis of all system by a simple e-mail, and the network virus of e-commerce may even cause the significant economic losses.

Repudiation issues of both parties. During the process of e-commerce transaction, some users may deny the transaction so as to shirk his/hers responsibility. Such like the following aspects: first, e-commerce information publishers denied the information that sent by themselves. Second, e-commerce information receivers denied information that received by themselves. Third, the buyers denied the order that booked by themselves. Fourth, the sellers have some quality issues, the buyers

denied the original transaction. However, it is very common to see the repudiation issues during the transactions of e-commerce.

Technology strategies for e-commerce information security

Network security strategy. The implementations of network strategy include the following aspects. First, the physical security of network, the first issue is to ensure the physical security of network information, physical security is the basic guarantee of information security as well as essential part of e-commerce information security. Second, firewall technology, the firewall system is not only a hardware or software, but also a component of hardware and software. It can realize access and control between networks, and you can filter the information transmitted over the network through firewall system so as to keep network information resource away from damage. Third, network security scanning technology, network security scanning technology is mainly for scanning on network vulnerabilities so as to reduce the security issues of network system. The network security scanning technology includes network remote security scanning, firewall system scanning and Web sites scanning etc.

The integrity and authenticity strategy of data information. The integrity and authenticity strategy of data information is to ensure the consistency of data, to prevent alteration and destruction by unauthorized access, the main technologies include the following aspects. First, encryption technology, encryption technology is a proactive information security measure, using certain encryption method, converting plaintext into ciphertext to prevent the illegal personnel stealing information of legitimate users and ensure the confidentiality of data. Second, digital signature, digital signature is an effective way of resolving the specified security issues of network communications, it can solve such problems as tampering, imitation, forgery and denial etc. and the function is special and indispensable. Third, digital certificate, digital certificate is a series data related to identity information of network users and it is used to identify the identity of all parties in network communication. The frequently used are cardholder certificate, merchant certificate, payment gateway certificate, bank certificate and issuer certificate etc.

Computer system security strategy. Most of security issues in computer system are mainly shown in the management and most of the systems can be with physical contact, therefore, it should pay more attention to enhance management of computer system storage security. In order to prevent illegal members contacting physical system and making malicious damage, the staff contacting physical system should be authorized, and control the access to directories, files and equipments etc. by the users with the authorization and ensure the information security of e-commerce. The access to network information directories and files is generally divided into change permission, reading permission, creation permission and execution permission etc. The network managers should set appropriate permissions for all users, and control the access to network system through setting access permissions.

The management strategy of e-commerce network security

Improve awareness on significance of network information security. During the management and using of network operation, people always put more emphasis on its practices and benefits, and ignore the security and confidentiality so existing the issues of high requirement of function and low requirement of security and confidentiality, high investment on hardware and software equipments and low investment on safe facilities etc. Therefore, to ensure the information security of e-commerce, the first step is to improve the awareness.

Establish the maintenance rules for the system. The regular maintenance of system is a basic security for a long-term stable operation. The strict management rules for maintenance of e-commerce system shall be set up and undertaken by the specialized technical staffs. The staff should be responsible for relevant daily maintenance work and management of system's hardware and software.

Establish risk prevention mechanism for the network. There are many kinds of network risk prevention measures, which can be divided to three types. First, the prevention before risk occurred, most frequently used information security technologies are belonging to this type; second, the inhibition of risk occurred, such as interception of data package and other methods; third, the remedy after risk occurred, such as data recovery and other measures. The establishing of network risk prevention mechanism for e-commerce can reduce the chance of risk occurrence and remedy as soon as possible in the case of any problem and avoid unnecessary losses.

Strengthen the cultivating of network security professionals. The rapid development of e-commerce provides a newer and higher requirement on cultivating network security professionals. The professionals should keep pace with the times and pay attention to the technological communications with foreign experience, grasp international and domestic advanced security prevention tools and technical measures, improve security awareness and cultivate high qualified professionals to maintain network security.

Strengthen network security legislation and law enforcement. The law is the first defense line of information security. Our country have announced a series of information security regulations from the beginning of 1996, and the establishment and implementation of these regulations play an important role to the standards, coordinate operation and management and the security of e-commerce. With the diversification of means and forms of network crime, network security legislation shall be established and improved not only according to local conditions, but also learning experience related to network information security legislation from abroad. It also needs to amend and supplement existing laws and regulations timely in order to make it more scientifically and perfect in line with our national conditions. In the aspect of law enforcement, it should strengthen the supervision, the lawbreakers must be prosecuted and the law must be strictly enforced to improve the efficiency and quality of law enforcement.

Conclusion

Network information security is the foundation of modern e-commerce development, e-commerce cannot process normally without network information security. With the development of e-commerce, the transaction means of network are becoming more and more abundant. Meanwhile, network security issues have become more prominent. Therefore, it is a strategic issue with highly attention and proactive communications by domestic and international for setting up a system of information security in the environment of e-commerce. Recently, firewall technology, data encryption technology and computer system security technology play a very important role in e-commerce information security. Meanwhile, it is also important to improve relevant laws and regulations, management rules and credit systems in time and to ensure the information security of e-commerce and promote the normal development of e-commerce industry in our country.

References

[1]Ding Xuejun, *"E-commerce Information Security Problems and Solutions"* [J]; Academic Technology, 2013 (2): 83-86.

[2]Wand Dongwei, *"Discussion Briefly on E-commerce Information Security"* [J] ; Network Communications and Security, 2012 (23): 73-74. ;

[3]Wand Xiaoxin, *"Study on E-commerce Information Security Problems and Solutions"* [J] ; Computer and Network, 2013 (29): 205-207.

[4]Hua Duo, *"Discussion Briefly on E-commerce Information Security Problems and Solutions"* [J] ; Da Jia Tan Magazine, 2012 (05): 191-192.

[5]Yu Xiaoxin, Chen Xiaohua, *"Discussion about E-commerce Security Problems and Solutions"* [J] ; Shenzhou Magazine; 2013(02).