E-commerce Security Research

Hanrong Chen
College of Computer and Information Science
Southwest University
Chongqing, China
chrong@swu.edu.cn

JunMei He
College of Computer and Information Science
Southwest University
Chongqing, China
wuqh@swu.edu.cn

***Abstract*-With the speed of computer network development, more economic activity went into the Internet era. It completed through the Internet such as online shopping, bank transfer and other commercial activities. The most important thing is for e-commerce security, e-commerce web site e-commerce activities, security is the foundation and guarantee. This article focuses on security problems in e-commerce sites and solutions strategy.**

Keywords-Internet, e-commerce, website security

I. INTRODUCTION

Currently, Internet applications, e-commerce categories become the fastest growing Internet economy, the main force of the most rapidly. According to China Internet Network Information Center, the latest statistics, as of the end of December 2010, China's netizens reached 457 million, an increase of online shopping users 48.6%, the fastest growing application of the user. Online payment and online banking also 45.8% and 48.2% of the annual growth rate, far more than other types of network applications, more of our economic activity is accelerating into the Internet era. According to statistics, the proportion of small and medium enterprises up to 92.7% Internet access, the larger the proportion of business Internet access is close to 100%. 43% of Chinese companies have an independent website or set up shop in the e-commerce platform; 57.2% of enterprises use the Internet to communicate with customers, to provide consulting services. Network in China in 2010 totaled 523.1 billion yuan shopping.

As a new online e-commerce transactions online by the large number of enterprises and consumers, but its security is still impeding the development of an important issue in e-commerce.

II. E-COMMERCE SECURITY PROBLEMS

According to reports, June 17, 2005 reported that the credit card company MasterCard said about 40 million credit card user's account by a hacker using computer viruses, compromised data included credit card user's name, bank and account number, which can misappropriation of funds to be used. If the hacker really use this information to misappropriation of funds, then those credit card users will not only great economic losses, and the violation of these credit card users' personal privacy. In Japan, there are three banks eBank, Internet banking and Mizuho Bank claimed that there are customers without the knowledge of the deposit has been transferred, type of crime, the inquiry to the bank, know that this is hacking. Mizuho Bank has undergone two similar cases, the loss was ¥ 5,000,000. Metropolitan Police response to crime in Japan high-tech center after receiving the report has been investigated and found from the victim's computer spy software that can automatically record the information entered into the computer, sent through the network to a third party. In addition, the online payment secure, and in-kind goods do not meet, sellers and consumers do not understand each other, worry-free protection, and so cheated after-sales service have a direct impact on further development of e-commerce activities.

E-commerce security problems can be broadly divided into: computer network security and the safety of their own e-commerce activities. The security of e-commerce activity itself can only carry on under a secure computer network environment. As e-commerce agreement with the TCP/IP protocol, its openness allows e-commerce security is threatened. Electronic payment is an important part of e-commerce activities, but if the electronic payment through an open Internet to achieve, and payment information is vulnerable to hackers attack and destruction, that information leaks and damage to a direct threat to the vital interests of businesses and consumers . Coupled with the crazy network virus spread malicious attacks on web server makes the security of e-commerce sites is particularly important. Therefore, we focus on the safety of the basic platform for all kinds of e-commerce - E-commerce Web site.

III. THE SECURITY OF E-COMMERCE WEB PRESENCE

The security of e-commerce sites into the system for security of the system itself and security of the information.The security system itself is the system hardware, operating systems and application software security; information security mainly refers to a variety of information storage and transmission security.

System hardware security is the prerequisite e-commerce website security. Hardware security includes the following: natural disasters (such as lightning, earthquake, fire, flood, etc.), physical damage (such as hard disk damage, equipment service life expires, external damage, etc.), equipment failure (such as power off, the electromagnetic Interference, etc.). electromagnetic leakage (such as computer operation listener process) and so on. Also includes operational errors (such as deleting files,

المنارة للاستشارات

Published by Atlantis Press, Paris, France.
© the authors

www.manaraa.com

formatting the hard disk, line removal, etc.), accidental omissions (such as system power-down, "death " system crash, etc.) and other human factors.Another room computer system may also damage the environment to the system hardware.

Operating system is the core of computer resources management system, which is the application system software platform, its security is directly related to the application of system security, operating system security can be divided into application security and vulnerability scanning. Are there any operating system vulnerabilities, hackers exploited a computer system to obtain unauthorized access to web sites of control. Therefore, the site scans the operating system requires regular and timely patch, uninstall or not install unnecessary services and protocols, to prevent more vulnerability there. In addition, you also need to install the necessary software and firewalls to kill the virus. Also should establish a comprehensive monitoring system on the system, and establish and implement effective user password and access control systems.

Application of e-commerce site is the most important pages on every visit to the site. Businesses through the production site to display e-commerce infrastructure and information platform, complete a series of e-commerce activities. Web designers generally more consideration is how to meet the user's applications, how to implement the services themselves. Web designers with little regard to the Web application development process of the loopholes, and loopholes in the normal use of these is very difficult to find. Some of these vulnerabilities by hackers gained control of the site, the implementation of the attack on the site, make the site suffer.

Database as an information warehouse, is the site to run the core of the information in the database is changed or if disclosure would give the company significant losses often, so their security is very important. Hackers withdraw from a data attack into just less than 10 seconds to be completed. Database management is not possible in such a short period of time that the invasion. When the database management discovered damaged when the data is usually late, and important data has been lost or tampered with. The database hacker attacks are usually very simple. Such as: crack weak passwords or use the default user name and password; use of unused and unwanted service vulnerability in the database; use unpatched database vulnerabilities; SQL injection; stolen unencrypted backup and so on.

In e-commerce activities, information transmission is inevitable, and Internet itself is unsafe. The original Internet is an open network of services for researchers, its builders did not take into account security issues. Therefore, almost all Internet protocols do not consider the security issues. This is the e-commerce activities in one of the most talked about, how in such an insecure environment, secure transmission of information.

IV. E-COMMERCE WEB SITE SECURITY POLICY

Firewall between internal network and external networks constitute a good protective barrier. All the internal network and external network connection between the protective layers to go through this, it transfers data packets between networks in accordance with the provisions of the security policy should be examined to decide whether to allow communication between networks. The use of firewall, internal network hosts do not directly exposed to attacks from the Internet, so the entire internal network security management is transformed into the firewall security management, security management such as more convenient and easier to control, but also the relatively more secure internal network. The most basic function of firewall access control and content control, in addition to the firewall also has a logging feature, the network can access a complete record of the case, as the network is under attack query basis. A firewall is a defensive way, its ability to protect the internal network is limited, the firewall could not vulnerable to virus attacks, on the Internet every day a new threat or attack, the firewall will be attacked. Therefore, the firewall can not protect the internal network, the intruder is likely to pass through the firewall into the internal network.

Once this line of defense against intruders broke into the system, they will without any blocking.Firewall can not initiate testing and analysis of network risk behaviors occur. The intrusion detection system is real-time monitoring of network traffic, it is suspicious transmission alarm or response measures proactive network security equipment. Intrusion detection systems often used for feature detection and anomaly intrusion detection monitoring, tracking system, events, safety record, the system logs and packet, on the occurrence and damage to the system before the intruder detection to intrusion attacks, and use of alarm and protection systems The alarm, block and other responses.

Web site's own security is also very important. Any sites are vulnerable, can effectively prevent the timely detection of vulnerabilities hackers attack the site. Network vulnerability scanner can be used to complete the network vulnerability scan. Device is a network vulnerability vulnerability and risk assessment tools to discover, explore and report on security risks and may be exploited for network security vulnerabilities. In addition, the construction of the site should also take into account the security-related issues. Such as the purchase of anti-tamper system, client data validity and integrity of the inspection, and certification of management pages for common method of hacking the server accordingly in the code design in the design and so on. Web site testing system can also be introduced by third-party security services companies providing remote security testing, because of their professionalism, you can also get satisfactory results.

In order to prevent hacking database, database management personnel should be properly managed the account, the password should be more than one type of characters added to prevent the password is compromised, should also change your password regularly. Do not install the database do not need or never used the service, in time for the database patch. In developing backup strategy should take into account when the specific content of the backup, backup, backup frequency and related storage media.

المنارة للاستشارات

Published by Atlantis Press, Paris, France.
© the authors

www.manaraa.com

Data encryption to prevent illegal good information access and information in the transmission process is illegal to steal. The most important to ensure the integrity of the current methods of information password-based digital signature and authentication is the ability to effectively prevent spoofing.E-mail is the main information on the network means of transmission, but also one of the main e-commerce applications. But it does not have strong security measures, so the Internet Engineering Task Force (IETF) has drafted a draft specification for expanded e-mail security. It added to the standard format for e-mail encryption, authentication and key management functions, allowing the use of public key and private key encryption methods, and supports a variety of encryption tools.

In addition, the prevention of computer viruses is also very important. Focus on ways to cut off the spread of the virus, anti-virus technology to improve network capacity; to prevent the virus into the site to avoid infection, to prevention; website regularly check narcotics, anti-virus, to avoid site damage.

V. THE MANAGEMENT OF E-COMMERCE SITE

E-commerce security management should not only from a purely technical point of view how to solve the problem, but rather from the idea of comprehensive security management to consider.From the perspective of e-commerce environment, technological environment is an important aspect; good laws, regulations, policies, environmental and scientific management, the successful e-commerce environment is another important aspect.In a sense, the latter is more important.

According to the survey, many domestic sites is mainly due to security problems business managers little or no safety awareness. Corporate managers believe that company size is small, does not become a target for hackers, only large companies only a security problem. This attitude, network security out of the question, managers throughout the site management is the most important factor. With the awareness of action will have, will establish a sound e-business management organization system, turn passive defense to active defense, to ensure the safety of the entire site.

Management organization to establish a sound e-commerce system can be characterized by each enterprise's own network or network security level into the various departments to determine the specific security objectives, the establishment of the relevant functional departments, designated the department heads, take responsibility. Regular meetings is very important. Discussed at the meeting should include: information that has emerged within the organization to discuss security issues and gives solutions to the possible risk assessment, formulate and revise the information security-related policies, to provide for the organization's information security guidance and support, coordination of information security management team and the relationship between the various departments to develop and improve scientific and rational information security management system, and so on.

With sound management of e-commerce system is not organized, commerce and the legal system is also very important. Commerce and the legal system is a very complicated system, which includes the legislative, judicial and administrative in many areas, covering the industry, market access, information security and authentication, intellectual property protection, electronic payment, digital signature, Internet content management and liability, and many other legal issues.

Thus, e-commerce management is a means to achieve through the management of security mechanisms to protect e-commerce site security purposes and rules. It is not just software and hardware on site management, including site management and internal use of personnel management, and social support system and a series of related laws and regulations related to the development and improvement.

VI. . SUMMARIES

With the national policy to promote and market opportunities of the traction, the Chinese small and medium Enterprises Website (an independent Web site or Web site), the ratio has reached a higher level. According to China Internet Network Information Center, the latest statistics, as of December 2010 reached 43%, of which 27.8% of the SMEs to establish an independent corporate website. The security of e-commerce sites to become more prominent and important, we believe that with further research to establish a safe and secure e-commerce system is entirely possible..

REFERENCES

[1] YUAN Duan-wu, WANG Ri-fen Research on the Safety Management of Electronic Commerce Websites Information Studies: Theory & Application, 2002 No.06

[2] ZHENG Jian, WEI Hao_cheng, HAN Xing Production and E-commerce Web Site Security Market Modernization 2009 No.02

[3] Liu Lei, Chen Yi Discussion about the website safety and answers tactics Network Security Technology & Application 2010 NO 10

[4] LIU Xiao-yu Analysis on Security of Electronic Commerce Website Journal of Tianjin Vocational Institutes 2008 No.02

[5] Liao Jian-ping Study on the Website Security Software Guide 2010 No.08.

[6] XIAO De-qin, QI Ming, PENG Li-fang E-commerce security technology and applications South China University of Technology Press 2005

[7] HU Guo-sheng E-Commerce Security South China University of Technology Press 2006

[8] GUAN You-qing, WANG Xiao-jun, DONG Xiao-yan E-commerce security technology Beijing University of Posts and Telecommunications Press 2005

المنارة للاستشارات

Published by Atlantis Press, Paris, France.
© the authors

www.manaraa.com