Research on Computer Network Information Technology Security and the Preventive Measures

Min Lai[1, a], Tao Chen[1, b*]

[1] Gannan Medical University, Ganzhou, 341000, China

[a]email, [b]email

* Corresponding Author: Tao Chen

Keywords: Computer network, Information technology security, Preventive measures

Abstract. With the progress of science and technology, computer technology has penetrated into all aspects of social life, has been popularized in the whole society. However, due to the characteristics and defects of the computer network, and other factors, the computer network information security issues have begun to attract widespread attention. This paper mainly analyses the meaning and way of computer network computer network information arrangement, analyzes the existing main problems of network information, the network information security to prevent relevant countermeasures to improve network security, improve the network information system.

Introduction

The connotation of computer network information security from the following several aspects: the broad sense, the computer network information security technology mainly includes information integrity, software reliability, confidentiality and availability. The integrity and authenticity of network data means that the protection is not illegal to change the network data. Another aspect of information technology to protect the safety of computer network, data storage, information requirements in the process of transmission is not illegal, modify or delete missing, the protection of computer network data integrity and authenticity. The confidentiality of network data means to encrypt and protect the confidential information of network users to prevent leakage and theft. The reliability of network system and the reliability of computer network system are the primary characteristics of the security of computer network information technology, that is, the availability and stability of the network. The stable operation of the computer network system, is the precondition and foundation of computer network can be efficient, positive, continuous work, and therefore the most basic features of computer network information technology security and reliability of the network system is the primary goal. Through the file transmission in the computer network and receiving and sending electronic mail, the other side of the transmission of information, online notification and other ways, the two sides or multi-party communication can achieve the purpose. This application is mainly used in electronic automation, office document production, etc., which plays an important role in improving work efficiency and productivity. The computer network system cannot pass the time by collecting information in different regions, summed up in a unified file, will summarize the related data analysis through comprehensive data processing, is sent to the computer, let others get feedback, and resource sharing. Through the network system, the greatest advantage of this use of resources sharing, can greatly improve people's work efficiency, reduce labor costs. At present, the computer network information technology has been popularized in all walks of life in the whole society. In twenty-first Century, the use of computer technology to deal with daily affairs and daily management has become the most prominent feature. While highly popularizing computers, it has also been paid more and more attention to the security of computer network information technology.

Common Problems of Computer Network Information Technology Security

Network Vulnerability. Network vulnerability is caused by operating system software or application software due to programming errors and logical defects. No matter what kind of software, in the development of writing has its own technical loopholes cannot be avoided. The invasion of hackers is through these vulnerabilities to computer viruses and Trojans implantation, to attack and steal the entire computer and control system, and finally to steal important information and data in the computer, or even bring down the entire system. The illegal use of computer network user address generally occurs in the land. Generally speaking, when the address is stolen, the network user displays the dialog box which has been illegally occupied on the top of the computer screen, and informs the user of the occurrence of the situation. Due to the illegal occupation of address only in the high authority of network users happen, and address of the user stealing the identity of their hidden illegal illegal harassment and invasion, so the illegal occupation of network address not only for network information security has also had some negative effects, at the expense of the interests of Internet users. At present, the most direct problem of computer network information security is the objective security problem, that is the external environment security issues. The external environment security problem is mainly a series of problems caused by the external force majeure in the process of using the computer. In spite of the profound impact of computers on human development, computers are still a more vulnerable machine. Therefore, once facing outside many objective problems, such as earthquake, fire, electricity, Water Leakage and many other issues, the lack of effective emergency mechanism for computer are often vulnerable to the direct impact of the basic work to stop the entire server, causing irreparable adverse consequences to individuals and hospital activities.

Virus Invasion. With the further pace of reform and opening up and the development of science and technology, the computer has become a channel of contact with the world. The computer not only ensures the reliability of people's access to data, but also provides accurate web information for people. It provides a broad prospect and development space for the promotion of cultural information and dissemination. In the modern society where computers have become more and more popular, it has become the basic way and tool for people to communicate with each other. The invasion of viruses not only has latent characteristics, but also destroys the information system because of its unique concealment. The vulnerability of the network system is mainly aimed at the basic characteristics of the Internet information technology. Generally speaking, the most significant feature of the Internet information technology which appear in the application process is open, based on open, people can share their information on the Internet, to achieve the optimal allocation of information resources. However, in the process of reality development, the openness of Internet information technology directly results in the vulnerability of network system. Now a lot of network in order to prevent the virus, have installed computer housekeeper and anti-virus software for network maintenance, but because people are not safety consciousness is very strong, so sometimes in times of crisis or other vulnerabilities, easily ignored. This vulnerability is reflected in the ability to withstand network attacks, unable to set up a timely and efficient firewall, network system once attacked, its impact and consequences are linked.

Human Error. Network security accident is not only due to the inevitable technical vulnerability of the software itself, but also caused by the lack of self-protection awareness of the user network security. For example, the protective effect of firewall for some computer network operators in order to avoid the interruption of additional certification procedures of the proxy server firewall, not knowing which to network information security poses a serious threat. Firewall is an important means to guarantee the network security and its control in and out of a network of authority to avoid the interference of external factors and the destruction of the objective, has important protective effect on the computer network security. Many network operators cause intermittent protection, forget the boot maintenance function, resulting in network security risks, so that other network hazards into the room. Network attack is the most common and most common security problem in the Internet Security problem. According to the attack theme division, network attacks can be divided into active and

passive attacks and active attacks refers to the network hacker intrusion activity on the system and server through a variety of ways, the integrity and effectiveness of the damage information for the target of active attack; passive attack refers to the intruder in the network can still keep the target interception, data information of some confidential work under the premise of normal behavior such as stealing. Whether it is active or passive attack attack them on computer network operations and service will produce great harm, network intrusion actions hackers once cause data loss or paralysis of the entire system, the consequences are unimaginable.

Preventive Measures of Information Technology Security Problems of Computer Network

Account Security Management. In view of the current Internet users network account stolen with this problem, in the actual network life, network technical personnel should do a good job of user account security. In general, Internet users in the network activities, usually use a fixed one or several account and password on different sites with different licensing requirements, and the security of the password is low, this will directly cause serious problems in user accounts stolen after the user in each big website information and personal secrets have been leaked. To solve this problem, the user in Internet activities, efforts to set up more complex, high security password should first password, attention cannot be set with the same or too simple account password, nor set and basic personal information is closely related to the personal password, such as birthday, ID number etc. Secondly; in the process of setting a password, the user should be carried out using numbers, letters and special symbol combinations, and to change the password regularly, so as to effectively improve the level of security password. Information encryption technology has the characteristics of small cost and strong protection, and it is the core part of network security technology and theory. With the rapid development of computer network technology and communication technology, cryptography has been widely concerned and popularized all over the world. Cryptography is not only used for encryption and decryption of information, but also gradually develops into security mechanisms, including identity authentication, digital signature, access control and so on. By using the principle and method of cryptography, the information encryption technology transforms the information reversibly, so that the illegal access cannot understand the true meaning of information.

Security Vulnerability Detection. Network security vulnerability detection is an effective means to ensure the security of computer network system, and plays an important role in the security of computer network system. It includes three aspects: computer system vulnerability detection, port monitoring and detection. Through the port monitoring and detection to achieve a comprehensive understanding of the system itself, which ports are used, what network interactive services; computer operating system type information can be detected. The use of technical means to detect the network security vulnerabilities, security problems of computer network system found in the attackers found safety problems existing in order to take the computer, network security measures, strengthen the protection of information security. Vulnerabilities and patches are the product of a series of possible deficiencies in current Internet activities. In the computer network information technology security measures, you can also install antivirus software, but also automatically retain the virus retained in the computer automatically. Access control technology is only allowed to access limited resources, protection of information resources, access control technology to those without access to the malicious user access or accidental access, protection of the use of information resources. Antivirus software is an important part of computer virus defense network information system, which can automatically identify the risk information, automatic upgrade and automatic scanning and other functions, which can effectively resist the erosion of computer virus. Antivirus software is widely applied to various fields of computer network, and enhance the safety performance of the computer network, the effective control of the virus on the computer, so that people use the computer network information security technology. Vulnerability is the weakness that computer network system has not found in the process of service operation, and network hacker can use these weaknesses to achieve effective intrusion to computer system in attack activities. From the technical level, the computer network system in the running process, almost could not exist without loopholes and defects, and to

effectively solve this problem, the most significant measures in the installation of the corresponding vulnerabilities and patches. First of all, users in the use of network services, should use specialized software or scanner of computer vulnerabilities timely scan; secondly, after scanning found loopholes should focus on the vulnerability remediation activities, and download the corresponding patches.

Data Backup Technology. In order to ensure data security and failures can be effectively restored, data storage and backup is very important, using the backup data to restore the entire system, including user data, system parameters and environmental parameters. Before the data backup, we should carefully consider the backup cycle, time, mode, remote storage mode, storage medium, information resources, data assurance, etc., using full backup and incremental backup mode. The advantages of full backup are high reliability and short recovery time; the disadvantage of full backup is that it occupies more resources and longer backup time, but also occupies more backup storage media. The advantage of incremental backup is that the backup time is short, the resource is small, and the amount of backup media is less. After selecting a good backup mode, the backup cycle and time should be further developed, and backup work should be carried out regularly. Backup itself is to ensure data security, in order to ensure the timely recovery of business after disaster. Full back up data stored in the mobile hard disk, the incremental backup data stored in the public disk and disk, with full backup and incremental backup combination of mobile hard disk storage and combination, to ensure the integrity and accuracy of data disaster recovery. Intrusion detection, as the second security measure after the firewall, has the characteristics of real-time detection, active and fast response, and is the key component to ensure the security of the network system. Intrusion detection on the external and inner attacks and misuse of the real-time protection and the performance of the network does not have any effect, it mainly includes data extraction, analysis, intrusion response of four parts processing and remote management. Intrusion detection is the real-time analysis of the user, system activities and other major detection tasks, monitoring the computer system at all times, analyzing and reporting the characteristics of attacks, to ensure the integrity of the system and data security information.

Conclusion

The construction of computer network security measures is not only an important measure to maintain social security and establish a harmonious society, but also the key to ensure the smooth progress of the network itself. The importance of the security of computer network information technology must be fully realized that the main factors influencing the safety of computer network information technology to accurately grasp, from various aspects of computer network operation, each process of comprehensive management, multi-pronged approach to ensure the safety of computer network and efficient operation, so as to promote the stable and harmonious development of society.

References

[1] Pei Lianqun, Liu Hailing. Research on Computer Network Information Technology Security and Preventive Measures [J]. Cyberspace Security, 2016(5): 86-87.

[2] Luo Yadong. Computer network information technology security and countermeasure analysis [J]. Electronic Test, 2014(24): 64-66.

[3] Guo Lu. Countermeasures Research About ComputerNetwork Information TechnologySecurity [J]. Cyberspace Security, 2015(5): 19-20.

[4] Liu Junfeng. Computer Network Information Security in the Application of Virtual Private Network Technology [J]. Wireless Internet Technology, 2016(12): 135-136.