Security Protection Strategies of Computer Communication Network

Jiangyan Sun

Modern Education Technology Center, Xi'an International University, Xi'an, 710077, China

Abstract

Computer communication network is widely used in all walks of life, which greatly facilitates people's work and life. However, at the same time, the security of the computer communication network also brings many negative effects to people. This paper discusses the common problems of computer communication network security, and gives the measures such as centralizing the software management, improving the hardware performance, enhancing the security awareness and encryptingthe important data to strengthen the security protection of computer network to provide some references for the relative teachers.

Keywords:security protection, computer communication network, network management

1. Concept of network security computer communication

Computer network is a new form of communication, which is combined by the computer technology and the communication technology. The communication line is connected with a plurality of computing devices which are in different geographical positions and can be operated independently, and the corresponding software is configured to achieve the communication system of the computer resource sharing purpose. The fundamental purpose of network information security is to prevent the transmission of information via the Internet from being illegally used, from the enterprise and individual perspective, involving personal privacy or commercial interests. The confidentiality, integrity and authenticity should pay attention to avoid others, violate personal interests and privacy. Computer network communication system, and computer device connection is

not simple as well as the corresponding computer control software connection management, this only refers to the computer network communication technology support system. Computer network communication system is the most critical amount of information stored in the system between the Internet and private information this information includes not only the Internet users have uploaded every kind of information and Internet users, including all Internet operators provided for Internet users every kind of service function, in order to build a perfect computer communication network the safety management system. We must understand the content of computer communication network from various aspects and formulate the corresponding safety control measures according to the specific characteristics of the information.

2. Problems of network security computer communication

There are still many problems in the current computer network communication security. These problems are mainly dividedin three aspects:

First, the technical personnel are not professional enough. In the actual work, the computer network is an important subject. In order to effectively use the network will need a number of professional and technical personnel. But from the current actual situation, the level of computer network security technical personnel is uneven. Technical personnel's own quality is the current more typical of a problem. If the problem cannot be solved effectively, it will be very easy to create security vulnerabilities. The entire system will become chaotic. Most of the current network management and network security awareness not strong, often some human errors, such as the password, the password is too simple, even directly to the password leaked to others, there are security management settings do not regulate the operation lead to safety hazards. There are some criminals or hackers to steal legal identity into the network and then a series of damage, malicious theft, tampering with the user part or all of the data, and even direct damaging the data.

Second, the prevention system is not complete. In the context of rapid development of information technology, network security issues have become increasingly prominent. The network security problem is mainly caused by viruses, hackers and malicious attacks and other forms. The control and prevention system is not perfect will cause serious impact to the system. The computer software system mainly refers to the loopholes in the software design is not considered, leading to the existence of certain defects of communication protocol and software application system, these bugs once some illegal molecules or hackers that will exploit these vulnerabilities invasion computer system. The cracks brought by the hacker may lead to paralysis of the entire computer system.

Third, the management mechanism is not perfect. From the perspective of the management system, the current computer communication management mechanism in China is not perfect. The management mechanism only pays attention to the economic benefits, ignoring the network security. It is a typical problem in China.

3. Security protection strategies of computer communication network

3.1 Centralize software management

The centralized management of software is an important part of computer communication network security. The centralized management of software is not only related to the quality of computer communication network protection, but also related to the security of the whole computer communication network. In order to increase the security of the computer communication network to a greater extent, not only the computer software security mechanism should be installed, but also the detection system technology should be used in combination. Of course, network security check software now has their testing methods, to detect the transmission of multiple computer communication network data to achieve to determine the safety of information transmission while monitoring of computer communication network. Bulk purchase is a general preference for almost all major software vendors. Centralized managementis conducive to the implementation of mass procurement. Centralized and unified management, to avoid the personal or sub sector information is poor or poor management led to the enjoyment of the many services cannot enjoy, including the savings of funds. If the enterprise is bigger, the loss of this part of the funds is very large. In addition, some software products allow ownership transfer, the enterprise can be under appropriate conditions, the transfer of purchased software products, to maximize profits. By strengthening the management of computer software can create a good image of the intellectual property rights of enterprises. The centralized management model can effectively adjust and make full use of the computer software resources in the enterprise.

3.2 Improve hardware performance

The security of computer communication network is based on the reliability of hardware performance. The general protection of the computer communication network security issues, from the following aspects, on the one hand should be based on the current technology, computer communication network in the process of development, generally only pay attention to the actual effect, on the contrary in protective security issues but not enough attention, therefore lead to computer hardware equipment the safety problems of closed. To this end, the relevant personnel to its design process, to continue to strengthen its defense technology, and computer system performance, in order to strengthen the security of the computer two on the other hand, to the hardware equipment safety of computer security, carries on the design, to the full range of in-depth consideration of security issues in equipment there, with security issues, to take protective measures, based on the computer communication network security performance guarantee, and guarantee letter. There are security risks during the process of transfer information, and related security protocols are optimized to guarantee the integrity of the information transmission. In the protection of computer

communication network security, not only to consider the effectiveness of computer communication network, but also should consider the security of computer communication network system itself. Therefore, the computer communication network data confidentiality and communication protocols should be considered in advance. In particular, it should be designed to identify security levels and security measures, reducing the vulnerability of network systemto prevent the invasion of the virus.

3.3 Strengthen security awareness

Technical personnel must strengthen their own security awareness. Computer communication network technology is an important means to safeguard the security of the system. At the same time of the use of computer network communication technology, we need some corresponding measures to the auxiliary. The accuracy of computer communication network security problems can be normal use of the computer and information. Therefore, the technical personnel can optimize the safety work of the publicity, and actively use some new technology, but in the application to ensure that the level of the technology itself. In addition, we must constantly optimize the technical personnel training system, in order to train the security awareness of technical personnel. It can grasp the professional and professional computer technology, computer communication network security protection technology, and strengthen technical personnel security awareness and prevention of network attacks to interference. In the process of using the computer communication network, it will inevitably encounter from external attacks, and the integrity of the information impact. Therefore daily life and work, we need to take the necessary lightning protection measures to avoid the installation of lightning rod to do defense work, and then to avoid the impact of computer communication when lightning weather in rabbits. We also need to regular the network and check the line to reduce the security emergency.

3.4 Encrypt important data

Data encryption transmission is an important method to protect the security of network information. The link encryption and end to end encryption are common encryption methods. The purpose of link encryption is to protect the link information security between network nodes. The purpose of endpoint encryption is to provide protection to the data of the source end user to the destination end user. Link encryption is mainly refers to the basic information encryption on the computer network communication links, the use of this way to carry out network information transmission security protection, usually also known as online encryption. The first is the information encryption operation in data transmission before operation, after on the basis of network nodes gradually decrypt decryption, after the completion of the need to re encrypt, using this method using different types of keys for data encryption and decryption operations according to the number of operating continuously in the transmission process, the absolute guarantee to reach efficient data security in some degree the. The end

to end encryption technology mainly refers to the transmission of data in the process of data transmission. When the data transmission is received before all the links cannot be carried out decryption operation, to achieve a high degree of computer network security purposes. Theend to end encryption technology can effectively curb node decryption defects. Theend to end encryption technology in the practical application process, other users can normally use the computer network and will not be adversely affected, but the end-to-end encryption work is the most important need to do security work. Compared with link encryption, the end to end encryption system is cheaper, and more reliable and easier to design and maintain.

4. Conclusion

In short, the computer communication network has become an important part of people's life and work. This paper gives some measures of the security protection of computer communication network. However, with the continuous development of computer communication network technology, the network will face some new security problems. Therefore, we should continuously develop more comprehensive and more practical methodsof security protection of computer network in the future.

References

[1]Ma Yuhong, The Function and Significance of Network Security Protocol in Computer Communication Technology, Wireless Internet Technology, 12(8), pp. 10-11, 2015.
[2]Sheng Hong, Analysis of computer network communications security issues and prevention strategies to explore, Electronic Test, 12(7), pp. 65-67, 2015.
[3]Li Jiawei, Computer network communication analysis of the security issues and preventive measures, Network Security Technology & Application, 14(11), pp.116-118, 2014
[4]Shao Kangning, Research on Data EncryptionTechnology in Computer Network Communication Security, Information Security and Technology, 7(2), pp. 29-32, 2016.