Universe
Scientific Publishing

Exploration of computer network technology and security management and maintenance

Quan Liu

China University of Geosciences (Beijing) Information Network and Data Center, Beijing 100083, China.

Abstract: With the rapid development of computer network technology, people's production and life style have undergone great changes. Due to the universal application and promotion of computer network in all walks of life, coupled with the deepening of smart phones, it makes people become more and more dependent on the information on the network. With the development of computer network technology, people's work, production and life have been greatly improved, but at the same time it also brings some information security problems related to it. In recent years, the network information security problems that have frequently appeared and been detected in China are strong examples. In the era of networking and informationization, enhancing people's understanding of computer network security and managing and protecting it are important means to ensure the normal operation of computer networks and safeguard information security.

Keywords: Computer; Network Technology; Security Management; Maintenance Measures

Introduction

From the point of view of realistic needs, computer network system security management and maintenance is of great significance under the premise of ensuring information security. With the opening of the network environment and interaction increasingly in-depth, all kinds of network technology has become an important support for network security management and maintenance, focusing on solving the network operation loopholes, the lack of monitoring and protection capacity is weak and other issues, to promote the safe and stable operation of computer networks.

1. Definition of computer network security technology

Computer network security technology is an important part of the computer management process. The use of appropriate security programs and processing methods can adequately protect computer software, ensure the security of data, prevent important data from being maliciously attacked or destroyed, and prevent the loss of data. Ordinary users can securely transmit private or confidential information when using the network. Network operators need to ensure the security of data transmission as well as provide timely defense and control against unexpected events.

2. Computer network security technology

Common security technologies for computer networks include anti-virus systems, network intrusion detection, firewalls, network security scanning, and data encryption. Among these technologies, firewall technology is the most commonly used, the most valuable application is network intrusion detection technology and anti-virus technology, followed by network security scanning technology, of which data encryption is the most promising. After adopting computer network security technology, the security of data can be effectively guaranteed, preventing the occurrence of security accidents, so that the security of the computer has been significantly improved.

2.1. Firewall technology

Firewall technology includes hardware and software located at the edge of the computer network that protects data on both the internal and external networks. By setting access rights, it realizes the control of access and communication between the internal and external networks of the enterprise and prevents the invasion of external insecurity factors. In addition, firewall technology can effectively control the transmission of internal data to the external network, so as to provide all-round protection for the information in the computer system. Filtering firewall and application gateway are the two most widely used technologies in firewall technology. Filtering firewall is to judge the legitimacy of data packets and whether the data is released by the firewall system by analyzing the input and output data packets in detail and grasping various information contained in the data packets, such as addresses. If the packet is ultimately judged to be ineligible, it is discarded and cannot enter the next system. Application gateways involve processing packets more efficiently during the filtering process. This is done on the principle of improving filtering efficiency and generating reports, specifically application service logs. In addition, application gateways have features such as data copying and transmission, which prevents hosts with different levels of trust from communicating with each other.

2.2. Data encryption technology

Data encryption is the process of encrypting the core of the data and then transmitting and storing it formally to enhance the confidentiality of the data. If the receiver wishes to know the encrypted data, he/she needs to enter the correct key. This can effectively avoid data being attacked by outside non-security, thus ensuring the security and integrity of the data. There are two main types of encryption for data encryption, namely symmetric encryption and asymmetric encryption. Symmetric encryption refers to the fact that the key for encryption is the same as the key for decryption, while asymmetric encryption technology refers to the difference between the encryption and decryption keys. In addition, the key length has an impact on data security. Therefore, data encryption technology should conform to the development trend of the times, and a variety of feature encryption techniques should be used when constructing database systems to reduce the incidence of network data theft events and ensure the security of information.

2.3. Network intrusion detection techniques

By analyzing different types of data information, it determines whether there is any theft and compares with the situation in the system to draw its characteristics. The system is able to send invasion information to the firewall in a timely manner when illegal invasion behavior is detected, and use the firewall to control the data, as well as regulate the access rights to ensure the security of the network. At the same time, it is able to detect and intercept the attacks in the network in real time and cut off the harm it causes to the system, greatly reducing the probability of suffering from network attacks and enhancing the security of the network. In order to better utilize their technical advantages, better meet the needs of users, reduce the security of the system, and guarantee the security of information resources, which requires everyone to continuously make improvements.

2.4. Anti-virus technology

Computer viruses can damage both the hardware and software of a computer. Computer viruses are highly insidious and often difficult to detect. It spreads quickly, has a great impact on the computer network, destroys file information, and makes the computer appear blue screen phenomenon and can not be used. Therefore, rapid detection and blocking of viruses is particularly important. After installing anti-virus software on servers and hosts, once there is a virus, it will be compared with the virus in the database, and once it is confirmed, it will stop the virus from attacking computer hardware and software. In order to detect and block viruses, the database needs to be updated in a timely manner. In addition, computers should be checked frequently for viruses to ensure the security of information and data.

3. Computer network security management and maintenance measures

3.1. Construct a perfect security system and strengthen network security management.

In order to ensure the safe and stable work of computer networks, a scientific and reasonable security architecture is needed as a guarantee. To this end, firewall technology, data encryption and access control are used to establish a comprehensive information security system to guarantee the security and stability of data storage, transmission and internal and external network structures in the information system. Data and information are analyzed, controlled, backed up, stored, and encrypted to ensure that there is no disorder or anomaly of data in the network environment. In addition, focusing on the open and interactive characteristics of the network, strengthen the various types of vulnerability and fragility of the computer network system, so that it is protected from external attacks from the network, which in a way undermines the security and stability of the network system, and continue to improve the level of security and protection of the network.

3.2. Focus on daily management and maintenance of network systems

Computer network administrators need to have a strong sense of network security, for general network attacks, pre-formulation of flexible processing methods, and do a good job of prevention and management. Computer administrators in the face of network attacks or other attacks, the need for different attack methods and specific circumstances, pre-detection and assessment, and accordingly take appropriate management countermeasures. Among them, pre-scanning and prevention of the data and information involved in the new situation is a prerequisite for a good comprehensive defense against attacks, and linked to the real environment in order to develop a set of effective countermeasures to ensure the successful implementation of distributed prevention of attacks, and enhance the efficiency of the use of a variety of network security technologies. In their daily work, computer managers should do a good job of daily security monitoring of computer network systems and system upgrades, regularly detect Trojan horses and viruses, and repair system weaknesses in a timely manner in order to enhance the security of the network system. Under the support of a variety of safe network protection technology, computer network managers and engineers use more perfect algorithms and intelligent technology to carry out programming and modeling to maximize the flexible processing to meet the diversified needs of users, and to give targeted technical services to maximize the security and stability of the computer network.

4. Concluding remarks

In summary, with the rapid development of computer network technology, network security has become an important factor affecting national security, personal privacy and property security. Therefore, network security has become a popular research topic. Networks are characterized by openness, and the article lays the foundation for the further development of computer network technology by recognizing and analyzing various possible security threat factors and proposing corresponding countermeasures.

References

[1] Zheng Yu. Exploration of computer network technology and security management and maintenance[J]. Industrial Innovation Research,2023,(20):125-127.

[2] Zhang Zhiqiang. A preliminary study on computer network technology and security management and maintenance[J]. Digital Technology and Application,2021,39(07):172-174.

[3] Dong Jingli. A preliminary study on computer network technology and security management and maintenance[J]. Digital Communication World,2020,(04):118.