Research on Computer Network Security Technology

Dong Tang[1], Yixin Yu [2]

[1] Chongqing Chemical Industry Vocational College, Chongqing, 401220, China

[2] Chongqing Electronic Information College, Chongqing, 400900, China

Keywords: Computer Network Security, Information Technology, Management and Improvement

Abstract: Computer networks are characterized by interconnectivity and openness, which leads to computer networks being vulnerable to malware, hackers and other unscrupulous attacks. Therefore, the confidentiality and security of network information has become a key issue affecting the development and application of computers. This paper discusses the computer network management and computer network security technology separately, and discusses the related content of computer network management on the basis of clarifying the influencing factors of network security, the identity authentication technology, firewall technology, encryption technology, and intrusion detection technology. The anti-virus technology has been analyzed accordingly, which is intended to provide reference and support for the development of computer network management and the practical application of security technology.

1. Introduction

With the rapid development of science and technology, China has entered the information age with the core of the network. However, behind the prosperity of science and technology, a series of security issues have also attracted people's attention. It can be said that computer networks are not only an effective driving force for social development, but also their own existing security issues have brought new challenges to people. It has become an urgent problem to be solved in the face of computer network applications. Therefore, it is necessary to study the computer network management and security technology, and to clarify the relevant content. It has positive practical significance for the long-term, stable development and better service of the computer network.

2. Computer Network Management

A reliable and stable computer network is what every user wants. When a network component is effective, the network management system is required to quickly discharge the fault source and process it in a timely manner. Generally speaking, fault management includes detecting faults, isolating faults, and correcting faults. The fault detection is based on the detection of the status of the network components. In general, simple non-critical faults are recorded in the error log, and no special processing is required. For some serious faults, an alarm is required, that is, a notification is sent to the network management operator. Network management applications should implement alarm processing based on relevant information. When encountering more complex network failures, the network management system should identify the cause of the failure through a series of diagnostic tests. Billing management is a record of the use of network resources, the purpose of which is to control and detect network operating costs and expenses. This form of management is particularly important in the application of some public networks. Billing management can estimate the cost and expense of using network resources and clarify the resources used. At the same time, the network administrator can also regulate the maximum usage fee of the user, thereby controlling the excessive occupancy of the network resources by the user, thereby indirectly promoting the improvement of the network efficiency.

Configuration management is an important part of computer network management. It initializes the network and implements network configuration to implement network service provision. Configuration management is a management form that integrates identification, definition, control,

  DOI: 10.25236/iccse.18.081

and monitoring. It has the necessary functions of a network object. Its management implementation aims to optimize network performance or a specific function.

Performance management is related to the performance of system communication efficiency, resource operation and other performance, and its performance mechanism is the monitoring and analysis of the managed network and services. Analysis of performance results in a diagnostic test being penalized or network reconfigured to maintain network performance. Performance management collects and analyzes the status data information of the currently managed network, and maintains and analyzes the performance log.

Security has always been a weak link in computer networks. In addition, users' high requirements for security have made the importance of network security management more important, and the role of the player is becoming more and more important. The implementation of management is mainly the application network. Security technology to provide a powerful guarantee for the application of computer networks.

3. Computer network security influencing factors and security technology

The security impact factors of computer networks mainly include the following aspects: First, unauthorized access. It mainly refers to the super-rights use or abnormal use of information resources and network equipment; second, it is a fake legitimate user. It mainly refers to obtaining illegal use rights through various illegal means of deception or counterfeiting; third, it destroys data integrity. Fourth, refused to serve. When the authorized entity has a delay in performing the right access or emergency operation, its service will be rejected; fifth, the virus threat. Intentional, unintentional destruction, modification, or modification of data in the absence of monitoring and unauthorized access. With the increasing popularity of computer networks, people have a certain dependence on computer networks, and computer viruses, as a negative product of computer development, have serious impacts and threats on the application of computer networks.

This technique is the process of confirming the identity of the communicating party, that is, the user must prove his identity when sending a clear service to the system. Typically, identity authentication technology uses a combination of biotechnology, electronic technology, or a combination of the two technologies to prevent unauthorized users from entering the process. Common methods of identity authentication include smart card technology, authentication mechanism based on authentication third parties, and password authentication method. Generally speaking, the authorization mechanism is associated with the identity authentication. After confirming the identity of the application service client, the service provider needs to grant the corresponding permission to the access action, thereby specifying the scope of the customer access.

Syntheticity is the characteristic of this technology. Its essence is to control the access rights of the network, forcing all links to be checked to prevent the network from being damaged and interfered by the outside world. As a control isolation technology, firewall technology prevents illegal access by setting corresponding barriers between the network and the insecure network, or applying a firewall to prevent illegal output of important information on the enterprise network. Usually, the purpose of setting up firewall software between the enterprise network and the Internet is to maintain the security of the internal information system. The enterprise information system applies access from the Internet through selective acceptance. It can prohibit or allow a type of Implementation of specific IP addresses can also reject or receive applications of a specific type of IP on TCP/IP.

Electronic documents are easy to spread and easy to spread, which easily leads to the loss of information. In order to prevent this from happening, it is necessary to apply encryption technology to keep confidential the electronic files or databases stored in the network, so that the contents of the files are illegally borrowed or not. In the current network transmission, "double key code" encryption is a commonly used form. The communicator simultaneously grasps the public key and the decryption key. As long as the decryption key does not leak out, the third party has a large Difficulty. Therefore, even if the electronic file is illegally intercepted, its content will not be leaked, thus avoiding the drawbacks caused by the characteristics of the electronic file itself.

In computer network management, in order to comprehensively strengthen the level of network management and comprehensively improve the quality of network security management, it should also actively introduce network security management of cloud computing. Practice has proved that the use of such cloud computing methods and conditions can comprehensively improve the operational level and security of computer networks. However, it should be noted that when using cloud computing for network security management, it is necessary to seek advantages and avoid disadvantages. First of all, in the network security management, based on the cloud computing method, we should pay attention to killing network viruses from the source, especially in the security management of search engines, accurately detecting illegal network access, illegal intrusion, illegal links, and so on. Second, three layers of network protection. In computer network security management, cloud computing can be used to build a triple security of network security. By detecting IP and port, the virus can be intercepted, the characteristics of the virus can be analyzed, and the illegal access of the network can be effectively locked. Finally, using this technical means, scientific prevention and control of important files, servers, etc. in the computer host device can also be realized.

In computer network application and management, how to ensure information security is the primary problem in open networks. In order to scientifically protect user information and effectively improve information security, scientific information encryption technology should be applied. Through this secure encryption technology, the information being transmitted in the computer network can be scientifically encrypted, and the information data can be converted into other types of encryption. Even if the information is stolen, the illegal personnel cannot obtain the content of the information. Greatly improved information security. In the application practice of the encryption technology, information encryption technology such as public key cryptography can be adopted. This encryption technology can be widely applied in an open shared network, and its encryption effect and security protection capability are relatively strong, and can be more convenient. Digital signature and information verification.

In the process of computer network management, in order to effectively deal with network risks and scientifically deal with network vulnerabilities, a scientific and comprehensive network security risk assessment mechanism should be constructed to timely analyze the security vulnerabilities existing in computer networks and timely conduct early warning and processing. First of all, in the process of network security risk assessment, the network security risk assessment model should be comprehensively constructed in combination with the characteristics of computer network management, and the neural network should be applied in computer network security evaluation. First, scientifically analyze the types of cyber risks, especially the attacks that the network is vulnerable to. Once suspicious targets are found, they should be cleaned up and killed in time to effectively reduce the frequency of attacks on computer networks and fully guarantee network security. Second, strengthen the risk prevention and control of computer hosts. In this system, it is possible to comprehensively identify the risks and hidden dangers that are easily encountered in the host computer, and at the same time, it can also strengthen the calculation and prevention of the host risk. Finally, the use of the system should also achieve management and prevention of the network layer, and comprehensively strengthen the risk calculation and processing of the network layer.

4. Conclusion

At present, the application of computer networks is becoming more and more popular. While bringing great convenience to people, it also brings certain hidden dangers, and the network security problem is becoming more and more serious. The computer network management content is clarified, and based on the network security influence factors, the reasonable and effective application of computer network security technology is emphasized, so that the computer network security problem is effectively solved, which lays a solid foundation for the future development and application of the computer network.

References

[1] Chang Li. Discussion on computer network security technology [J]. China Management Information, 2010, 22

[2] Xing Yunxin. Discussion on current computer network security technology [J]. China E-commerce, 2011, 12

[3] Tang Lei. Computer network management and related security technology analysis [J]. Electronic World, 2012, 3

[4] Wang Hang. Discussion on the function and application of computer network management [J]. Enterprise Technology and Development, 2011, 8

[5] Zhang Dan. Recognition of computer network management [J]. Heilongjiang Science and Technology Information, 2011, 33