Studies in Social Science Research
ISSN 2690-0793 (Print) ISSN 2690-0785 (Online)
Vol. 4, No. 3, 2023
www.scholink.org/ojs/index.php/sssr

Original Paper

On Computer Communication Network Security Maintenance Measures

Hongqiao Wang[1]

[1] Xihua University Chengdu, Sichuan, 610039, China

Received: July 6, 2023 Accepted: July 21, 2023 Online Published: July 24, 2023

doi:10.22158/sssr.v4n3p134 URL: http://dx.doi.org/10.22158/sssr.v4n3p134

Abstract

With the rapid development of China's science and technology, today's Internet communication technology has also followed the ever-changing, but there is still a certain network communication information security problems, and this problem is not to be underestimated. Network communication security has a close relationship with national important documents and information protection confidentiality, social security and stability, national development, social and economic development. The use of Internet technology to commit crimes generally does not leave traces of the crime, which increases the chances of using the network to commit crimes.

Keywords

Computer, Communication network, Security maintenance measures

1. Introduction

In the current information age context of computer communication technology level continues to improve, although it brings convenience to people's daily life as well as work, but the phenomenon of data and information theft, hacking and virus invasion and other phenomena are common, network security problems occur from time to time. Computer communication network security has become an important issue in the development of computer communication network at this stage, which should comprehensively analyze the influencing factors, based on the current situation of computer communication network system operation and the existence of security problems, to take targeted measures.

2. At This Stage of Computer Communication Network System Operation in the Process of Existing Security Problems

2.1 The System Itself Has Defects and Deficiencies

The survey found that the main deficiencies existing in the computer communication network system are manifested in the following aspects. First, the innate openness of the network is the main source of security problems. In the context of the current Internet era, openness is the root cause of computer communication network security problems, although the computer network users through the Internet can timely access to the required information materials, but the protection of user data and its important information and so on needs to be further strengthened. Secondly, the main defects of the computer communication network is also manifested in the system software, especially the rapid development of information technology, but did not quickly update the software, can not effectively adapt to the needs of development, so that the system's own problems and defects gradually exposed. This is a more common problem at this stage, at the same time, it is also a computer communication network defects themselves.

2.2 The Existence of Computer Viruses

The existence of various computer viruses is also one of the reasons for the frequent occurrence of network communication system security incidents. The biggest function of computer network communication system is to connect computers of different LANs and WANs to realize language communication and file data transfer. Any form of communication may be mixed with more or less viruses, weak attack virus can often be intercepted by firewalls and other simple defense functions, but with the update or mutation of various viruses, the communication network system is not able to crack or remove the strong attack virus in time, the entire network system will collapse, paralyzed, resulting in more serious economic losses.

3. To Strengthen the Computer Communication Network Security can Take Effective Maintenance Strategy

3.1 Introduction of Centralized Management Mode of Control Software

From the computer communication network application practice can be seen, through the search engine can search for a lot of software. A small portion of them are green plug-in-free tools, and many of them add the application platform packaging and download modules from various websites. In the download process, if you use one-click installation or default installation mode, you will download a lot of useless software. Not only will it take up a lot of hard disk space, but also adversely affect the operation of the computer system. Among them, some of the default installation software will have a negative impact on the overall security of the computer communication network system. From this point of view, the introduction of centralized management mode of control software tools is particularly important. Specifically, the appropriate software installation mechanism should be added as a barrier for users to install software, and then with the help of detection tools to effectively detect the installation of software, through the security check before installing the application. Through this model, you can effectively improve the security and reliability of computer communication networks. At the same time, but also to strengthen the control of data and information transmission process.

3.2 Network-based IDS Security System

IDS is Intrusion Detection System, is the abbreviation of Intrusion Detection Systems. Intrusion detection system is mainly used to monitor the operation and transmission status of the computer communication network for early warning of security threats, is a kind of listening device, under certain conditions of security maintenance strategy. The IDS can detect foreign data and other data that invade the system, and will refuse access to unknown data, thus ensuring the security of the computer communication network. With the rapid development of China’s science and technology, the country’s research on computer communication networks continue to deepen, the maintenance of computer communication networks are more and more ways, and its security level is also slowly improving. But for the computer communication network in the application process of the problems that still need to be further improved, the use of advanced science and technology to effectively ensure the normal operation of the computer communication network, so as to ensure its full application in China’s major industries, to bring more convenience to our lives.

3.3 Utilize Advanced Computer Communication Network Security Control Technology

3.3.1 Network Encryption Technology

Ensure the security of computer communication networks through the setting of data encryption, the setting of encryption is mainly composed of key, ciphertext, algorithm and plaintext, and its core is to give information to disguise. Commonly used encryption methods have two categories: symmetric encryption and asymmetric encryption, symmetric encryption in the data encryption and decryption of the same key, so this method in the specific operation process is not only easier, but also has a high efficiency, in the computer network communication is widely used. Asymmetric encryption method is different from symmetric encryption method, in the encryption and decryption operation process using completely different keys, mainly public and private keys, and public and private keys need to be paired to open the encrypted file, the public key can be used openly, while the private key needs to be kept by the holder, with absolute confidentiality. The key to both encryption techniques lies in the management of the key.

3.3.2 Intrusion Detection Technology

General firewall is only to protect the internal network from external attacks, for the internal network there is not enough to monitor the degree of illegal activities, intrusion system is to make up for this point and the existence of the IDS is called computer network security in the intrusion detection protection, mainly used to identify network intrusion behavior, and immediately respond to a variety of appropriate security measures to defend against the invasion and then alarm, it is a relatively new type of computer network security, the intrusion detection technology is a relatively new type of computer network security. It is a relatively sophisticated technology for computer networks.

3.3.3 Vulnerability Scanning Technology

In the face of network complexity and constantly changing situation, just rely on the relevant network administrators to carry out security vulnerabilities and risk assessment is obviously not possible, only rely on the network security scanning tools can be optimized in the system configuration of the security vulnerabilities and security risks eliminated. For example, in some government departments and important large-scale state-owned enterprises, will regularly scan for vulnerabilities and patches. The information center will deploy special technicians to the jurisdiction of the responsible machine room and information equipment area for vulnerability scanning, scanning the vulnerability to record, and to the Microsoft official website or some IT security website to download patches, and then through the server for the LAN internal push, this means can reduce the computer vulnerability backdoor, so that viruses or hackers have no target for attack. In some important period, some of the conditions of the unit will also simulate the red and blue confrontation, the blue side will be based on the real situation to build servers, and then the red side of the vulnerability scanning, and then according to the vulnerability of the real hacking, and the red side of the some will be informed in advance, and some will not be informed. In this way, through the real simulation exercise, some problems will be exposed, and then improvements will be made according to the problems.

3.3.4 Firewall Technology

Firewall technology can effectively control access between various networks, for those unclear information data and links will be certain security testing, according to the results of the test to determine whether the communication can be carried out, real-time monitoring of the information network. There are software and hardware firewalls, commonly used software 360 Firewall, Rising Firewall, Kingsoft Firewall, etc., hardware firewall brands are Cisco, Deep Trust Service Technology, H3C, Huawei, Green Alliance Technology, etc., the hardware firewall is the firewall software is written to the hardware device, thereby reducing the CPU load, thus making the system more stable and secure. The advantages of firewall technology are more, it has the advantages that it can protect network services, check the access of external systems to internal systems, carry out collective security management, increase certain confidentiality and so on.

3.3.5 Strict Authentication Technology

The stricter and more complex the authentication means, the more it can prevent illegal login, and at the same time, it will greatly reduce the risk of being hacked. Therefore, verifying the customer’s identity before communicating with the other party over the network can effectively prevent illegal login and thus information theft. Only through the authentication and the correct password is authorized to log in to some of the services of the server, you can access, send and receive information.

4. Conclusion

In the network environment is becoming more and more complex today, the security of network communication more and more attention, and the vulnerability of the communication system itself are determined by the network security not only rely on a single type of software can be protected, but also must rely on a sound management and supervision system. Communication network security maintenance is a long-term lasting subject. We must adapt to society and constantly improve the technical level to ensure the smooth progress of network security maintenance.

References

Bao, J. C. (2018). Computer communication network security maintenance measures. *Electronic technology and software engineering*, *2018*(06), 218.

Cai, Y. (2020). Analyzing computer communication network security maintenance measures in the information age. *Electronic Technology and Software Engineering*, *2020*(23), 257-258.

Chen, Y. L., Wang, T. L., & Geng, H. Y. (2016). Computer network communication security problems and preventive countermeasures. *Communication World*, *2016*(10), 106.

Han, S. C. (2015). Analysis of computer communication network security maintenance measures. *China High-Tech Enterprise*, *2015*(21), 70-71.

He, M. (2015). Analysis of computer communication network security maintenance measures. *Communication World*, *2015*(15), 15-16.

Huang, W. (2015). Analysis of network security technology and protection system. *Microcomputer Application*, *21*(12).

Lin, Y. J. (2015). Analysis of computer communication network security maintenance measures. *Network Security Technology and Application*, *2015*(10), 54-55.

Lu, C. (2018). Analysis and discussion of computer communication network security maintenance measures. *Information system engineering*, *2018*(06), 70.

Sheng, H. (2015). Analyzing computer network communication security problems and preventive strategies. *Electronic Testing*, *2015*(7), 65-67.

Tsidan Lobu. (2013). Analysis of security maintenance measures of computer communication network. *Digital user*, *19*(06), 38+33.

Wang, G. B. (2021). Research on Security Maintenance Measures of Computer Communication Network. *Fujian Computer*, *37*(01), 60-61.

Xu, J. S. (2021). Research on Security Maintenance Measures of Computer Communication Network. *Computer Knowledge and Technology*, *17*(24), 61-62.

Yan, J. (2015). Analysis of computer communication network security maintenance measures. *Information communication*, *2015*(05), 182.

Zeng, S. (2020). Exploration of computer communication network security maintenance measures. *China New Communication*, *22*(03), 29-30.

Zhang, Q, B. (2015). Analysis of computer communication network security maintenance measures. *China new communication*, *17*(04), 53.