HILL PUBLISHING

Advance in Information Technology and Computer Science, 2024, 1(1), 1-4
https://www.hillpublisher.com/Journals/aitcs/
ISSN Online:
ISSN Print:

Computer Network Information Management Security Protection Issues and Measures

Xiaoman Qiu, Yuanchao Qi, Shengzhi Zhu

Wuhan Donghu University, Wuhan 430212, Hubei, China.

How to cite this paper: Xiaoman Qiu, Yuanchao Qi, Shengzhi Zhu. (2024) Computer Network Information Management Security Protection Issues and Measures. *Advance in Information Technology and Computer Science*, 1(1), 1-4.
DOI: 10.26855/aitcs.2024.12.001

Received: October 13, 2024
Accepted: November 4, 2024
Published: November 26, 2024

***Corresponding author:** Xiaoman Qiu, Wuhan Donghu University, Wuhan 430212, Hubei, China.

Abstract

Due to the rapid development of the national economy, the Internet technology has been spread and penetrated in various industries, and has brought a rich variety of information to people, so the network has gradually become an indivisible part of people's daily life. Nowadays, the computer network information management security protection work is increasingly concerned, in order to ensure the smooth development of the work, need to strengthen the understanding of the computer network information management security protection work, pay attention to and master the technology in the field of computer, avoid hackers, network data theft and virus attacks, reduce the effects of malicious operation, and ensure the smooth development of the network information management and security protection work.

Keywords

Computer; network information management; security protection; measures

Introduction

Due to the continuous development of computer network technology, the importance of network management continues to increase. At present, in order to ensure network security and stability, various network security technologies are also emerging. In the specific application process, it is necessary to combine the actual situation with the operating environment for comprehensive consideration. Only by taking all risks into consideration can we effectively prevent and control various network security risks.

1. Conceptual Explanation of Computer Network Security Technology

Computers use a variety of technologies to carry out daily operations, among which the most effective means is computer network security technology, which can promote the safe and stable operation of computers, ensure the security of computer hardware and software equipment, avoid computer viruses, and effectively protect the personal information security of users. Different from other computer technology characteristics, the most important feature of computer network security technology is that it has strong concealment and latency. Computer viruses also have this feature. Most network viruses are hidden in computer software programs and can break out in a short period of time, resulting in the leakage of user personal information. Therefore, in view of the strong concealment of computer viruses, it is necessary to fully connect all links and strengthen the comprehensive protection and security detection of computers. In addition to the latent and hidden characteristics, computer network security technology also has a strong transmission power. Since computer network security technology covers a wide range, it can effectively prevent various viruses. In the development of China's computer industry, computer network security technology plays

Note: The article was originally published in *Industry and Information Technology Development*, and this is an authorized translation of it.

an important role, so relevant personnel must strengthen the comprehensive analysis and research of network security technology to effectively improve the efficiency of computer network security operation.

2. Problems and Causes in Computer Network Information Management

2.1 Computer system vulnerabilities

In the process of studying the network security issues of computer systems, we can find that the impact of the operating system cannot be ignored. It is an important foundation for network operation and information transmission, and technological innovation plays a very important role. Everything will face the possibility of being replaced by new things, and this is also true in the development of the computer industry. Therefore, computer operating systems need to be continuously updated, and some shortcomings and deficiencies are usually made up during this period. If a computer has a system vulnerability, it will inevitably provide conditions for virus intrusion and hacker attacks. In order to ensure the safe application of users and the effective operation of the computer system, the vulnerabilities and shortcomings in the operating system must be repaired as soon as possible.

2.2 Information security awareness issues

At present, many users do not pay enough attention to computer network security. In order to achieve more convenient and quick operation, they often ignore the effective protection of personal information security and fail to pay attention to the potential safety hazards of personal information resource leakage. Most criminals also seize this awareness of users to conduct information security fraud. If users do not protect personal information resources properly, criminals will have an opportunity to take advantage of it and cause adverse effects on their daily production and life. At present, many companies have established independent network systems, which record the company's privacy information and financial situation. If during the installation of the computer network system, the technicians fail to implement information security protection work, or the programmers fail to effectively improve their own security awareness, when the computer is attacked by external security, it will lead to a large amount of corporate information resources leakage.

2.3 Hackers and network virus attacks

From the perspective of network hackers, their work purpose is to carry out illegal destruction or intrusion through loopholes in computer network systems, to manipulate terminal computers through network programs specifically programmed by humans, or to steal some of the data or cause damage, etc. These network programs specifically programmed by humans have very strong replication capabilities and can be replicated on a large scale in an instant, which will directly undermine the stability and security of computer network systems. According to the types of viruses that cause network security problems, most viruses have extremely strong adaptability and aggressiveness, and usually do not distinguish between the targets of attack during their intrusion. Therefore, when network security risks occur, they will inevitably cause great damage to the security and stability of the computer, which will cause some internal files and information to be lost, damaged or leaked.

3. Application Measures for Computer Network Information Management Security Protection Issues

3.1 Raise the public's awareness of protection and ensure computer network security

During the period of entertainment or work on the Internet, due to the lack of active protection of network security, identification and response to network risks, there are hidden dangers of being hacked. Therefore, people's low awareness of Internet protection is one of the important reasons for the frequent occurrence of network security accidents. Therefore, we should strengthen the publicity of network security, make people realize the importance of network security, make people have a deeper understanding of hackers and viruses, and deeply realize that they should strengthen their prevention when surfing the Internet. On the one hand, we should change people's concepts, increase people's attention to network security, and develop safe and good Internet entertainment and work habits. On the other hand, we should also cultivate people's habit of checking and killing viruses regularly and master some conventional methods to prevent virus invasion (such as installing firewalls, installing anti-virus software, cleaning rogue

software independently, not browsing illegal websites or phishing websites, etc.), so as to reduce the probability of viruses and hackers invading computer systems from the root, thereby reducing the losses caused by network risks to people.

3.2 Use a variety of advanced computer network security prevention technologies

3.2.1 Firewall technology

Firewall technology has long been used in my country's computer network security protection work. The reason why it is specifically mentioned here is mainly because it has always been an important barrier to network security prevention. Even if other advanced computer network security prevention technologies are introduced, the important position of firewall technology is always irreplaceable. Therefore, in the era of big data, firewall technology will continue to play a powerful security protection role and safeguard people's information security.

3.2.2 Data encryption technology

As an important means to deal with open networks, data encryption technology has been widely used in many industries. Data encryption technology is divided into two categories, one is symmetric encryption technology, and the other is asymmetric encryption technology. The two share the responsibility of protecting user network dynamic data. First of all, symmetric encryption technology is relatively simple and fast. Whether it is encryption or decryption, only the same secret key (SecretKey) is needed, so the encryption efficiency is quite high. It is often used in the core of multiple encryption protocols. The DES symmetric encryption technology currently common in the financial field belongs to this type of technology. Secondly, asymmetric encryption technology requires a pair of secret keys, namely public key and private key. The former is used for encryption. The latter is used for decryption. Since the private key is usually only held by the data exchanger, compared with symmetric encryption technology, asymmetric encryption technology is more secure, but the encryption efficiency is relatively low. Nowadays, asymmetric encryption technology is often used in identity authentication, digital signatures and other aspects.

3.3 Strengthening user account security

There are many different types of computer network software today, which include a large number of user accounts, which can be divided into different types of accounts, such as electronic accounts, login names, etc. There are two most common application methods for network systems, namely cracking the key and obtaining a legitimate account. In this regard, in order to avoid threats caused by hackers and ensure that the account security level is greatly improved, it is necessary to introduce more complex system login accounts to prevent them from being cracked. In addition, it is important to avoid setting up similar or identical accounts, and to combine letters, numbers, symbols, etc. into special symbols, so as to obtain passwords and accounts with higher security levels. The password length must be updated regularly.

4. Conclusion

In summary, in order to ensure the smooth development of computer network information management, people need to pay more attention to computer security protection, improve overall security awareness, and use diversified means to avoid risks in computer network management. If the above suggestions are not implemented, it will not only affect the enterprise, but also increase people's unsafe factors in work and life. Therefore, it is necessary to strengthen computer network information management, solve the problems existing in the computer network system, and make computer network information develop on a healthy path.

References

[1] Feng Qingxi. Computer network information management security protection issues and measures [J]. Digital Communication World, 2022(09):188-190.

[2] Yang Jia. Computer network information management and its security protection strategy [J]. Guizhou Agricultural Mechanization, 2021(04):47-48+51.

[3] Gao Wenbo. Research on the application of big data technology in computer network information management [J]. Wireless Internet Technology, 2021, 18(11): 85-86.

[4] Li Long. Application in computer network information management [J]. Industrial Innovation Research, 2020(14):45-46.

[5] Zhang Di, Li Ying, Zhang Xianhua. Computer network information management and its security protection strategy [J]. Information Systems Engineering, 2020(01):57-58.

[6] Huang Ying. Analysis of countermeasures for computer network information management and its security management [J]. Computer Fan, 2018(11):73-74.

[7] Ren Yanhua. Research on computer network information management and security protection strategy [J]. Electronic Commerce, 2018(06):57-58.

[8] Yun Xiaobo. Analysis of computer network information management and its security protection measures [J]. Computer Knowledge and Technology, 2018, 14(14): 35-36.