

The Influencing Factors and Preventive Measures of Computer Network Security Technology

Zhiwei Li¹, Hefeng Liu²

1. Zhengzhou University of Science and Technology, Zhengzhou 450000, China.
2. Henan Air Cargo Development Co., Ltd., Zhengzhou 450000, China.

Abstract: Because the application scope of computer network technology is getting wider and wider, the security issue of this technology has gradually attracted the attention of the public. In addition, the openness of computer network technology is relatively strong, and it can be easily and quickly shared on a large scale, so it also determines that the computer network is susceptible to influence and attacks. In order to improve the stability and security of the computer network, it must be aimed at the security of the computer network. The threat factors put forward effective preventive measures.

Keywords: Computer; Network Security Technology; Influencing Factors; Preventive Measures

Introduction

On the one hand, computer network technology is very helpful to the improvement of our quality of life, but on the other hand, there are also problems such as being vulnerable to virus intrusion. Therefore, in recent years, there have been frequent incidents of users' privacy being leaked and property infringed. In order to ensure that the important data in the computer and the private information of the user will not be maliciously stolen and leaked, technicians need to conduct in-depth research on the factors that affect the security of the computer network, and actively research and implement effective measures.

1. A brief introduction to computer network security

The meaning of computer network security is to protect the security of computer users' data processing systems with the help of related technologies, and to ensure that computer users' hardware, software, and data will not be maliciously leaked or destroyed. Moreover, the meaning of computer network security will vary from user to user. For example, computer security considered by ordinary users means that personal privacy and confidentiality cannot be stolen by others, and that privacy and

confidential information can be effectively protected during the transmission of privacy and confidential information; Network providers believe that computer network security means that the user's information and information transmission process are protected, and there will be no problems such as data loss in the face of sudden natural disasters and wars.

Nowadays, users' computer network security is threatened from many aspects, and most computer network attacks are concealed and latent. If computer users neglect to prevent network security threats, they are likely to be vicious assault. Furthermore, network attacks are also severely destructive and harmful. Once a malicious attack from the outside is successful, the computer is likely to be paralyzed, causing users to suffer serious economic losses due to information leakage and other reasons.

2. Influencing factors of computer network security technology

2.1 Problems in the network system

Because the computer network is not under the management of the government or an organization, any user can browse related information on the Internet with the help of a mobile device. Therefore, personal privacy or important corporate information is likely to be maliciously damaged and leaked. Nowadays, the operating systems used in a wide range of our country have certain problems, and system vulnerabilities give hackers an opportunity. And the reasons for the vulnerabilities may be hardware, software, improper configuration, functional design, and so on. Moreover, the TCP/IP protocol is also one of the important factors that threaten the security of our computer network. The clear mode of transport makes the data of this protocol easy to be intercepted or eavesdropped by others during the transmission process, and the process of modifying the IP address does not require an identity. Authentication, resulting in the information of the agreement being easily intercepted and tampered with by others.

2.2 External threats

The influence of the outside world on computer network security is mainly divided into four aspects: natural threats, hacker attacks, virus intrusion and illegal access. First of all, severe natural disasters and bad weather conditions will cause the failure of mechanical equipment, which will lead to the failure of effective support for computer network security. Furthermore, malicious attacks by hackers will also threaten user information, because the field of computer technology is developing very rapidly, but there is a certain lag in the development of corresponding security technology, so hackers can use more advanced computer technology to find system vulnerabilities, and then Conduct surprise attacks on other users' computer network systems. Hacker attacks are the most important factor causing computer user network insecurity. Furthermore, virus intrusion is also an important reason for the leakage of computer user information. Before viruses damage users' computer systems, users generally seldom find viruses lurking in computers, and the concealment, infectiousness, destructiveness, and stress resistance of computer viruses have shown a trend of increasing year by year. Finally, illegal access refers to malicious operations on the computer without the permission of the computer user. Because illegal visitors

can ignore the restrictions on their access operations by writing programs and other means, it is likely to cause damage to the personal privacy and important information of computer network users.

3. Precautionary measures for computer network security

3.1 Continuously improve the design of computer systems

Because the systems used by computer users in our country have problems of unreasonable design, professionals should devote themselves to studying the defects of computer systems, and then solve their weaknesses by constantly improving the design of network systems. Among them, technical personnel especially need to establish and improve the control function of network access. If network access can be controlled more effectively, the security of the computer network can be further improved^[1].

Computer professionals need to continuously update and upgrade the operating system to ensure that the security, reliability and integrity of various systems can be continuously improved. Technicians need to ensure that the computer's operating system can effectively control access operations, so as to prevent other personnel from malicious and unauthorized access to the information in the computer. Moreover, the storage protection function is also an important criterion for evaluating the quality of the operating system. An operating system with a high-level storage protection function can ensure that the read and write operations of information occur within the specified range. Finally, complete management capabilities can monitor the access operations of computer data files in real time.

3.2 Continuously improve network security protection

In order to more effectively avoid the impact of external factors on computer network security, first, the staff need to establish a complete server room in accordance with the regulations, and after completion, they need to undergo strict inspections by the public security and fire departments. Waterproof, fireproof and lightning protection equipment of the important equipment department of the computer system needs to be adequately equipped, and the staff also need to conduct regular inspections and maintenance of important equipment.

3.3 Continuously improve the security awareness of computer users and managers

Personal computer users also need to realize the importance of strengthening network security, and strengthen personal network security awareness through active learning. For example, choosing different passwords, updating anti-virus software in time, and scanning the system regularly can all improve the security of personal information. In addition, the security awareness of computer management personnel also needs to be cultivated and improved. Nowadays, the situation of computer network security in my country is still severe. Therefore, management personnel need to continuously improve the security management system and strengthen security management, and continuously improve their professional ethics and network security. Professional management capabilities are dedicated to providing a safer and more reliable network environment for computer users in our country.^[2]

4. Concluding remarks

The construction of a computer network security system requires the joint efforts of managers, technicians, and users. Nowadays, there are still many hidden dangers in computer network security in my country. Therefore, professionals need to conduct in-depth research and comprehensively summarize the factors that threaten computer network security. Committed to perfecting the design of computer systems and improving the level of firewalls, anti-virus and other technologies. The vast number of computer users in our country also need to continuously improve their security awareness and work together to improve the reliability and security of computer networks.

References

- [1] Xie Q. Influencing factors and prevention strategies of computer network security technology[J]. Network Security Technology and Application,2021(02):161-163.
- [2] Cheng SH. Analysis of Computer Information Network Security Technology and Security Precautions[J]. Small and Medium-sized Enterprise Management and Technology (Late Edition), 2020(09):180-181.

About Authors:

1. Zhiwei Li(June 1984—) male, Bengbu, Anhui, Undergraduate, teacher, lecturer. Research direction: information security
2. Hefeng Liu(November 1975—) male, Zhengzhou, Henan, Postmaster, Aviation Safety Inspector Level 3. Research direction: safety management personnel