Journal of Electronics and Information Science (2023)
Clausius Scientific Press, Canada

DOI: 10.23977/jeis.2023.080301
ISSN 2371-9524 Vol. 8 Num. 3

Analysis of Factors Influencing Computer Network Security Technology

Guohui Zou[1,a,*]

[1]Longnan Secondary Vocational School, Longnan, Ganzhou, Jiangxi, 341700, China
[a]cswl0924@163.com
**Corresponding author*

Keywords: Computer; Network security technology; influence factor

Abstract: With the advent of the information age, the development of internet and computer technology has brought new opportunities and challenges to various industries, and has also changed people's lives. Whether it is the economy, politics, and culture, they have all become faster with the development of internet platforms, and the world has gradually become a whole, allowing people from all over the world to achieve real-time communication. Of course, with the development of the times, computer networks have gradually encountered some problems, which have been exploited by illegal elements, resulting in network crises and posing huge challenges to computer network security. Based on this, this article provides a detailed analysis of the influencing factors of computer network security technology, uncovers the existing problems, and explores corresponding development directions, providing certain countermeasures.[1]

1. Introduction

With the rapid development and widespread application of computer networks, computer network security issues are becoming increasingly prominent. Computer network security is not only related to personal privacy and property security, but also to national security and social stability. In this information age, it has become a global challenge.The development of computer network security technology cannot be separated from the progress of computer technology and the development of network technology. With the continuous updates and upgrades of these two technologies, computer network security technology is also constantly developing and improving. However, computer network security problems still exist. Hacker attacks, virus infections, phishing and other security threats continue to emerge, bringing huge risks and losses to people's production and life. This article will explore the factors that affect computer network security and the measures to control these factors. Only by comprehensively strengthening the research and application of computer network security technology can we better ensure the security of computer networks. Because a computer network platform is a virtual platform, although many user information is authentic, there can also be the phenomenon of impersonation.

There is a sentence that mocks internet identity: "The person sitting opposite you chatting is not necessarily a person. This also indicates that computer networks have invisibility. Of course, not only does user information have concealment, but viruses also have concealment. It can crash the computer network at any time and steal some important information. Or it could be invading user data, such as some hackers packaging viruses to attract users' attention and induce them to download, thereby successfully entering users' privacy space and collecting important information such as property information. In fact, the computer penetration rate in China is quite high, and most of the computer knowledge has gained basic popularization. But because computer virus is not something that ordinary people can deal with, it is completed through various data program settings, so it is highly technical and difficult to prevent, especially the hidden nature of it makes people confused.

2. The significance and characteristics of computer network security

The significance of computer network security technology is to ensure the security of computer networks, prevent hacker attacks, virus infections, phishing and other security threats, protect personal privacy and property security, and maintain national security and social stability. With the popularization and application of computer networks, people are engaging in more and more activities online, including shopping, bank transfers, socializing, etc.[2] These activities all involve personal privacy and property security. Computer network security technology can protect personal privacy and property security, prevent personal information theft, account theft, etc. At the same time, computer networks have become an important component of national security, including government agencies, military agencies, transportation and other important fields that rely on computer networks. Computer network security technology can ensure national security and social stability, and prevent threats such as hacker attacks and cybercrime.[3]

In addition, the security of network systems is also an important component of computer network security. The network system includes network topology, network protocols, network devices, network management, and network security policies. If the network system is not secure, such as unreasonable network topology, insecure network protocols, vulnerabilities in network devices, improper network management, or a lack of effective network security strategies, it will leave opportunities for hacker attacks. Hackers can exploit vulnerabilities in network systems to carry out network attacks, such as DDoS attacks using network device vulnerabilities. Therefore, when using a computer network, users should choose a safe and reliable network system, strengthen network security awareness, regularly check and update network equipment and software, strengthen network management and security strategies, to ensure the security of the computer network. At the same time, users should also regularly backup important data to prevent data loss or being attacked by hackers. Therefore, when purchasing a computer, users should pay attention to its performance and choose a computer with higher configuration to improve its security.

3. Characteristics of Computer Network Security Technology

Because a computer network platform is a virtual platform, although many user information is authentic, there can also be the phenomenon of impersonation. There is a sentence that mocks internet identity: "The person sitting opposite you chatting is not necessarily a person. This also indicates that computer networks have invisibility. Of course, not only does user information have concealment, but viruses also have concealment. It can crash the computer network at any time and steal some important information. Or it could be invading user data, such as some hackers packaging viruses to attract users' attention and induce them to download, thereby successfully entering users' privacy space and collecting important information such as property information. [4]In fact, the computer penetration rate in China is quite high, and most of the computer knowledge has gained basic popularization. But because computer virus is not something that ordinary people can deal with, it is completed through various data program settings, so it is highly technical and difficult to prevent, especially the hidden nature of it makes people confused.[5]With the continuous increase in the number of computer users in China, the construction of the network environment has become particularly important. In order to provide users with a safe and reliable network environment, the country needs to increase its management of the network and continuously crack down on hacker behavior. Relevant departments can ensure network security by implementing precise positioning for users, strengthening information tracking capabilities, and regulating user behavior when using computers. Professional personnel are also needed to take action in computer network security prevention. In fact, most enterprises, groups, and countries have relevant computer security technicians to prevent hacker intrusion, while also ensuring the confidentiality and security of data. They need to have a strong resilience, be able to respond quickly when network security incidents occur, and take effective measures to deal with them. In addition, computer security technicians also need to have strong risk awareness and predictive ability, be able to predict and identify potential network security threats in advance, and take corresponding measures to prevent them.

At the same time, in order to prevent network attacks, it is necessary to match corresponding information, continuously improve firewall functions, and enhance network security prevention capabilities. In addition, it is also necessary to strengthen network security education, enhance users' security awareness, make users consciously comply with network security regulations, and jointly maintain network security. Computer networks are an intangible world, therefore they have a diffusive nature. They contain information from the entire world, and as long as users have mobile phones or access the internet, they can leak a lot of information. Especially in the information age, computer technology and internet technology are developing faster and faster, making information dissemination faster. Everything that happens in a second can be quickly exposed and pushed to people's daily lives in a timely manner. Therefore, this also makes people's communication faster and faster, enabling them to understand the world without leaving their homes. But this also creates loopholes for hackers, allowing them to spread the virus faster and with a wider range of impacts. In most cases, hackers only need one computer to control the information of many users, and using one computer can spread the entire computer community, not only causing personal property damage, but also causing losses to companies and even the entire industry. Of course, it can also cause losses to the country.

4. Factors affecting computer network security

With the advent of the information age, the number of network users is constantly increasing, and they are familiar with basic mobile and computer operations. However, due to the fact that the popularization of computer knowledge is mostly based on basic level content, and there is no detailed explanation of knowledge such as hackers and viruses, many computer users' awareness of network security prevention is relatively weak. [6]Most users feel that they are just chatting and working on a daily basis, without any important information, which will not cause significant losses. Therefore, they do not attach importance to information security content, nor do they actively learn about network security knowledge. Especially since China has a large population base, the corresponding number of internet users is also large, which gives hackers a lot of room to attack computers. In fact, information leakage is a common problem in daily life, but there are also corresponding preventive measures. However, due to the weak awareness of users, these preventive measures have a relatively small effect. The hardware facilities and network system of the computer itself are the foundation of computer network security. If the computer hardware facilities are not strong enough, such as insufficient configuration of CPU, memory, hard disk, etc., it will affect the running speed and stability of the computer, and also increase the risk of hacker attacks. Hackers can exploit vulnerabilities in computer hardware facilities to carry out malicious attacks, such as exploiting CPU vulnerabilities for cryptocurrency mining.

5. Control measures for factors affecting computer network security

Firstly, in order to ensure computer network security, the most basic thing is to cultivate the security awareness of network users. It is necessary to increase the importance that users attach to computer network security. By continuously promoting basic security awareness, everyone should be aware of hackers and viruses, and take timely preventive measures. It can be carried out through community explanations, symposiums, and other means. Secondly, in addition to improving users' security awareness, it is also necessary to enhance their operational skills.

Users need to understand basic operational skills such as how to set strong passwords, how to avoid using public wireless networks, and how to identify phishing emails. We can help users improve their operational skills by conducting network security training and providing network security manuals.The internet is not a place outside the law, and although China's management of network users is becoming increasingly standardized, the emergence of hacker behavior is still difficult to avoid. In order to ensure network security, China needs to improve laws and regulations, strengthen supervision and management of the network. Relevant departments should strengthen their crackdown on cybercrime, promptly investigate and punish hacker behavior, and protect the security of users' personal information. At the same time, emergency response to network security incidents should be strengthened, and timely measures should be taken to prevent the escalation of the incident.

6. Conclusion

Computer network security is a complex system engineering that requires control from multiple aspects. Improving users' awareness of prevention and operational skills, improving the comprehensive quality of computer security technicians, constructing a complete network environment, and improving laws and regulations are effective measures to control the factors affecting computer network security. Only by comprehensively strengthening the research and application of computer network security technology can we better ensure the security of computer networks.

References

[1] Chen Wenbing. Exploring the Application Strategies of Computer Information Management Technology in Maintaining Network Security [J]. Computer Knowledge and Technology: Academic Exchange, 2015, 0 (12X): 35-36

[2] Xu Hong, Mao Xiumei. From the construction of security measures for multimedia video on demand systems to discuss the current situation of network security and corresponding technologies [J]. China Management Informatization (Comprehensive Edition), 2005, 0 (A09): 72-74

[3] Cai Meng, Chen Zhizhong, Wang Jun. The application strategy of computer information management technology in maintaining network security [J]. Electronic Technology and Software Engineering, 2017, 0 (21): 190-190

[4] Sun Xueyang. Starting from me, starting from a young age, and becoming a diligent person - Reflections on Network Information Security [J]. Off campus education in China: mid-year, 2010 (6): 35-35

[5] Chen Hang. Discussion on the Practice of Network Security Construction in the Logistics Industry - Taking China Railway Express Co., Ltd. Shanghai Branch as an Example [J]. Information Technology and Informatization, 2018, 0 (2): 114-118

[6] Li Hongliang, Gai Xingjie, Li Lu. The influencing factors and preventive measures of computer network security technology [J]. Electronic Technology and Software Engineering, 2018, 0 (24): 188-188