

Security Problems of Computer Network and Preventive Measures

Yijia Wang

Jilin Justice Officer Academy, Jilin, Changchun 130062, China

Keywords: Computer, Network security, Precautions

Abstract: With the rapid development of computer network technology, the importance of network security has become increasingly prominent in the application of computer network. The problem of computer network security has attracted more and more attention from all walks of life. Judging from the current situation, China's information network security has transitioned from communication security and data protection to network information security research. Facing the potential safety hazard in the computer network, it is particularly important to take relevant measures to protect the safety of the computer network. How to ensure the security of computer network information has become an important issue that people pay close attention to. This paper analyzes the main factors that threaten network security, and on this basis, discusses several strategies for network security.

1. Introduction

Computer network is an important structure in the whole information network system. Based on its network technology, a huge information society has developed. The network system is all-encompassing, and all the information of the whole society can be displayed on it. The amount of information is huge, which brings great convenience to social development and people's daily life [1]. At present, people often ignore the importance of computer network security when they use computers to accept vast amounts of information, which leads to the threat of computer network security taking advantage of it. Computer network has serious security risks and affects the application of computer network. The Internet has brought great help to our life, study and work, making it easier for us to get the latest information [2]. Generally speaking, the Internet has become a part of our life for today's human beings. Whether we work or live, we cannot do without the help of the Internet. However, because of this, computer network security is becoming more and more important [3]. With the continuous development of science and technology and the advent of the information age, computers have become essential items in people's lives. Computers have brought many conveniences to people, but of course there are some problems in themselves. It not only brings convenience to people, but also faces more, more serious and complicated network security threats, which makes the security problems become increasingly prominent. Therefore, it is necessary to strengthen the management of computer network security in order to eliminate the influence of unsafe factors so as to ensure the security of computer network.

2. The Influence of Computer Network on Social Development

Today's era is an era of electronic information, computers and networks have become an indispensable part of people. The form of networking has created many hidden dangers for the normal operation of computers. There are also some loopholes in the system compilation of the computer itself. At the same time, people's safety awareness is insufficient, and the problems existing during the use of the computer can't be repaired in time, providing opportunities for many criminals [4]. First of all, with the development of the network, the pace of social development in our country is accelerating. The most obvious characteristic of the era of computers and networks is information. The emergence of computers and networks has greatly improved the speed of information dissemination. In the practical application of computers, the security problems of computer systems are mainly hidden troubles in computer hardware and software, work efficiency,

operation speed, data and information. There are more and more channels for people to obtain information, and they can receive information at the first time of information release, which has strong timeliness and timeliness.

Secondly, as far as individual human beings are concerned, the use of computers and networks has a great impact on their work and has changed the way human beings work. For example, computer technology has made great changes in modern e-commerce and logistics. Computer technology has a penetrating influence on the various structures of productivity. Computer technology has brought more reliability to information and improved people's ability to master information. The continuous progress of human society has gradually accelerated the pace of scientific and technological development. In the production process, we can use computers and networks to control every link of production in real time. For modern society, the popularization and development of computer network will have a great impact on all aspects of social production and life, especially after the network is widely accepted and used by the people as a production and life tool, the role of computer network will become even greater [5].

Human society has experienced several technological revolutions, and the arrival of the computer network era has announced the arrival of a new technological revolution. The development of computer network technology has promoted the adjustment of production structure of enterprises to a great extent, making the social class structure have also undergone earth-shaking changes, which are most obvious in modern enterprises. At the same time, the development of information technology will also promote the progress and development of information-related industries such as biotechnology and electronic technology. However, the development and utilization of some new materials and new energies will also be greatly developed in this process, thus making science and technology more prominent as the first productive force in human society. However, if the network is not properly used, it will seriously affect the development of our society.

3. Problems Faced by Computer Networks

The current era is an era of scientific and technological information, and people's lives have been significantly improved under this background. The development of network makes the society form an independent virtual space, in which there are a lot of potential safety hazards. At present, there are still many problems that need to be solved urgently in computer network security. These problems are mainly manifested in five aspects: the destructiveness of computer viruses, Trojan horse programs and hacker attacks, computer user errors, loopholes in the network system itself and spam and spyware. The specific contents are as follows:

3.1 The Destructiveness of Computer Viruses

The destructiveness of computer viruses affects the security of computer networks. In daily use, floppy disks, hard disks, compact disks and networks are the main ways to spread viruses, which are destructive, replicable and infectious. Computer viruses destroy computer resources. From an objective point of view, on the basis of continuous development of time, even the perfect system will have some loopholes, and the system will come into contact with a lot of networks and information during operation, which will cause hidden security risks in the system. Computer viruses are also constantly developing and evolving. From "worm" virus to CIH and worm-loving virus, their harmfulness is becoming more and more serious. The network is the best way to spread the virus. As a form of information, the virus can propagate, infect and destroy with it. Once the virus has control, it will actively look for more targets [6]. The harm to computer users is very great. If the computer virus runs lightly, it may reduce the working efficiency of the system. If it runs heavily, it may damage files or even delete files, causing data loss, destroying system hardware and causing various unpredictable consequences.

3.2 Trojan Horse Programs and Hacker Attacks

Trojan horse programs and hacker attacks also restrict computer network security to a certain extent. Computer hackers often have professional computer knowledge, the ability to use various

computer tools, the imperfection and defect of the information network itself, and become the target of attack or the way to use it. IP address is very important information for computer users. If the IP address is incorrect or modified, it basically belongs to the scope of illegal intrusion. Of course, such acts as modification or theft of IP addresses are basically done by hackers. It invades other people's computer information systems by illegal means through the technical means it has mastered, so as to obtain secret information or destroy the validity and integrity of information [7]. "Hacker" is the most important factor affecting the network security at present, and is also a common method of enemy attacks and computer crimes. They usually use illegal invasion of important information systems to eavesdrop, acquire and attack sensitive and important information about the invasion network, modify and destroy the normal use of the information network, resulting in data loss or system paralysis.

3.3 Computer User's Operation Error

The security threat to the computer network caused by the misoperation of computer users is also a potential security hazard in the current computer network security problems. For example, if there is a problem with computer hardware, the network will not work normally, or the computer will be attacked and the network will be restricted. At the same time, the network itself has some congenital deficiencies, hiding many security problems. In addition, the operation of the system is not perfect enough. Most users do not take relevant security precautions due to insufficient understanding of network security in the process of applying computer networks, which easily leads to computer network security accidents, such as weak user security awareness and simple user password setting. Once the system is attacked by the outside world, if no corresponding measures are taken, it becomes easy to collect, thus causing leaks. Both state secrets and banking systems are stored using digitalization and networking. Once the system is harmed by viruses, it will cause serious consequences.

3.4 Vulnerabilities in the Network System Itself

Network software cannot be 100% defect-free and leak-free. The loopholes in the network system itself make computer network security a security threat. At the same time, the most obvious advantage of computer network is its openness. The invasion of some computer viruses, the attacks of various network hackers, and the insufficient security awareness of computer users themselves are all common computer network security problems. At present, there is no perfect operating system and network software, and there are always some defects or loopholes. In addition, programmers have left "back doors" in the software for their own convenience [8]. The "loophole" and "back door" of the system become the fuse of most hacker's intrusion into the network. This openness is a double-edged sword. On the one hand, the openness of the computer network is conducive to users' communication on the computer network; On the other hand, openness affects the security of the computer network system and makes the computer network vulnerable to attack. There is no sound legal regulation to restrict the uploading of information on the internet, thus creating opportunities for the dissemination of false information, which will have a serious impact on society.

3.5 Spam and Spyware

Spam and spyware are also important factors that make computer network security in trouble. In the application process of computer networks, some people use the "publicity" of e-mail addresses and the "broadcasting" of systems to carry out commercial, religious, political and other activities, forcing their own e-mail into other people's e-mail boxes and forcing others to accept junk e-mail. The application of e-mail is constantly on a common basis, people's mailboxes will often receive some strange, unknown addresses of e-mails, which will not show the sender, and these e-mails are extremely dangerous. Different from computer viruses, spyware usually illegally invades computer information systems by stealing passwords and other means, stealing system or user information, and carrying out corruption, theft, fraud, financial crimes and other activities, threatening user privacy and computer security.

4. Computer Network Security Precautions

4.1 Establish a Perfect Network Security Management Mechanism

The protection of computer network security needs a perfect security management mechanism as the foundation. The proposal and improvement of the security management mechanism need the support of relevant laws and professionals. In the process of using computer network, computer users have a wide range of user accounts, including system login accounts, e-mail accounts, online bank accounts and other application accounts. Strengthen the security protection of user accounts. At the same time, there may be problems with our own hardware or software, which may lead to inaccurate data. We should find professional technical personnel to summarize the problems in the testing practice from a comprehensive perspective, conduct research, and come up with a reasonable design scheme to intercept unsafe information. From two angles to improve, first of all, from a macro perspective, constantly improve the computer network security maintenance laws and regulations, to better ensure the normal operation of the computer network system, to ensure its safety. Secondly, from a microscopic point of view, specific users must be specified in detail the computer network system rights they enjoy. It is to try not to set the same or similar account number, to set the account number and password by the combination of numbers, letters and special symbols, and to set the long password and change it regularly.

4.2 Strengthen the Awareness of Computer Network Security

Strengthening the awareness of computer network security is very important to protect computer network security. According to the investigation and analysis of the reasons for the occurrence of computer network security, it is concluded that computer users often make improper operations, which leads to illegal elements taking advantage of opportunities and various losses, even some losses are irreversible. Scan the network flowing through it to filter some attacks, prevent the attacks from being executed on the target computer, prevent “hackers” from visiting to the greatest extent, and prevent “hackers” from arbitrarily changing, moving or deleting information on the network. As soon as the computer receives the warning signal from the early warning system, it will carry out covert screening technology on all internal information in the computer, and clear up malicious intruders from outside in time, thus establishing the first safeguard of the computer security system. Constantly encourage relevant users to actively learn some basic security protection measures, can form a good habit of using computer networks, provide an additional layer of protection for computer network security protection, and create a safer computer application environment for themselves.

4.3 Increase the Promotion and Upgrade of Firewall Technology

Firewall is an important guarantee in computer network security. Firewall is mainly the protective layer for computers to connect to the network environment outside. It can filter the network environment in time and control various factors brought by the environment to ensure computer network security. For computer networks, installing firewall and antivirus software is the key to prevent computer network security. Among them, firewall is a special network interconnection device used to strengthen access control between networks and protect the internal network operating environment. Which can detect that behavior violate the security policy in the computer network. Through the intrusion detection system, combined with audit records, the intrusion detection system can identify any unsafe activities and take active response measures to limit these activities, thus ensuring the safety of the system. In recent years, China's network security technology is continuously improving, and the tasks faced by the firewall are becoming more and more severe. It is necessary to have both traditional and modern technical characteristics. Firewall protection is a basic measure in the computer security protection barrier. The first task is to set up the software parameters of the computer and install a high-tech firewall so as to reduce system vulnerabilities to a great extent and make the operating environment of the computer reliable and safe.

4.4 Increase Research on Computer Encryption Technology

Encryption technology is an important product in the continuous exploration of computer network security. With the development of computers, it also has a very large development space and has made some progress. Encryption technology can ensure the security of computer network and prevent it from being invaded by various viruses or hackers. According to the analysis technology adopted, it can be divided into signature analysis and statistical analysis. Signature analysis is used to monitor attacks on known weaknesses of the system. A technical means of hiding information content to prevent illegal users from acquiring information. In order to improve the security and confidentiality of data, data encryption technology is used to prevent secret data from being obtained by external analysis. It mainly uses transformation and replacement methods to protect the transferred information into a secret file, and then the file is inspected and transmitted. The encrypted information is stolen in the storage or transmission process in time, which can also ensure that the information will not be read out, thus achieving the purpose of protecting the information. It is necessary to write down an evaluation of its detailed records, explain and give examples of some problems encountered in the detection process, so as to optimize the system more safely and establish a safe mechanism system to detect the safety problems.

5. Conclusion

In a word, in order to ensure network security, we should not only strengthen computer network system management, but also apply firewall technology, data encryption technology, and set up intrusion detection system and physical isolation gateway on the computer. In the process of computer network security prevention, firewall, antivirus software, file encryption and digital signature technology should be installed, the security protection of user accounts should be strengthened, vulnerability patches should be downloaded in time, intrusion detection and network monitoring should be carried out, and the strategies of computer network security prevention measures should be continuously explored. In addition, it is necessary to establish a good computer network security system and improve computer security awareness, so as to reduce losses as much as possible and ultimately ensure the safety of the network system.

References

- [1] Li Jinxin, Computer network security and preventive measures. Electronic technology and software engineering, no.015, pp.187-187,2018.
- [2] Wang Xuemei, On computer network security loopholes and preventive measures. Science and technology wind, no. 9, pp.74-75,2017.
- [3] Cai Zhengang, Computer network security and preventive measures in the era of big data. Digital world, no.1, pp. 220-220,2018.
- [4] Yang Liqing, Computer network security precautions. Electronic technology and software engineering, no. 004, pp. 212-212,2017.
- [5] Wang Chunlin, Computer network security and preventive measures in the era of big data. Information recording materials, vol. 020, no. 005, pp. 71-72,2019.
- [6] Sun Qi, Analysis of computer network security problems and preventive measures. Digital world, no. 1, pp. 176-176,2018.
- [7] Li Qi, Computer network security and preventive measures in the era of big data. Electronic technology and software engineering, no. 020, pp. 207-207,2018.
- [8] Li Yuening, Research on computer network security precautions. Communication world, no. 9, pp. 25-26,2018.