

Research on Computer Network Security and Protection Technology under the Background of Big Data

Caijuan Huang, Zhuohua Liu

Guangdong Jidian Polytechnic, School of Electrical Engineering, Guangzhou, Guangdong, 510515, China

Keywords: big data; information security; computer network; Safety factor; Protection technology.

Abstract: Today's society has entered the data era; the arrival and development of the big data era has brought many changes to our life. Computer network is an essential tool in our daily life and work. With the gradual deepening of computer technology, the security of computer security network information has also received more attention. Based on the overview of network security in the era of big data, this paper analyzes the factors that affect the computer network security in the era of big data, and puts forward some suggestions for network information security protection strategies.

1. Introduction

With the continuous progress of science and technology, the development of computer network is more and more mature and perfect, but in the era of big data, computer information security has become a key concern of people from all walks of life. It is undeniable that big data provides great convenience for serving people's production and life, and it also plays an important role in promoting the development and progress of social economy. However, the risk of computer information network security is also increased, and the network technology crimes reported in social news are emerging in an endless stream, and the vital interests of the masses related to it will be affected and damaged. Therefore, it is necessary to take scientific and reasonable measures to improve this situation and ensure the information security of Internet people. In order to prevent the occurrence of computer network information security problems, we need to fully combine the characteristics of big data and network technology, scientific control and reasonable prevention, so as to promote the healthy development of computer network industry.

2. Overview of Information Security in the Context of Big Data

At present, the application of big data related technology has become an inevitable trend of development and innovation in China's multi industry fields. At present, with the increasing public demand for information resources, the content of information resources in China's social environment, as well as the current public demand for information resources transmission, access and storage and other aspects are also reflected in a higher level. Among them, due to the explosive growth of the current amount of information, people in the information society and the information age are showing a relatively abundant demand for actual information. Due to the increasing demand for information in daily life, both the public and enterprises need to get a better technology platform in information technology to meet their actual needs for information.

Big data technology is one of the technology types that can process information resources at high speed. While the speed of data processing is constantly improving, the application of big data related technology also makes most traditional industries get greater convenience in their own system construction. Through the use of big data related technology, enterprises can more easily store and process their own internal related information. When individuals use computers, they also break through the limitations of traditional computer technology, making information search and acquisition more convenient. In this regard, the development of information technology in the

context of big data, as the main theme of China's information technology development, has a certain high speed in the actual process

3. Factors Influencing Computer Network Security under the Background of Big Data Era

3.1 Man Made Destructive Factors

Improper operation or malicious attack of users will cause great damage to the computer network information security system. In particular, the malicious attack on the computer system has a great power to destroy the computer network system. This kind of malicious attack can be divided into two situations, one is the active malicious behavior attack. Some people take the initiative to use different attack methods to destroy the security and integrity of the computer network system, in order to destroy the relevant information. This kind of attack damages the information greatly. The other is passive attack, which refers to the operator's attack on the system in order to get some data information without affecting the security of the computer network system. Both active attack and passive attack will lead to the destruction of computer system information, leading to the leakage of information, which will seriously affect the security of computer network information.

3.2 Computer Network Virus

Computer virus has a great concealment, it is difficult to be recognized, and the computer virus is very destructive to the network. After the virus appears in the computer system, the virus will spread widely in the system through the normal program, which will cause a great threat to the security of the system. If the influence of computer virus is not great, people can use some application anti-virus software to deal with the virus and remove the virus. But if the virus enters the computer application system and appears in the process of people using the network, then the destructive power of this virus to the network system is hard to imagine. This virus will seriously destroy the hardware and software system, and It will severely damage the network data file.

3.3 Spam and Information Theft

The dissemination of garbage information mainly includes mail transmission and news, etc. it is compulsory to spread business, politics, religion and other information to others through the dissemination of garbage information. The main reason that information is stolen in computer network is that it is invaded by spyware. The difference between spyware and computer virus is that spyware does not damage computer system, but mainly steals system and user information, which involves computer security and user information security, and threatens stable and smooth network operation environment. Therefore, garbage information and information stealing are one of the factors that affect the security of computer network information

3.4 The Computer Itself is Vulnerable

The loopholes of the computer itself will also bring some hidden dangers to the computer network. Because of the loopholes of the computer itself, the system is easy to infect viruses and be invaded by others. This has laid a hidden danger for the computer network security, which is easy to be used by lawbreakers, thus providing favorable conditions for the network hacker invasion and virus invasion.

3.5 The Hidden Danger of Network Fraud

In recent years, with the continuous development of social economy and the updating of science and technology, some lawless people commit fraud through computer network, which causes important losses to people's property security. The computer network has the characteristics of openness, virtuality and freedom, which makes the network fraud appear frequently. Some lawbreakers carry on the network fraud through the network chat tool, and then realize the purpose of fraud by spreading false information or advertisement. "Xuyuyu case" further presents the

network fraud in front of people, which also reflects that the current situation of network fraud is very serious, and the cases caused by network fraud also cause people's widespread concern.

4. Network Security Strategy in the Era of Big Data

4.1 Network Firewall Technology

Network firewall technology is an internal protection measure to control network access. Its function is to prevent external users from using illegal means to enter the network system, so as to protect the internal network environment to a certain extent and provide a certain guarantee for the stability of the network operation environment. Firewall technology can check the data in the network transmission on the basis of safe network interaction. The implementation of the security measures through the operation in the established program determines the transmission block or permission of the target network data. The classification of firewall is based on the technical differences, and the firewall is divided into address conversion type, proxy type, detection type and packet filter type. The formation of targeted firewall access control under different technologies can organize threats outside the internal network environment and provide a certain guarantee for the normal operation of the network environment.

4.2 Network Monitoring and Supervisory Control

In recent years, intrusion detection technology has been widely used, but also has been developing. The role of intrusion detection technology is to detect whether the monitoring network has been abused or will be invaded in use. The analysis techniques used in intrusion detection include statistical analysis and signature analysis. The performance of signature analysis is to detect the attack behavior of the system weakness that has been mastered. The statistical analysis method is to use the statistical theory to judge the action mode in the stable operation of the computer system, so as to determine whether the operation action is within the safe range. The application of network monitoring and control technology in computer network provides a certain basis for the information security protection of computer network.

4.3 Encryption of Data Preservation and Circulation

Data preservation and circulation are universal in computer network. It is the requirement of computer network security protection strategy to protect the security of data preservation and data circulation in the era of big data. The data saving method requires file encryption. File encryption technology is a corresponding technical measure to prevent data from being stolen and destroyed on the basis of improving the security of information system and data confidentiality. Encryption protection in data flow refers to the use of digital signature technology. The purpose of data signature technology is to provide encryption services for the security of data flow and transmission. The encryption service of data signature technology is divided into two kinds, one is line encryption, the other is end-to-end encryption. Line encryption pays more attention to the security protection of line transmission. In line transmission, the security protection strength of the target information that needs to be kept secret is increased by using different encryption keys. The end-to-end encryption requires the use of encryption software. On the basis of encryption technology, the sender of the file encrypts the target file sent in real time through encryption software, and transmits the security information by converting the clear text in the file into ciphertext. When the target information reaches the destination, the receiver of the information needs to decrypt the ciphertext with the key. It is the ciphertext that can be converted into a direct one Then read the plaintext of the data.

4.4 Construction of Network Information Security Environment

Building a perfect network information security environment is an important measure to protect network information security. In order to construct the network information security environment, we should strengthen the construction and maintenance of the network facilities, apply various security measures in the network information system, strengthen the database system, strengthen the

construction and maintenance of the specialized and comprehensive computer network information security system, strengthen the construction and maintenance of the internal system database of the computer network, and guarantee the information stored in the database Safety of breathing. In order to ensure the security of key data information and the reliability and stability of data center operation, data storage system should be established based on the needs of data security and distributed storage management. We should be able to establish the evaluation standard of network information security, and judge the operation condition and operation quality of the network information security system based on this standard, so as to ensure the safe operation of the network information system.

4.5 Strengthen the Optimized Management of Network Resources

The optimized management of network resources can protect the network security and prevent the malicious attack of bad Web pages. Therefore, people need to strengthen the optimal management of network resources. Relevant organizations should be able to do a good job in the classified management of network resources; strengthen the supervision of network resources, find out bad network information, and eliminate it in time; create a safe application environment of network resources for people, so that people can get the information resources they need from the network safely and efficiently. Relevant organizations should do a good job in the integration and management of network resources of relevant websites, optimize and upgrade the service functions of hardware and software, make the network resources more concise and clear, provide people with a green platform for resource sharing, and enable people to better live and work with the help of network means.

5. Conclusion

Under the background of big data era, more attention should be paid to the security of computer network information in preservation, dissemination and circulation. The openness and coverage of computer network require the establishment of a stable and safe operation environment of computer network, and the strengthening of computer security information technology is of great significance to the establishment of a healthy and stable computer application environment.

References

- [1] Ma Yi. Discussion on computer network information security protection technology under the background of big data era [J]. Computer knowledge and technology, 2017,13 (25): 59-60.
- [2] Tang Ying. Computer network information security and protection measures against the background of big data [J]. Modern industrial economy and informatization. 2018 (1): 50-51.
- [3] Lv Fazhi. Computer network information security and protection measures in the context of big data [J]. Fujian computer, 2018 (6): 78-79.
- [4] Zhang Sen. computer network security and preventive measures in the era of big data [J]. Network security technology and application, 2018 (01): 55-59.