Analysis of Computer Network Information Security in the Age of Big Data

Chen Xi

College of Arts and Science of Jianghan University, Wuhan, China

Keywords: Big Data Era; Computer Network Information; Security Issues

Abstract: With the rapid development of economy and technology, the arrival of the era of big data has become a trend that people cannot avoid. In the era of big data, people's daily life is inseparable from network and technology, and computer networks have become inevitable demand of work and life, but currently people are facing the biggest problem in the process of using computer networks that is how to ensure the security of computer networks. Due to the emergence of computer networks, network security has become a new topic in the era of big data. Many users of computer networks have experienced theft of information, which has led to a decline in user experience. How to ensure computer networks in the era of big data safety has become the most important issue at the moment.

1. Introduction

Improving the computer network environment is the primary problem solved by technicians in the current technological development. With the development of computer networks, the use of Internet of Things technology and the use of cloud disks have doubled the number of people using computer networks. The increase in the amount of information has also led to an increase in the amount of information. Human beings entering the era of big data are the phenomena we must accept now, but the problem of computer network security arising from the era of big data is also a difficult problem in current computer networks. Long-term computer network problems will lead to a decline in people's trust in computer networks, and at the same time, they will be angry and troubled by their privacy violations. In the era of big data, computer networks must be secured.

2. An overview of big data

The so-called big data era has the following two characteristics: First, the amount of information that people can get in the era of big data is larger than before, which is its most basic characteristics, but with the continuous development of science and technology People have higher and higher requirements for the accuracy and timeliness of information, which leads to the need to improve data processing capabilities. Second, there are more and more ways to process information in the era of big data. Words are used to communicate, and current technological developments have made people diversified in the ways they can be used in interactions, such as video, pictures, audio, etc., which are the characteristics of the era of big data.

Second, how to ensure computer network information security in the era of big data

In the era of big data, the information explosion has become a very familiar situation for the people. In the face of excessive information and the security risks faced in computer networks, computer network users have many concerns when using computer networks, in order to ensure their use. Personal information in computer networks is not leaked. As a computer network user needs to clearly protect the importance of personal information, it can be carried out in two aspects when preventing computer network security risks, which are to prevent computer network security risks from technical aspects. Prevent the hidden dangers of computer network security from the aspect of management.

DOI: 10.25236/csam.2019.019

3. Implement security technology in computer networks

In the technical aspect of preventing computer network security risks, as a computer network user needs to use various information security prevention technologies to effectively ensure the use of computer networks to avoid viruses and hackers, and the use of computer networks. Illegal intrusion, etc., as a computer network researcher needs to provide users with a software system that can guarantee the security of computer networks, and regularly update them to prevent computer network security risks, and in the era of big data, computer network researchers need to increase The research on anti-virus software enables it to truly protect users' personal information protection in the use of computer networks, mainly through the following aspects:

3.1 Firewall isolation technology

When using a computer network, the firewall can effectively intercept all illegal intrusions outside the intranet used by computer network users, so that these illegal intrusions cannot be invaded into the computer network, if the computer network is exposed to viruses or When it is a hacker, the firewall in the computer will detect the information that is trying to invade the computer. If the detection result is different from the security setting requirements set by the computer network user, the firewall will issue a warning to the user to remind the user that there is a virus. And the hacker tries to invade, and directly intercepts these intrusions directly outside the computer network. In the process of using the firewall by the computer network users, the information of the computer network users can be effectively ensured not to be leaked. The application of firewall technology in computer networks can also ensure the detection of computer networks. Once abnormal data information appears in the computer network, it can be directly identified, helping computer network users to effectively avoid problems in use. Firewall technology can all information. Filtering, only the information detected by the firewall and safe can enter the internal network, present it in front of the user, as the user also needs to set up his computer network before using the computer to ensure effective security isolation. Protect your privacy.

3.2 password technology

The use of cryptography in the use of computer networks can effectively control the software system in the computer, help the software in the computer to encrypt, so as to ensure that the information in the computer will not be leaked. In the era of big data, if a computer contains large amounts of data, it is necessary to protect the information in the computer by applying multiple passwords to the software. When the computer network user uses the password technology, the computer network user can also remotely control and remotely control the password technology. When using the password technology, both computer network users need to encrypt the information transmission technology and encrypt the user identity. To ensure the security of the computer network users when using the computer network, both parties can also use the real name, or use the identity card information to protect both parties, and the information to be transmitted is protected from threats. In the current use of computer network software, there are many ways in which cryptographic techniques can be utilized by users to encrypt information.

3.3 Using Intrusion Detection System

The so-called intrusion detection system mainly refers to the system that the computer network user uses in the computer network to detect and intercept the illegal intrusion. Unlike other systems in the computer, the intrusion detection system has its own defense function. And with the computer monitoring function, the main monitoring object of the intrusion detection system is the user in the use of the computer network user. If the user is improperly operated when using the computer network, the computer will be introduced with a virus and cause a system vulnerability. The application of the intrusion detection system in the computer network can ensure that once the computer network user makes a mistake in the operation, the relevant information is obtained through the analysis of the current big data era, and emergency measures that can be repaired are taken according to the actual situation. During the monitoring process of the intrusion detection system, the system also detects the virus that attempts to invade the computer in the use of the computer network, ensuring that all viruses have no chance. However, the intrusion detection system needs to be used in the case of a computer network user's network. If the computer is not connected to the network, then the intrusion detection system cannot function. When the computer tries to connect to the network, the system analyzes the security of the port that the computer needs to connect. If the connected port is not secure enough, the intrusion detection system will directly check whether the network source is secure and ensure that the computer network user is connected. In the process of the network, the security of the computer can be guaranteed, and the repair function provided by itself can be utilized to make the system vulnerabilities be compensated. In this way, the computer can ensure that there is no breakthrough point of intrusion in use, improve the safety factor of the computer network in use, and promote the stability of the computer network.

3.4 Scanning for vulnerabilities in computer networks

Computer network users can install related system vulnerability scanning software on the computer before using the computer, and set the automatic startup function, which means that when the computer network user turns on the computer, the computer network is in the initialization state and the software is started. Status, and start scanning the computer network and the application software in the computer to prevent loopholes. Because the scanning software judges whether the vulnerability in the computer network, and the source of the vulnerability, etc., are all realized by using the computer network and then analyzing the network data, it is required to use the scanning software when the computer uses the scanning software. The abnormal data is scanned, the hidden dangers are found in time, and the information about the security risks in the computer network is semi-disclosed, so that other software in the computer can check the missing files of the computer. As the scanning software, the computer itself can not only determine the computer. The various vulnerabilities that exist in the system can also attack the virus intrusion problem in the computer. The application of the scanning vulnerability software in the computer network can greatly improve the security of the computer network information application.

3.5 Control access rights

When computer network users use computer networks, controlling access rights ensures that many computer network users have their computer's network in isolation from attempts to illegally invade, thus ensuring that computer network users use their computer networks when they use their networks. The environment has become more secure. When using control access rights, it is necessary to set certain requirements on the computer access behavior. The person who requires the computer must ensure that it has achieved the computer usage behavior before it can have access rights, so that it can enter a specific computer network through the computer. Enjoy specific web services. At the same time, as a computer network user can also combine password technology, identity authentication technology, etc., to make the access rights of computer networks become more urgent and strict, to ensure that computer network users are more secure when using computer networks, improve the overall computer Network security factor.

3.6 Identification Technology

The purpose of using identity technology in computer networks is to verify the identity of the computer network user, to ensure that the computer network used is the person, and to use the user's facial information or fingerprint information to ensure the computer when applying the identity recognition technology. The ability to identify the identity of computer network users, while using cryptographic technology can make identity technology more secure and an effective means of authentication. As a computer network technician, the biometric information of the computer network user can be input into the network system that needs to be identified, and the computer system needs to use the input parameter information as a reference for identifying the user. As a computer network user, when you log in to the account for the first time, you need to establish your own account in the computer, and reset your own login password to ensure that this password will become the login authentication method for computer network users in the future, using identity recognition technology. Only after the computer network user has successfully authenticated can the user continue to log in to the computer network and use the computer. If the user information is entered incorrectly, it cannot be used. However, the password authentication method and the identification technology have a relatively low security factor. Since the biometric information of the computer network user is unique, it is difficult to copy. Therefore, when applying the computer network, it is more secure to select the identification technology, but the current Technology will encounter many problems when using identity technology. For this reason, computer network researchers need to conduct more in-depth research on this issue.

3.7 access control technology

The application of access control technology in the computer network can ensure that the access range of the computer network user can be controlled when accessing the computer network, that is, the user can apply the access right only when the network scope permits, and obtain the range. Computer network resources within. At the same time, the computer network also needs to control and manage the resource access rights of the computer network users, and requires the user to ensure that one person has an account when logging in to the network to prevent the computer network resources from being maliciously occupied. Application access control technology can prevent hackers from invading. Once a hacker wants to access a computer network, it must obtain relevant permissions. If the technology can be effectively applied, the security factor of the computer network can be greatly improved.

4. Implement security management prevention on computer networks

The so-called security management prevention refers to the computer network security management personnel and the relevant departments in the actual application of the computer network, requiring them to continuously strengthen the network environment management, and establish a good network application order and management system in the computer network. In today's continuous strengthening of computer network information security, in addition to the need to vigorously develop computer network technology, it is also necessary for relevant departments to formulate supporting laws and regulations for computer network security, so that there are laws to follow and laws to follow, so as to ensure that in practice When using computer networks, users can be safe to use. At the same time, computer network administrators must meet the requirements of people in the era of big data for computer networks, and regularly improve their professional quality to ensure that they can be guaranteed when managing computer networks. Computer network user information security.

5. Conclusion

In summary, in the context of the era of big data, it is necessary to truly ensure that users will not be stolen when using a computer. It is not only necessary for the relevant computer network technicians to repair and adjust the computer usage system. At the same time, computer network users are required to improve their awareness of protection of information security. As relevant departments in China, it is also necessary to formulate relevant laws and regulations according to actual needs, to provide guarantee for computer network information security in the era of big data in China, and to ensure that Chinese netizens will not steal private information when illegally using computer networks. In the era of big data, users can have a secure network environment when using computer networks.

References

[1] Zhao Ying. Research on Computer Network Information Security and Protection Strategy in Big Data Era [J]. Information and Computer (Theoretical Edition), 2018(23):211-212.

[2] Lai Dehui, Chen Haitao. Computer Network Information Security and Protection Measures under the Background of Big Data [J]. China New Communications, 2018, 20(20): 146.