Research on Computer Network Information Security Risks and Solutions under the Background of Big Data

Song Lingyi

College of Computer Engineering, Sichuan Vocational and Technical Collage, Suining, Sichuan, China

Keywords: computer network information security; big data; solution

Abstract: In this era of rapidly changing information, information security risks also follow. The method to solve this problem is mainly based on the risk sources and characteristics of network information. The main contents of its countermeasures include computer network information security management, strengthening system security performance, preventing various security risks, and finally realizing computer network information security. This paper analyzes and discusses the effective protective measures under this background.

1. Introduction

At present, people are inseparable from the use of computer networks, and even the development of many enterprises are inseparable from computer networks. Therefore, the problem of network information security protection has gradually attracted extensive attention. In addition to strengthening the management of computer network information security, effective research and innovation of protection measures are also needed. In the context of big data, computer networks will produce a large number of important information content. Whether individual users or business units, if important information and data contents are lost, it may cause extremely serious losses. In order to provide users with higher security, we must start with security protection measures and study the computer network protection technology under the background of big data, so as to improve the use security of computer network.

2. Overview of Computer Network Information Security

The advent of the big data era will indeed have a great impact on the use of computer networks. In addition to providing development opportunities for computer networks, it will also bring a series of security risks and hidden dangers. Therefore, protective measures must be taken to deal with and eliminate the information security problems of computer network, so as to provide users with more secure use guarantee*(Hu Zhongyao,2019)*. To be exact, big data refers to all kinds of information and data generated during the operation of computer network. For example, people can obtain information content that meets the needs of work at any time in their daily life. However, in the process of information sharing or transmission, there are a lot of security problems, which may steal users' personal information and important data. Therefore, it is necessary to strengthen the security protection of computer network information to avoid serious losses. Although there are security risks in the use of computer networks, in order to avoid criminals stealing relevant information and data, users can carry out real-time protection through security protection measures, so as to reduce the probability of security risks and ensure the security of information transmission and sharing.

3. Influencing Factors of Computer Network Information Security

3.1. Security vulnerability

The era of big data is closely related to the popularization and application of computer networks. In such an environment and background, computer networks are vulnerable to a variety of factors, resulting in security problems, which can not ensure the safety of users. The most common is the risk problem caused by security vulnerabilities, because security vulnerabilities in the process of

  DOI: 10.25236/icmmct.2022.016

computer operation will provide hackers with opportunities to invade, which will have an adverse impact on their own use. Secondly, it will also improve the probability of virus intrusion, which will also threaten the use of computers, cause problems such as information and data loss, and lead to network paralysis in serious cases. Therefore, security vulnerabilities will seriously endanger the security of computer network system and can not effectively protect the use of users. In particular, enterprises will store and transmit important data, which adds computer network information security and protection measures against the background of potential big data.

3.2. Natural and human factors

Computers are mainly composed of extremely complex and sophisticated electronic components. They are very sensitive to external environmental factors and are easily disturbed or affected by natural factors. For example, when air humidity and vibration are too strong, computer equipment will be affected. In this case, the security of network information will be greatly reduced, which will also cause faults, system faults, information and data loss and other security problems. It is also possible that the user's use and operation may cause problems. Because many users are not professionals, they are more likely to make mistakes in the operation process, which will cause some damage to the computer system. If they cause system vulnerabilities, they will also be attacked by hackers. Secondly, many people have insufficient awareness of prevention in the process of use, and are easy to disclose their relevant information, which undoubtedly increases the security problem of computer network use.

3.3. Hacker virus

Hacker virus is a common security risk in the use of computer network. Many criminals use computer networks like professionals in related industries. Therefore, in any era and environment, it is impossible to avoid the security problems brought by hackers. In the past, hackers used professional tools to invade users' system vulnerabilities, intercept or monitor data information, and even destroy users' computer operations. Secondly, through network viruses, these viruses will spread on a large scale. Especially when the scope of the virus is large, it cannot be processed with anti-virus software, which will lead to serious damage to the computer system and the disclosure of information and data. Although the security of the network system has been improved in the big data environment, there are still incidents of hackers using viruses to invade, which will cause huge losses to users. Therefore, corresponding protection must be done to avoid virus attack. As shown in Figure 1:

Figure 1 Hacker factors.

4. Computer Network Information Security Protection

4.1. Network openness

At present, the use of computer network has a very significant openness, which also brings a series of security risks. Although TCP / IP protocol can play a certain role in the security protection of computer network, due to the development of the times, these methods have no protection effect and can not even meet the needs of computer network use*(Liao Lanfang, Li Yaopeng,2019)*. Due to

the openness of computer network, it does bring some difficulties to the security protection work, and also leads to the vulnerability to many factors, such as frequent hacker attacks and stealing important data and information. Therefore, the security problems brought by the openness of the network can not be ignored. At present, more effective protective measures should be taken to prevent various security factors, so as to ensure the safety of users in the open computer network environment.

4.2. Low risk awareness

At present, computer network has been popularized and developed in an all-round way. It is not only applicable to the office of enterprises, but also applicable to the daily life of many people. However, with the development of the times, computer network technology is becoming more and more complex. Many customers do not have professional ability and are not aware of their own operation and risk, which also leads to computer network risk. Many people search through potentially high-risk web platforms when looking for the resources they need. However, due to the lack of clear cognition of users, relevant data information is lost. In view of this situation, users' risk awareness should be improved. In the process of use, it is necessary to set difficult access passwords and install various computer network protection measures to improve the security factor of computer network.

5. Computer Network Information Security Protection Measures

5.1. Establishing good safety awareness

In the process of using computer network, a large number of security problems are related to users' own security awareness. Therefore, in the context of big data, we must first improve users' security awareness in order to fundamentally avoid security problems. Therefore, users should establish a good sense of security, know more about network security knowledge, and cultivate good operation and use habits. Secondly, we should avoid browsing websites with low security, strengthen the protection of important information and data, and prevent the disclosure of private information and personal information. In addition, we should strengthen the protection of account and password, improve the password level, achieve the protection effect, and replace it regularly to prevent the occurrence of computer network security problems.

5.2. Strengthening the safety protection of software and hardware

The overall structure of the computer consists of software and hardware. Therefore, in order to ensure the security of computer network, we must first strengthen the security protection of software and hardware, so as to avoid security problems such as information and data leakage, prevent information loss and destruction, and greatly improve the security of computer network. Generally speaking, the main purpose of hardware management is to repair and maintain the computer, check whether there are potential safety hazards, and properly replace accessories and equipment to improve the operation and use of the computer. In order to protect the security of software, we should use anti-virus software and other technologies to clean up junk software regularly to avoid virus data remaining in the computer. In addition, we should regularly attack the system, including patches and software, to ensure the normal operation of the software, set the functional restrictions of the software, and avoid causing computer network security problems.

5.3. Setting security permissions

For the security of computer network, relevant permissions can be set to form encryption effect. For enterprises, it will have a high safety factor, which can ensure the security of file transmission and sharing in the big data environment and avoid the loss of data information. In practical work, important data information must be encrypted to prevent strangers from reading and obtaining information content. In addition, relevant security permissions should be set according to the needs of enterprises and individuals to prevent the loss of data information during operation. At present, in the process of computer network use, it can be effectively protected by ID security permission, so as

to improve the security management in the process of use and provide convenience for information access, query and other work. Therefore, relevant enterprises and units should pay attention to the application for identity security license. As shown in Figure 2:

Figure 2 Network real name system.

5.4. Using monitoring intrusion detection technology

For the intrusion and attack of some criminals, monitoring intrusion detection technology can be used to ensure the security of computer network. Generally speaking, artificial intelligence detection technology and statistical detection technology can be combined to prevent the intrusion of criminals and improve the security of computer system and information data. Secondly, monitoring technology can effectively combine statistical analysis and feature analysis to judge whether there are potential information security risks or attacked security risks in the operation of computer network, so that users can prevent and effectively maintain computer network information in advance. Especially in the big data environment, there are many kinds of malignant software and viruses. Using this technology can reduce the threat of computer network security problems and reduce the interference of malware.

6. Conclusion

In the big data environment, there are various forms of network malicious attacks. The basic attack form of network security access using data packets makes it difficult to guarantee the network information and data security of relevant units, which will not only affect the protection function of the computer, but also cause irreversible damage to the data information stored on the computer platform. Therefore, relevant units need to coordinate and protect all kinds of data information according to their own data information use scenarios, so as to reduce the application risk of computer network information security. In addition, in the era of big data, in addition to optimizing the safety protection measures in supervision, we should also launch a more comprehensive data and information protection barrier in combination with anti-virus software with different application attributes. Finally, firewall technology is an important part of enterprise information security protection under the background of big data. Whether its parameter configuration has protection flexibility is related to the interests of all units and the development of units.

References

[1] Hu Zhongyao.Computer Network Information Security and Protection under the Background of Big Data Era[J].Communication world,2019,26(01):39-40.

[2] Liao Lanfang, Li Yaopeng.Computer Network Information Security and Protection Methods in the Era of Big Data[J].Electronic testing,2019(09):130-131.