Analysis and Countermeasure Research on Influencing Factors of Computer Network Security Based on "Big Data"

Chenglong Du

Guangdong University of Science and Technology, Dongguan, Guangdong, 523073, China

email: 179074904@qq.com

Keywords: Big Data; Computer Network Security; Countermeasure

Abstract: With the development of the times, science and technology have been rapidly updated and progressed. Internet has gradually affected our daily work, life and learning. Computer information network has brought unprecedented benefits to social progress and the rapid development of various industries. At the same time, it has also produced many problems. The research on the application of computer network security technology in the era of big data is of great significance. Based on this, this paper expounds the content of big data network security and related issues one by one according to the characteristics of network security management in the environment of big data. And an effective big data network security management scheme has been formulated, which has played a reference role in the computer network security protection work under the big data environment.

1. Introduction

The era of big data has brought a lot of convenience to people. People can find the required data more conveniently and quickly. However, due to the lack of related technologies in the process of use, it has brought a lot of network security problems to people, which has restricted the big The development of the data age [1]. At present, data information has become an indispensable thing in people's lives, such as the transmission of political and economic information, and the purpose of sharing data information through computer networks, bringing efficient and rapid development of computer networks [2]. As we all know, the network has strong virtuality. Internet users communicate and communicate in a virtual space, which to a certain extent will promote the possibility of cyber crime. Big data has penetrated into almost all industries and fields in our life. Computer information network has created a digital new world through the collection, storage, sharing and calculation of big data, which we cannot see but affects us all the time [3]. In order to better adapt to the development environment of big data network, it is imperative to do a good job in the management of big data computer network security and improve the level and capability of network security management.

2. Computer Network Security in Big Data Environment

2.1. Information content security risk

The security risk of network information content is the main problem to be solved in the framework of computer network security under the big data environment, and it is also one of the main directions of network security management at the present stage. When users operate computers, they are often influenced by their subjective consciousness, thus burying hidden dangers in the security of computer information network. Under the open characteristic of computer network information system, the self-protection ability of TCP IP protocol used in computer information network is weak, which results in the fragile security of computer information network [4]. In addition, when people get information through the Internet, they are likely to be tempted by some external conditions to leak their own information. When leaked information is spread out, users will have no privacy, causing great trouble to users to some extent. Once the network information security cannot be guaranteed, the development of network information management will also be hindered.

  DOI: 10.25236/mmmce.2019.077

Illegal elements can illegally obtain the privacy information in the network, and then carry out network attacks or seek profits [5]. The other is passive attack behavior, i.e. cracking or intercepting data information passively without any impact on the normal operation of the computer network. After the operating system itself has problems, it will cause problems in the user data management of the system. Regular repair of the operating system can effectively reduce the losses caused by system vulnerabilities.

2.2. Security risks at management level

The open nature of computer networks in the context of the era of big data provides convenience for viruses to attack computer networks. At the same time, the virus's own unique storage, concealment and executive characteristics. The network security risks at the management level mainly come from the enterprise side. In the management level, the root cause of cyberattacks or illegal network intrusions is mainly through network attacks or illegal intrusions, which can cause enterprise network systems to become paralyzed [6]. In the management of account security protection, users need to establish a good sense of computer security application and management. Under the condition of ensuring a good sense of security, the account password should be set scientifically, while ensuring that the account password will not be leaked [7]. This kind of network security risk attack environment is complex, and it is difficult to prevent network security, and it is difficult to find the attack address and attack source, which makes the economic losses of enterprises increasing. By dealing with the complex settings of the account number, increasing the difficulty of password cracking and changing the user's password regularly, the risk of users being stolen and leaked can be effectively avoided, which is a more effective computer network information security protection strategy.

2.3. Physical component security risk

The security risks of physical components are relatively small and relatively easy to be ignored. However, once they are unable to construct security risks, their problems are more serious, which can easily lead to a large number of embarrassing phenomena in computers and local area networks. For each network user, the computer operation technology and security protection concept will be different, and it will be very different in the process of setting user password and network operation [8]. The staff does not have a strong sense of security and prevention. In the course of work, the risks and vulnerabilities in the user's host system cannot be discovered in time, and the hacker can easily invade the user's host system, resulting in information destruction and leakage. Network computer hardware systems are mostly composed of circuit boards, chips and electronic output and input devices. The operation of the devices requires high external environmental conditions. Failure to pay attention to environmental treatment of environmental temperature, humidity, heat dissipation and other related aspects will lead to computer hardware damage and network security problems. This involves computer security and user information security, and poses a threat to a stable and smooth network operating environment. Therefore, spam and information theft are one of the factors that affect the security of computer network information.

3. Solutions to Computer Network Security Problems in Big Data Environment

3.1. Pay attention to the construction of information management security system

With the leap-forward development of Internet technology, users often store key personal privacy information such as name, address, consumption record and contact mode in the accounts of various platforms. The management of network security information in large data environment needs to start with the user's account security. Users themselves attach importance to the security protection of computer network information account, which is one of the most effective ways to actively protect computer network information. Paying attention to the security protection management of computer network information is through the internal protection measures of computer network security. When protecting the internal factors of network security, we should attach great importance to account

security management. Under normal circumstances, account security management involves a relatively large number of contents, including computer system accounts, online banking accounts, communication accounts, etc. Through real-time protection, the overall security of the account can be ensured. According to different types of network accounts, various network security information management modes are adopted to effectively reduce the security risks of user accounts. Secondly, setting special symbols in account security management can effectively avoid the occurrence of identical passwords due to simple password setting. Secondly, attention should be paid to the length of passwords and their regular replacement. The computer network security system mainly carries out detection work on computer data passwords, software, U disks, patch upgrades, etc. Because the security prevention system is a prerequisite for computer network data information management, only by ensuring the normal operation of the security system can a secure environment be provided for computer network operation.

3.2. Realizing the application of intelligent firewall technology

Firewall technology is a technology that scientists have gradually developed in the era of big data. This technology can achieve perfect isolation between internal and external networks. As a modern protection technology, firewall technology can prevent external users from entering the computer system in an illegal way to achieve access and intrusion of the computer system. In the early stage, the network security firewall technology application mainly adopts the passive protection mode, and does not have the automatic protection capability, and the network security protection effect is not high. At the current stage of the development of big data network environment, both network attacks and network intrusions are initiated using automated and intelligent management technologies. This can protect the internal computer network to a certain extent, thus effectively ensuring the internal stable operation of the computer information network. The construction of an intelligent firewall network system cannot control the network security risks of the external environment alone, but must have the capability of analyzing and processing the internal network security risks, so as to effectively improve the practicability and functional characteristics of the network firewall. The formation of targeted firewall access control under different technologies can organize threats outside the internal network environment and provide certain guarantee for the normal operation of the network environment.

3.3. Actively do a good job in standardized management of data security

The standardization of data security management will directly affect the efficiency of big data network security management. In terms of data processing, the first thing is to form an effective data management system to ensure that technicians can carry out network data security management according to the security operation standards. Improving the safety awareness of network users is also a quick and reliable way to ensure network safety, strengthen the safety education of network users, and master basic network safety technology and network safety knowledge is helpful for network users to use the network more safely and conveniently. Through the relevant software, the information nature of the user's computer to be invaded can be monitored in time so as to make relevant decisions. Intrusion information monitoring technology is not only a dynamic and real-time monitoring technology, but also a network device with active defense function. In many cases, it can also make up for the loopholes and deficiencies of the firewall. The core of this kind of data encryption technology lies in the difficulty of encrypting the data storage algorithm and the confidentiality of the encryption algorithm. When the hacker attacks the system, if the data encryption technology is hindered, the key is usually the main attack of the hacker. Optimize the basic network security management structure, so that the network security management work forms multiple sets of network security management modes, so as to take effective network security prevention and management solutions for different network security management problems.

4. Conclusions

In summary, the computer network security risk control and management in the big data

environment needs to comply with the current network security management standards, and do well the network security risk warning and control without affecting the normal conditions of the network system normalization application. And develop a network security plan. In order to ensure the security of computer network information, it is necessary to give computer network information security protection a high degree of attention, increase the security of computer network information security, improve the professional quality of computer users, and establish a good awareness of computer network information security protection. Only by solving the current network security problems can the confidentiality and security of relevant information be improved and people can use it more confidently. In addition, the intelligent technology of data information can reduce the workload of staff, improve the efficiency of computer network operation and management, and promote the steady development of computer enterprises. Strengthening computer security information technology is of great significance to the establishment of a healthy and stable computer application environment.

References

[1] Dupont Q, Fidler B. Edge Cryptography and the Codevelopment of Computer Networks and Cybersecurity. IEEE Annals of the History of Computing, 2016, 38(4):55-73.

[2] Jakalan A, Gong J, Su Q, et al. Social relationship discovery of IP addresses in the managed IP networks by observing traffic at network boundary. Computer Networks, 2016, 100:12-27.

[3] Krzysztof S, Liqiang W, Xiangyang L, et al. Big Data Analytics for Information Security. Security and Communication Networks, 2018, 2018:1-2.

[4] Stasiuk O I, Grishchuk R V, Goncharova L L. Mathematical Differential Models and Methods for Assessing the Cybersecurity of Intelligent Computer Networks for Control of Technological Processes of Railway Power Supply. Cybernetics and Systems Analysis, 2018, 54(4):671-677.

[5] Ni Z, Li Q, Liu G. Game-Model-Based Network Security Risk Control. Computer, 2018, 51(4):28-38.

[6] Bisht N, Ahmad A, Bisht S. Application of Feature Selection Methods and Ensembles on Network Security Dataset. International Journal of Computer Applications, 2016, 135(11):1-5.

[7] Cheng L, Duo-He M, Hong-Qi Z, et al. Moving Target Network Defense Effectiveness Evaluation Based on Change-Point Detection. Mathematical Problems in Engineering, 2016, 2016:1-11.

[8] Ender Yüksel, Nielson H R, Nielson F. A Secure Key Establishment Protocol for ZigBee Wireless Sensor Networks. The Computer Journal, 2018, 54(4):589-601.