Discussion on computer network security in the era of big data

Sufang An
Beijing Open University Beijing 100081

Abstract: with the advent of the cloud era, big data technology has penetrated into various industries and fields and become an important factor of production. However, due to the openness and complexity of network technology itself, the computer network security problem under the background of big data has become increasingly prominent. In order to solve this problem, this paper analyzes the main problems existing in the computer network, and discusses the solutions and countermeasures from the aspects of optimizing protection technology, optimizing firewall technology, updating isolation technology, etc., in order to discuss and solve the computer network security problems in the era of big data.

Keywords: big data; Computer network; Safety issues; Countermeasures

With the wide application of cloud computing, Internet of things, mobile Internet and other technologies in production and life, all kinds of data are stored and recorded. Mankind has entered the era of big data, and big data technology has become an important force driving the transformation and innovation of production and life style. However, with the increasing complexity of the big data system and the rapid progress of data sharing and transmission, the potential network security problem has become a key issue that can not be ignored in the era of big data. Once the network responsible for data transmission has security problems, such as network interruption, data leakage and data tampering, it will directly affect the operation of the whole system, The computer network security problem in the era of big data has been widely concerned by the majority of researchers. This paper first analyzes the security problems of computer network in the era of big data, and then puts forward the corresponding solutions.

1. Analysis of computer network security in the era of big data

1.1 Operating system vulnerabilities and risks

As the basic operating environment of computer system, the operating system plays a very important role, which leads to the operating system being a relatively more concentrated area of network security risks, especially the cloud operating system in the era of big data. In the process of using the computer, users need to run the operating system to complete the corresponding instructions. Once the operating system crashes, the computer will also lose all functions and functions. Vulnerabilities in the operating system provide more possibilities for Trojan virus to attack computers, making computer network security problems frequent. Generally speaking, in the design process of the computer operating system, in order to facilitate subsequent updates, the background space will be reserved on the operating system. Its essential purpose is to facilitate the maintenance and management work. At the same time, the operating system belongs to the multi-user system, which also makes the operating system a place to be targeted and attacked, and there are certain risks in the normal operation of the computer. As the main constituent element of the network system, the vulnerability of the operating system is bound to increase the security risk of the computer network, which is a key problem that must be paid attention to and solved urgently.

1.2 Wanton spread and infection of network virus

Network virus refers to the program code that destroys the data of the computer. It will not only change the normal running program, but also automatically copy or modify it to other programs, which makes the computer unable to operate normally, and it is difficult to remove and repair the computer. At the same time, computer viruses are highly infectious. They can be spread through a variety of channels. For example, they can be disguised as all kinds of mail, inserted into unsafe mobile media, or installed with programs from unknown sources. There will be a risk of virus transmission, which will damage the Internet environment, resulting in a wide range of computers unable to use normally. In the era of big data, device links are closer and data transmission is more frequent, which leads to more and more transmission channels and virus types, and the transmission speed is faster and faster, which has become one of the important factors threatening the security of computer networks.

1.3 Weak user safety awareness and lack of prevention

In the era of big data, users use computer networks more frequently. People often retrieve information, operation instructions, or mine and analyze information data according to their own needs. In order to effectively prevent potential security problems and improve the effectiveness of computer network security management, it is urgent to enhance users' awareness of network security, so that they can truly participate in the maintenance of network security and purification of the network environment. Only when each of us fully attaches importance to network security, continuously improves our own security literacy, and uses computers and network equipment in strict accordance with the specifications, can we solve the hidden dangers of network security from the source, so as to build a healthy, pure and green network environment. However, at the present stage, the majority of users lack the relevant prevention awareness and identification ability when using the computer network. For example, users have recessive bad Internet habits, often click the pop-up box to browse some untrusted websites, download programs from unknown sources or without signatures, which leads to computer virus infection and covert transmission within a certain network range, thus bringing potential security risks to the entire computer network system. In addition, e-mail is also a serious disaster area threatening the security of computer network. When users click the link in the e-mail from unknown sources, it will also lead to the spread of virus or the loss of information, making the computer vulnerable to network attacks.

2. Solutions to computer network security problems in the era of big data

2.1 Building a data driven virus defense system

Ensuring the security and stability of the system is the primary link to solve the computer network security problem under the background of big data. Network virus invasion is the main factor threatening the computer system. Once the computer is infected with virus, it will cause immeasurable loss to the data. Therefore, it is necessary to strengthen the virus prevention of the computer system to ensure the normal operation of the whole system. Usually, you can set up an anti-virus module in the background program. Once you find suspicious software or web links, you will automatically remind the user and stop the access operation, and often use the network anti-virus software to carry out anti-virus treatment on the computer, and timely repair and update various types of vulnerabilities in the system, so as to fundamentally improve the security and stability of computer network operation.

However, in the traditional computational virus detection method, only when the virus appears can we build an effective protection method according to the characteristics of the virus, which belongs to the prevention system only after the virus has caused a wide range of harm, which can be called "follow-up" prevention system. In order to overcome the lag of this method, with the substantial improvement of the real-time performance of the big data acquisition method, researchers quickly find viruses and build a prevention system by analyzing data in real time, which is called "parallel" prevention system. This method greatly avoids the risk of large-scale virus transmission to the computer network. However, with the increasing complexity of the computer network, even if the virus can be found at the first time, the construction of the prevention system will take some time, which will still bring risks to the network system. In order to solve this problem, we can analyze the data situation in complex networks through data mining, knowledge mapping and other technologies, and build a data-driven virus detection model and prevention system. That is, we can discover potential virus risks and system hidden dangers in advance based on data, and timely investigate and solve them to avoid the emergence and spread of viruses, which can be called "leading" defense system.

2.2 Optimize firewall technology to achieve accurate virus isolation

In order to scientifically respond to hacker attacks and intrusions, the isolation technology needs to be updated to make it more targeted. In today's computer networks, the isolation technology mainly realizes the effective defense against hacker attacks through the construction of data channels and physical isolation. In order to reduce the interference and damage caused by the massive spread of computer viruses to the computer network, it is necessary to optimize and upgrade the firewall technology, accurately isolate the computer viruses, and then provide effective support for the prevention and control of network viruses. Big data technology can provide comprehensive information resources and timely update relevant content, and can timely identify potential risks and threats. Through big data technology, we can understand the mode of user access and accurately locate the areas and time points where there may be potential security risks. For example, if users access more frequently and frequently in a certain period of time, it proves that risks are prone to occur in that period of time.

The emergence of computer network security problems is directly related to the improvement of the firewall system. By building a perfect firewall system, we can comprehensively control and deal with various security threats in the computer network. As for the firewall system, its main function is to isolate different types of networks, ensure user information security by setting firewall or intrusion detection mechanism in the system, as well as effective identity recognition and other security measures, and restrict the user's use rights and access content between different networks. Therefore, we must improve the firewall technology according to the computer network security problems. For example, tcp/ip protocol can be used to isolate various networks and restrict their access rights. In addition, the site where the computer host is accessed can be isolated from the protected website by setting a dedicated IP address, key management and intrusion detection, so as to better protect the privacy of computer users and data information security.

2.3 Improving encryption technology to ensure data security

Data encryption technology is a common method to ensure the security of data and information. Using encryption technology to compress and encrypt the files in the computer can effectively prevent the data from being infected with viruses in the transmission process, and physically realize the isolation of data channels. A variety of encryption methods can be used in data transmission to further enhance the security and stability of computer network information transmission. The commonly used encryption methods include AES encryption algorithm, DES encryption algorithm and IPSec protocol. At the same time, all kinds of data and information generated in the network should be strictly confidential, so as to ensure the security and stability of different types of information, and strengthen the effective defense against hacker attacks and intrusions by building a data channel isolation mechanism. In addition, in the application of computer network, it is necessary to strictly abide by relevant regulations and laws and regulations to carry out file encryption.

2.4 Building rules and regulations to enhance users' safety awareness

In order to meet the needs of modern society for information security, it is necessary to strengthen users' awareness of information security. How to cultivate users' good network security awareness is a long-term and arduous task for any organization. Relevant research shows that many network security problems are caused by bad network usage habits. In the process of using the computer network, users should update and maintain the computer system regularly. Organizations should strictly control and manage the access rights of various systems, especially for the wide variety of equipment and interconnection in the big data system. A strict and efficient access system is particularly important, which can greatly reduce the harm and impact of hacker attacks and intrusions on computer systems. During the network security attack and defense exercise of the education industry in a province in 2022, many vulnerabilities were caused by simple or unreasonable access rights in the supply chain, which suggested that each organization structure should establish corresponding risk prevention mechanisms for network security issues, and should also strengthen its own security awareness and level when using computer networks to improve its quality. Especially when using large-scale Internet platforms, we need to pay more attention to relevant security issues, and we should also have a certain self-protection ability and prevention consciousness to ensure that the legitimate rights and interests of ourselves and others are not infringed. Relevant departments can use big data technology to continuously track, research and analyze computer network security issues, and constantly summarize experiences and lessons in the process to improve the security management mechanism, so that it can play a role of prevention and protection.

At the same time, each organizational structure should strictly implement the national network security level protection system, formulate the internal security management system and operating procedures, determine the first person in charge of network security, and implement the responsibility of network security protection; Formulate and implement a hierarchical access mechanism for information systems and hardware equipment, and clarify the importance and application scope of each system and equipment; Improve the operation and maintenance mechanism of the core equipment, ensure the safe and stable operation of the equipment, strictly control the scope of influence after the occurrence of security problems, and develop efficient and feasible response methods to ensure the safe and stable operation of the computer network.

Concluding remarks

The application of big data technology in social development provides more convenient and efficient services for people’s production and life, and also promotes the transformation of economic model. However, the rapid development of big data technology has also brought some threats to computer network security. Therefore, we should optimize the technical means of computer network security, strengthen the application practice of major data, strengthen the awareness of user information security, and improve the supervision mechanism of computer network to ensure the computer network security under the background of big data. At the same time, how to make full use of artificial intelligence technology to analyze the network operation situation, predict network viruses and risks, and build a defense system in advance is a major research direction to ensure the safe operation of computer networks in the future.

References:

[1] Baolong Wang Discussion on the application of artificial intelligence in computer network technology in the era of big data [j]China new communications, 2022,24 (18): 104-106

[2] Fengming Li Computer network security defense system based on big data and artificial intelligence technology [j]Electronic technology and software engineering, 2022 (17): 1-4

[3] Hua Zheng,Aoying Ji,Wei Liu,Tong Xia,YeDing Ding Network security vulnerabilities and preventive measures in the era of big data [j]Digital communication world, 2022 (08): 84-86

[4] Hui Xu Application path analysis of computer network security in public institutions under the background of big data [j]China new communications, 2022,24 (13): 92-94

[5] Limin Yu,Lixin Xin Effective application of computer technology in food enterprise safety management process under the background of big data [j]Food safety guide, 2022 (18): 51-53