Computer Network Security Processing Technology in Big Data Environment

Chuanxue Wu

Hubei Engineering University, Hubei , China

ABATRACT. *With the continuous development of social development process and the open sharing characteristics of data presentation, it provides more efficient network information services for the majority of audiences, and also brings the security of computer network information. Therefore, based on the background of big data, this paper analyzes the problem of computer network information security, and proposes targeted security processing technology countermeasures, aiming to provide help for the security of computer network information technology.*

KEYWORDS*: big data; computer network security; processing technology*

1. Overview of big data meaning

Big data, like the content expressed by its literal meaning, collects and organizes a large amount of data with the same characteristics into a variety of information, big data has the characteristics of low wood[1], accurate positioning, fast update, etc. Data is not just a storage medium for network information, it contains a variety of data formats. [In recent years, with the continuous updating of computer technology, the application of big data not only makes people's life more convenient, it is for the country. Development also has a very important strategic significance. However, because the popularity of big data is too fast and the scope is too wide, the information security problem of big data transmission is serious, and the safe storage of information is not guaranteed. The economic losses caused by it will have an impact on the country's economic development, and will also hinder the popularization of computer technology.

2, big data environment computer network security issues

2.1 Hacking

In the process of troubleshooting computer network security failures, relevant personnel found that hacking is a major cause. There are two main types of hacking: First, hackers conduct proactive attacks. That is, in the process of destroying data information, hackers are targeted, resulting in a large amount of data loss and huge losses. Second, hackers conduct passive attacks[2]. In the process of intrusion, some data information is cracked to a certain extent, or the data information is intercepted, but the computer network can still operate normally, and the process is passive. No matter which form of hacking, it will have a greater impact on the data information, resulting in the loss of data information, which will have a greater impact on the subsequent operation of the computer network and bury hidden dangers. In severe cases, it can cause embarrassment in the computer network.

2.2 Spam and information theft

In the daily life, I often receive some spam. There are many ways to spread spam, including mail distribution, software distribution, and so on. The spread of spam will spread a large amount of data. The information is stolen, mainly because the computer network is invaded by some illegal software, but there is a certain difference between these illegal software and computer viruses. The illegal software will not affect the computer system, but will have a certain degree of data information. Stealing seriously affects the security of user information, and it also brings certain harm to computer security. Spam and information theft is also an urgent need to solve computer network information security issues[3].

2.3 Trojan virus invasion

After fully observing the computer virus, you will find that the computer virus has a long process of latency. As long as the computer is connected to the network, it provides a certain intrusion opportunity for the virus. When a computer is invaded by a virus, it can cause great harm. At present, the types of computer viruses are very numerous. In order to improve the defense ability of computers to a certain extent, it is necessary to check and kill computer viruses. In general[4], you can install some virus killing software on your computer to solve the problem of computer virus intrusion. For the Trojan horse invasion problem, the essence of the Trojan is a kind of artificial computer virus, which will bring great harm to the computer.

2.4 system vulnerability

In the process of continuous development, the computer will fully research and investigate the user's habits and actual needs, and based on this, the computer will be continuously upgraded to meet the needs of the majority of users. However, in the process of continuous upgrading and patching, there will also be system vulnerabilities. During the use of the computer network, it may be attacked, resulting in the lack of relevant data information. At the same time[5], the computer is faced with different groups. The usage habits between users are different due to various reasons, which increases the probability of system vulnerabilities to a certain extent, resulting in the security of the computer being compromised. Small, and has caused some obstacles to the development of network security protection technology.

3. Computer network information security prevention processing technology

3.1 Strengthen the effective use of firewall security systems

Combining several years of learning experience, through in-depth analysis of the above major influencing factors, we can establish an effective information security protection measures to reduce the economic losses caused by network security, and today's big data era is unstoppable[6]. The benefits it brings are far greater than the losses caused by it. By actively responding to network security issues, actively seeking solutions and purifying the network environment [continually strengthening network firewall technology, isolating network viruses, and resisting network attacks [nearly this year, with People pay more and more attention to network security issues. Firewall technology has been updated several times, and its anti-attack capability has been improved. It can withstand most network attacks.

(1) Use anti-virus software. Anti-virus software is a computer network system software specially designed for computer network viruses. With the reasonable application of firewall, it can effectively detect viruses that endanger the security of computer network information. In addition to killing known viruses, it can also detect the maliciousness of some hackers. Attack programs that help enhance the security of your computer network. During the application of anti-virus software, you should upgrade the anti-virus software virus database to ensure that you can check the latest computer viruses and ensure the security of network information.

(2) Apply network firewall technology. This kind of technology is a computer network security protection technology that effectively controls the security of network access, which can ensure the security and stability of the internal network environment of the computer. Firewall technology is mainly based on network interactivity, by using the established program to check the network transmission data to see if it meets the transmission requirements or standards of network data, thereby preventing or allowing the passage of network data.

(3) Application of network monitoring technology and intrusion detection technology. In recent years, intrusion detection technology has been rapidly developed and widely used. It mainly monitors whether there are abuses or intrusions in the use of the network. Commonly include signature analysis techniques and statistical analysis techniques, the former mainly for those The computer network system weaknesses that have been mastered are detected; the latter is based on statistical theory to determine whether the computer system's operating actions are within a safe range, thereby protecting the security of computer network information.

3.2 Strengthen related software and hardware management

In order to ensure the security of computer network information, in addition to actively citing advanced anti-virus software and technology, it is necessary to strengthen the use and management of software and hardware of related computer network information systems, thereby improving the reliability and security of computer network system operation. For example, the administrator of a computer network system should formulate a scientific and reasonable management plan, effectively maintain the software or hardware in the computer network system, ensure the suitability of their operating environment, and pay attention to regular updates and upgrades. Software or hardware devices with quality problems, such as anti-virus software, should be upgraded in time to ensure that the virus database is updated to the latest state. Otherwise, the virus database data may not be enough to check the latest virus data, so that it can be effectively improved. Reliability and security of computer network information operations.

3.3 Enhance personnel safety awareness

On the one hand, we must do a good job in the education and training of all computer network system operators, and regularly instill relevant technical knowledge of computer network information security operation methods, such as how to use various types of security control software, or how to do it during the application of computer network systems. Operations, etc., ensure continuous improvement of the level of operation of their computer network systems. For example, when using a computer network system in peacetime, pay attention to the security protection of various accounts such as online banking, computer systems, and mail. For example, the corresponding account password setting should be more complicated, such as comprehensive use of numbers, letters, punctuation, etc. To avoid being too simple, but also pay attention to regular replacement of account passwords. On the other hand, it is necessary to do a good job in the technical assessment of all computer network system users, and to assess their actual operational skills, in order to encourage all operators to independently improve their operational skills, to ensure that they better meet the new era of computers. The network information security operation requirements ensure the reliability and security of the computer network system operation.

4. Conclusion

In summary, the security problems of computer network information in the context of the era of big data are complex, including personnel operation problems, natural disaster factors, network characteristics, hacker or virus intrusion, information theft and spam. In order to effectively prevent computer network information security issues need to start from the awareness of safe operation of personnel, actively apply some advanced security protection software and technology, and at the same time strengthen the use of related software and hardware management to ensure the security and reliability of computer network system operation.

References

[1]Yang T , Jia S(2016). Research on Network Security Visualization under Big Data Environment. International Computer Symposium. IEEE Computer Society.
[2]Karthikeyan P , Amudhavel J , Abraham A , et al(2016). A Comprehensive Survey on Variants And Its Extensions Of Big Data In Cloud Environment[C]// International Conference on Advanced Research in Computer Science Engineering & Technology, ACM.
[3]Bachupally Y R , Yuan X , Roy K(2016). Network security analysis using Big Data technology. Southeastcon, IEEE.
[4]He S , Zhang C , Guo W , et al(2015). Worms Propagation Modeling and Analysis in Big Data Environment. International Journal of Distributed Sensor Networks, vol.12, pp. 1-9.
[5]Xu H, Fan G, Ke L(2017). Improved Statistical Analysis Method Based on Big Data Technology. International Conference on Computer Network, no.9, pp. 123-136.