ISSN 2616-7433 Vol. 4, Issue 11: 33-37, DOI: 10.25236/FSST.2022.041105

Probe into Computer Network Information Security and Protection Strategy in the Age of Big Data

Qi Yina

Wuhan University of Engineering, Wuhan, 430000, China

Abstract: *With the progress of computer network technology, the arrival of big data era has brought great changes to various fields in China, and people's lives have been inseparable from the application of information technology. In the era of big data, data information is shared and transferred quickly in the cloud through the network. Network technology has played a very important role in all aspects of the country's politics, economy and people's livelihood, bringing convenience to people's lives and work. But at the same time, computer network information security problems have also emerged frequently, giving people an alarm about how to protect data information, It is an urgent problem to avoid the hidden danger in property, reputation and even security brought by data leakage to the country or individuals. This paper conducts research and analysis on this, discusses how to improve the security level of computer network information in the era of big data, and gives specific protection strategies.*

Keywords: *Big data era; Computer; Network information security; Protection strategy*

1. Introduction

According to the survey results of CNCERT (National Internet Emergency Center) and CNNIC (China Internet Network Information Center) in 2016, 52% of Internet users had network security problems while surfing the Internet, and the cost of dealing with network security incidents reached 15.3 billion yuan. After the arrival of the big data era, the problem of information security has become more and more serious. However, there are still some Internet users in China who do not realize the importance of network security issues. There are still 4.4% of Internet users who have not used any security software. In addition, less than 8% of Internet users have installed security protection software on their mobile phones. Compared with developed countries that have entered the network era quickly, the information security awareness of Internet users in China needs to be improved.

2 Big data application and network information security

2.1 Big data application

Big data is one of the most important information technologies. With the development and popularization of computer networks, it has been widely used in various fields of social life. One of the most representative is the application of data technology in the public security system. Today, China's public security work collects and analyzes information through big data technology, which greatly improves work efficiency. Big data technology is widely used in military management, law enforcement, urban and border control, which has played a great role in the stability of our society[1]. Through the analysis of big data technology, Digital working mode has brought great changes to our country.

2.2 Network information security under big data

Although big data technology brings great convenience to people's life and work, it also brings new information security problems. The Network Security Law of the People's Republic of China stipulates that the necessary protective measures to be taken to maintain the integrity of network data and the stability of network operation, or to protect confidential data, are network security protection capabilities. Specifically, network security means that the data information of the country and individuals is under protection, and they have certain self-protection ability in the face of illegal network interference and attacks. In the age of big data, the anonymity and concealment of computer

ISSN 2616-7433 Vol. 4, Issue 11: 33-37, DOI: 10.25236/FSST.2022.041105

networks are challenged, and the problem of information security is becoming more and more serious, such as man-made hacker attacks and virus attacks, which may cause great damage to the network security protection system[2]. In addition, the possible data leakage accidents or personal information exposure require corresponding information security protection measures to deal with, Therefore, Chinese computer industry practitioners should pay attention to information security issues and accelerate the construction of computer network information protection system in the era of big data.

3. Factors affecting computer network security in the context of big data era

3.1 Natural disasters

Computer hardware equipment is usually fragile, unable to withstand the damage caused by natural disasters. Environmental changes caused by high temperature, fire, water inflow, vibration, extrusion, electric shock and other natural disasters will damage computer hardware equipment, thus losing saved data. Therefore, natural disasters are also one of the factors affecting computer network security.

3.2 Human operation error

Human error may also lead to information security problems. Because the computer needs human operation to play its function, once there is an operational error, there may be potential information security risks. Some users cannot protect information security correctly due to their unskilled operation or weak information security awareness. Operations such as setting passwords and transmitting information may lead to data leakage. Therefore, mistakes in human operations may affect computer network security.

3.3 Network openness

The modern Internet has the characteristics of universality and openness. It is inevitable that it will interact with other users and network nodes in the application process, so there are network security risks. Due to the open nature of the Internet, it is difficult for users to be in a closed ecological network, which leads to data information often being in an open state. Once users accidentally expose it or others intentionally use it, network security incidents will occur. Therefore, if the network is used under a lower security protocol, there will be network security risks.

3.4 Hacker attack

Malicious hacker attacks are the most destructive network security problems, which are mainly divided into two situations: the first is that hackers actively take some means of attack to destroy data or steal information, which will damage the confidentiality and integrity of data information. The second is to invade the computer network to intercept information or crack some confidential data, which greatly reduces the security of the entire computer network. In serious cases, it may also lead to paralysis of the entire network, and a large number of users in the network cannot use it normally.

3.5 Spreading of Junk Information and Stealing of User Information

Junk information and spyware are also network security issues. Many people who have no intention transmit junk information through email or SMS, including many commercial, religious, and reactionary illegal information, which will bring trouble to users' normal life, and also represent the destruction of users' personal information security. In general, spyware appears at the same time as spam information, which will steal user information when being used by users, leading to the disclosure of user personal information, affecting the daily life of users, and damaging the stability of the computer network operating environment.

3.6 Computer virus invasion

The progress of computer network technology has also strengthened the concealment and spread of computer viruses. In the age of big data, once computer viruses invade the network system where users live, they will cause great damage. Due to the hidden and destructive characteristics of computer viruses, it is difficult for users to find viruses at the beginning. Once the virus starts to execute, its vulnerability and strong infectivity will cause problems in large network nodes. Traditional computer

ISSN 2616-7433 Vol. 4, Issue 11: 33-37, DOI: 10.25236/FSST.2022.041105

network viruses are mainly spread through optical disks and hard disks. In the age of big data, viruses spread through the network will be stored in the computer once downloaded by users, posing a greater threat to data and spreading faster, which has brought great damage to computer network security [3].

4 Analysis of computer network security protection strategy

4.1 Establish a machine room with complete functions

Hardware equipment is the basis of computer network operation, so to protect computer network security, we must first establish a complete computer room to prevent natural disasters and man-made damage. Nowadays, all major enterprises and units need to work through computers. In this case, a computer room with complete functions and strong protection capability will avoid damage to hardware equipment. When building the computer room, the basic hardware requirements are fire prevention, lightning protection, independent power supply lines, moisture-proof, relative sealing and monitoring. This will reduce the security risks caused by human intrusion or natural disaster damage, and protect the computer network security from the physical level.

4.2 Strengthen the education and training of relevant personnel

The computer can only play its due function and value through human operation, so improving the safety awareness of relevant personnel and educating and training them is an effective way to improve computer network security. If the computer industry practitioners can generally have a strong sense of security protection and security protection capabilities, the stability of the information system and the security of the computer network will be further guaranteed. Therefore, it is necessary to carry out education and training on network security popularization, and require the relevant personnel who use public network systems and master confidential information to operate in strict accordance with the specifications, Avoid information leakage due to human error. In addition, network maintenance and information security protection also need professional network security personnel to implement, so we should build a professional network security team with strong sense of security responsibility, strengthen inspection and prevention, and protect network security.

4.3 Reasonable and effective use of firewall technology

Reasonable use of firewall technology can effectively improve the level of computer network security, reduce hacker attacks and virus intrusion. Nowadays, all major enterprises are generally aware of the importance of information security in network office, and have established a firewall system to protect enterprise information. However, simply establishing a firewall can not guarantee the absolute security of information. If you want to make good use of firewall technology, you need to further standardize the corresponding security protection management system. When enterprises and institutions choose firewalls, they have many options such as address translation type, packet filtering type, proxy type and so on. They should choose firewalls with different technical characteristics according to the network environment and the size of the enterprise. If necessary, they can also establish multi-layer firewalls to prevent illegal intrusion and prevent important information from being damaged or leaked [4].

4.4 Flexible application of anti-virus (Trojan) software

Antivirus software is the most powerful tool to protect personal information. Combined with firewall technology, it can effectively check and kill viruses and trojans, and maintain the stability of the internal security environment of the computer network. After the anti-virus software is installed in the network terminal, the hard disk and system will be comprehensively scanned, and Trojan horses and viruses will be cleaned to prevent people from accidentally downloading or storing some harmful software when using the computer in daily life. It is worth noting that anti-virus software needs to be updated frequently. In the age of big data, the virus iteration speed is very fast. When users use anti-virus software, they should choose software with fast update speed, wide scanning range and strong cleaning ability to protect the network information security in a long term. Antivirus software now has broad development space. If the popularity can be further improved, the network security environment in China will also be improved [5].

ISSN 2616-7433 Vol. 4, Issue 11: 33-37, DOI: 10.25236/FSST.2022.041105

4.5 Setting Network Access Control Points and File Encryption Links

Due to the openness of the Internet, information leakage may occur in the process of data circulation. To ensure that data will not be damaged or stolen, network access control points and encrypted files can be set to improve the computer network security level. By encrypting files, users can improve the security of computer local information. If network access nodes are set up, network access control is strengthened, and passwords and other encryption methods are used to enhance protection when information is called, illegal thieves will spend more time stealing files, and firewalls can respond and protect in a timely manner, improving the security level of computer networks.

4.6 Establish a complete computer network management system

For computer users in enterprises and institutions, a complete set of computer network security system will greatly improve the level of computer network security. In the era of big data, people can't work without the network and information data, so we should integrate the network security management system into the daily management system to ensure the computer network security at all times. First of all, it is necessary to establish an enterprise computer management platform, record and manage daily operations to avoid potential safety hazards caused by operational errors. At the same time, it is also necessary to strengthen the training of relevant workers, establish the concept of information security, so that employees can understand the basic knowledge of computer security, and skillfully use information security protection software. In addition, enterprises can also control the internal information access of computers through big data technology, and ensure that the access times are controlled and the sources are traceable through digital authentication channels, so as to further improve the stability of the internal network operation and avoid the network information security problems brought to enterprises by illegal intrusion.

4.7 Identity authentication

The establishment of an identity authentication system for authorization management and access control through strict identity authentication will greatly improve the level of computer network security. Individual or enterprise users can prevent others from entering their own network system under unknown circumstances by strengthening their identity authentication. When conducting identity authentication, they should choose an authentication method with strong security protection ability. In addition to common passwords, passwords, dynamic authentication, etc., there are now more secure biometric authentication, such as voice, face recognition, fingerprints, etc, Verify user information to play the role of security protection. In terms of security, users can also use multiple identity authentication. For example, the mobile SMS dynamic verification code plus password can greatly enhance the level of information security. In addition, the transmission and storage of verification data should also be emphasized, and HTTPS must be used SSH and other encryption protocols for transmission. Try to use different passwords to log in to different websites and software. When using biometrics and other methods for verification, you can use symmetric encryption algorithms to store information and carry time stamps for verification to avoid information leakage or theft[6].

5. Conclusion

While big data technology provides convenience for people's life and work, it also brings hidden dangers in data and information security. Therefore, it is necessary to improve the security level of computer networks to avoid data destruction and information leakage from causing problems to computer users. To improve the computer network security level, individual users and professionals need to work together. On the one hand, they need to improve their information security awareness in the daily use process to avoid data information leakage due to operational errors. On the other hand, they need to improve the work quality of professionals, develop and update anti-virus software and firewalls that keep pace with the times, and strengthen the protection of websites, systems and software during operation, Provide better security protection services. In the context of the vigorous development of computer network technology, only by always paying attention to network security issues and constantly improving the level of information security protection, can we reduce security risks and make greater contributions to the society by information technology.

ISSN 2616-7433 Vol. 4, Issue 11: 33-37, DOI: 10.25236/FSST.2022.041105

References

[1] Fadhil Saif Aamer, Kadhim Lubna Emad, Abdurazaq Sayl Gani. Protection measurements of computer network information security for big data[J]. Journal of Discrete Mathematical Sciences and Cryptography, 2021, 24(7) : 1959-1965. DOI: 10.1080/09720529.2021.1959996

[2] Wang Qi, Li Ling, Hu Shuai. Computer Network Information Security Protection Faced by Digital Art Museums Based on the Internet of Things[J]. Wireless Communications and Mobile Computing, 2021, 2021. DOI: 10.1155/2021/2297733

[3] Wang Fang. Research on Computer Network Information Security and Protection Strategy in the Age of Big Data [J]. Computer Fan, 2018 (05): 66

[4] Wang Dongfang, Ju Jie. Research on Computer Network Information Security and Protection Strategy in the Age of Big Data [J]. Wireless Internet Technology, 2015, No.76 (24): 40-41

[5] Chen Huanfei. Thinking about the security and protection strategy of computer network information in the age of big data [J]. Electronic Paradise, 2018 (10): 0345

[6] Yang Yuan. Problems and Protection Measures of Computer Network Information Security in the Era of Big Data[J]. OA Journal of Computer Networking, 2022, 1(2)