Research on Computer Network Security Prevention in the Big Data Era

Caili Liu

Xi'An International University, Institute Of Technology, Xi 'An, Shaanxi, 710077, China

Keywords: Big data, Computer network security, Data

Abstract: In the context of the popularization and development of computer networks, although big data technology has been widely used in many industries and can provide important help for people's lives and production, it is also restricted by various computer network security risks. How to effectively eliminate or prevent these hidden computer network security hazards has naturally become an important issue of concern to all sectors of society. Based on this, this article analyzes the common hidden dangers of computer network security in the current era, and puts forward some feasible computer network security prevention strategies, hoping to provide a certain reference for the protection of the privacy of computer network users.

1. Introduction

With the advent of the era of big data, the value of all kinds of data information has become higher and higher, whether it is data information generated in the production activities of various industries, or all kinds of data information that are closely related to people's daily life. Both can become a vital strategic resource, playing an important role in marketing, scientific research, research and development of machinery and equipment, urban construction, and financial transactions. However, it should be noted that because data information has a high value, the computer network security risks it faces are also very large. Once the data information is lost due to network security issues, the consequences are often more serious. In the era of big data, it is naturally necessary to strengthen computer network security.

2. Hidden Dangers of Computer Network Security in the Era of Big Data

2.1 Computer Virus

In the era of big data, because all kinds of information and data basically need to be managed by computers, and computers, as electronic products, have outstanding fragility characteristics. It is basically impossible to know in advance whether there are errors in their operating procedures, so people use When a computer performs data input, storage, processing, and output operations, it is often easy to cause various computer viruses to invade it, and cause the computer function or the data stored in it to be destroyed, and sometimes data is maliciously tampered with. From the perspective of transmission methods, computer viruses can usually be divided into two categories: resident viruses and non-resident viruses. Resident viruses refer to directly storing the resident part of the memory in the computer RAM after invading the computer. After that, the on-hook system is called and merged into the operating system until the computer shuts down. Non-resident viruses will not reside in the computer's memory, but will run automatically and destroy computer functions and computer internal data [1]. Of course, although computer viruses are very common, they are only a set of codes or computer instructions, and their types are very diverse. Therefore, the effects of different types of computer viruses are often very different. For example, after some harmless viruses invade the computer, they will only occupy disk space to a certain extent, and basically have no other negative effects; while some computer viruses are extremely dangerous. After invading the computer, they often directly delete programs and destroy Data, clear the memory area, and even exceed its own algorithm, causing all kinds of unforeseen catastrophic damage.

2.2 Hacking

  DOI: 10.25236/icited.2021.079

Hackers, as a group of people who are proficient in various programming languages, familiar with various operating systems, and master IT technologies, often launch cyber attacks on other users' computer systems for various reasons. Because of their extremely complex attack objectives, Under the influence of network concealment, the cost of network attacks is very low. Therefore, with the popularization of the Internet and computers, hacker attacks have gradually become one of the most common computer network security risks. At the same time, in the face of diversified hacker attacks, it is also difficult to effectively prevent such computer network security risks. For example, some hackers will use special software to continuously send massive amounts of information to the target server, causing the information to exceed the upper limit of the system's information processing capacity, thereby achieving the purpose of network attacks such as system crashes and network congestion. Some hackers use special network monitoring tools to obtain real-time information about the computer's data flow and network status, and then intercept the transmitted data.

2.3 System Vulnerabilities

The various functions of the computer and software must be realized by the operating system, such as memory management, peripheral management, switch machine, etc., all need to be run in accordance with the relevant programs of the operating system, and the operating system has various vulnerabilities in programming , It is one of the most important computer network security risks. Generally speaking, in the face of various network security issues, when programmers design computer or software operating system programs, they basically pay attention to patching system vulnerabilities. However, because the programming of operating systems is very complicated, programmers Under the restriction of ability, security technology level and other factors, it is difficult to completely avoid system vulnerabilities. Therefore, once the system vulnerabilities are discovered by hackers, they may use these vulnerabilities to illegally access the computer operating system and conduct various networks without authorization. Attacks, and expose the data and information in the computer to many security threats such as leakage, loss, and malicious modification [2]. In addition, the vulnerabilities of the computer operating system are not entirely caused by design problems. If the computer itself has hardware vulnerabilities, no matter what program the programmer designs, the hardware problems can easily be manifested by various software installed in the computer. This will also bring security threats to the data and information in the computer.

2.4 Improper Network Management

In addition to network security risks such as hacker attacks, computer viruses, etc., such as computer network users failing to implement network security management in place, human error in daily work, damage to hardware facilities, etc., will also bring huge problems. Computer network security risks. For example, in the daily management of computer hardware equipment, some users often ignore the impact of external environmental factors on the operation of hardware equipment, fail to strictly control the computer operating environment, and prevent fire, earthquake, lightning and other accidents. , Once the computer has problems such as damage to electronic components and burned circuits, it may cause the computer to stop running, and the data information stored in the computer may also face the risk of loss. When some users use the internal network, they often face computer network security problems such as the disclosure of login passwords and the failure to clear network files in time.

3. Effective Strategies for Computer Network Security in the Era of Big Data

3.1 Improve Virus Detection and Killing Capabilities

In order to achieve effective prevention of computer network security risks, firstly, effective preventive measures must be taken to avoid the intrusion of computer viruses, and at the same time, to improve the virus detection and killing capabilities of computers, and to comprehensively find

and remove hidden viruses in computers. Generally speaking, the prevention of computer viruses should be achieved by installing various anti-virus software, and at the same time regularly updating the anti-virus software, so that when the computer is running, once a virus may invade the computer, the anti-virus software will quickly It is detected and intercepted, and when a computer virus cannot invade the computer, it naturally cannot affect the computer operating system and the data information stored by the user. At the same time, in order to avoid the omission of anti-virus software in virus interception, a full-scale virus Trojan scan must be performed regularly to screen out and remove abnormal files. If various browsers are frequently used, special security monitoring software must be installed. In order to achieve effective prevention of abnormal browser modification behaviors, so as to avoid accidental installation of malicious plug-ins during the use of the browser [3]. In addition, if the computer has invaded the virus, you can use the self-starting principle (divided into direct self-starting and indirect self-starting), open the computer to delete the virus startup item in the registry file, and then restart the computer immediately. To prevent the virus from writing back to the registry, or use batch processing and other programs to close the virus service. Of course, this type of operation requires the user to have a certain level of technology. If you cannot organize the virus to start automatically through this method, you can also choose to redo the system (important files should be backed up in advance).

3.2 Application of Security Technology

In response to various network attack methods adopted by hackers, computer network users also need to flexibly apply network security prevention technologies according to actual conditions to effectively resist hacker network attacks. For example, when important data information needs to be stored in the computer, data backup technology can be applied to realize automatic backup of important data information through related backup software. Specific backup methods include remote mirror backup, database backup, regular tape backup, and cloud backup. Wait. For the leakage of data and information in the process of transmission, data encryption technology can be used to encrypt the data to be transmitted, so that it can become meaningless ciphertext after the encryption function is converted. The receiver uses the decryption function to decrypt the data to restore the data information to meaningful plaintext.

3.3 Fix System Vulnerabilities in Time

In order to reduce the hidden dangers of system vulnerabilities, system developers usually carry out continuous screening of system vulnerabilities and fix system vulnerabilities by regularly updating patches. For computer network users, if the developers fail to discover or System vulnerabilities that have not been discovered in time are patched to prevent the vulnerabilities from being exploited by criminals. It is necessary to install various security vulnerabilities checking tools to comprehensively detect high-risk vulnerabilities in the system and realize one-click repair of system vulnerabilities that have been discovered. In addition, because system vulnerabilities can be divided into many types, specific preventive measures must be taken for different types of system vulnerabilities. For example, after the computer operating system is upgraded, web pages and HTML mail scripts may automatically call the operating system programs and affect the browser defect recognition function of the system upgrade server. Once the IE browser defect is not discovered in time, And hackers who have mastered these IE browser vulnerabilities can take this to peek at computer files and bring data leakage risks to users. For this kind of system vulnerabilities, users also need to download the IE browser patch on the official website regularly, and update the IE browser to the latest patch version [4]. For Windows Media Player vulnerabilities that may cause user data leakage, script calls, etc., you need to use the vulnerability to not affect the characteristics of local media files. When you need to play a file, first download the file you want to play to the local, and then Play it to prevent hackers from launching network attacks. If a user finds that a webpage pops up on the computer operation interface after playing a special media file, the webpage needs to be closed to prevent hackers from calling programs according to fixed scripts to carry out network attacks.

3.4 Strengthen Network Security Management

For computer network users, in order to achieve effective prevention of computer network security risks by strengthening network security management, they must first establish a sound emergency management mechanism based on the sudden characteristics of network security accidents, and integrate various types of network The emergency plan for security incidents has been clarified so as to make timely and correct responses to problems such as hardware equipment damage, hacker attacks, etc., to minimize the impact of network security incidents. For example, after the computer hardware electronic components are burned, the relevant power supply should be cut off in time, and only then the specific fault conditions should be investigated, and professionals should be arranged for fault diagnosis and maintenance, and other hardware devices can be started after the failure safety hazard is determined to avoid other computers. The hardware device burned again [5]. At the same time, computer network users must also strengthen network security training for relevant staff to enhance their awareness of network security, and at the same time help them with basic computer network security precautions to reduce network security problems caused by human error.

4. Conclusion

All in all, although the popularization and application of big data technology has brought many network security risks to computer network users, as long as you are familiar with the characteristics of various network security risks such as hacker attacks, computer viruses, system vulnerabilities, and poor network management, at the same time Taking effective countermeasures in the application of network security prevention technology, system vulnerability analysis and repair, virus detection and killing, and strengthening of network security management will inevitably achieve good computer network security prevention effects.

5. Acknowledgment

Shaanxi Province Educational Science “13th Five-Year Plan” Project: Research on the effectiveness of excellent traditional culture teaching in private colleges and universities guided by cultural education. Item Number: SGH20Y1419

References

[1] Yang Zhaofeng, Fan Aiwan, Peng Tongqian. Research on the idea of building a computer network security system based on the big data environment. Information Technology and Informatization, 2019, (11): 148-150.

[2] Zumulaiti·Ekramu, Ekbeir Muhtar. Research on the Application of Data Encryption Technology in Computer Network Security. Grand View Weekly, 2020, (7): 102-103.

[3] Fu Meiling. Application analysis of data encryption technology in computer network security maintenance. Digital Communication World, 2019, (2): 180, 211.

[4] Xu Gang, Wang Weijia, Deng Ying. Analysis of the data network security guarantee strategy of the information resource platform under the big data environment. Digital User, 2019, 25(29): 60.

[5] Zhang Lingling. Application and research of big data in network security defense. Information System Engineering, 2019, (8): 87-88.