Analysis of Computer Network Information Security and Protection Strategy

Xiaobo Ming[a], Ying Chen, Jinhua Guo

Shangrao Vocational and Technical College, Jiangxi, Shangrao, 334001

Abstract. Computers are closely related to our life and work. We have entered an era in which computers are not available in all walks of life. Among them, many important documents and materials will be stored in the form of electronic files in the computer. However, computers are not absolutely safe, and cases of information theft occur from time to time. Most people usually keep information confidential in the form of encryption. How to avoid the problem of computer information security. Computer network security involves all aspects. To solve these problems, there are many levels of technology, such as cryptography technology, network security technology and so on. Our country has also done a lot of research on the security protection of computer network technology, and these research results have also achieved certain results in the actual construction of computer network. In order to ensure the normal operation of computer networks, ensure information security and prevent information leakage and theft, a special protection system has been established to ensure the security of computer network information by setting up computer detection, security assessment and other links. However, with the rapid development of science and technology, the updating of electronic products is faster and faster, and the challenge of Wechat for network security information is more severe. How to protect computer network information security needs to be solved urgently, this paper discusses this.

Keywords: Computer network information; Information security; Security protection.

The storage of massive data also brings certain challenges to computer technology. Many information security technologies and tools need to be solved urgently. Traditional information technology has been unable to meet the storage needs of massive data. At present, the most prominent and serious problems of computer information security in the era of big data are data theft, data improper addition and deletion and tampering, personal privacy disclosure and so on.

The protection of computer network information security also needs a certain system to protect, but also users themselves take reasonable protective measures and so on. The process of computer information security protection needs all kinds of strategies to be used together and deployed reasonably. Only in this way can we minimize the probability of infringement of information security and get security assurance.

1 Computer network information security

1.1 Virus attack problem

Many users do not have a good sense of safe operation in the process of using computer networks. For example, they can easily guess or crack account passwords by others, and then make their accounts stolen by setting up some important accounts in a simple and random way. In addition, other computer users' attacking behavior will also lead to computer network information security problems. This kind of attacking behavior includes not only other people's use of substantive network attacking behavior to destroy the integrity and security of computer network information, but also the user's own initiative to be attacked. For the sake of this, active attack means that there are some viruses in many computer networks in our country at present. Network viruses have strong latent and infectious characteristics. When users click on network links with viruses or use computer networks with viruses to edit relevant programs, they will rush out. Large viruses invade or cause viruses to hide in the execution program, which not only reduces the efficiency of the system, but also duplicates the relevant information in the computer system or deletes the important files in the system, thus bringing certain losses to the computer network users [1]. The following is an example of Alipay, which briefly describes the virus attack of computer network information security. Alipay is an online cash transaction means, and it is also the most commonly used

[a]Corresponding author: 44954510@qq.com

independent third party payment platform for modern people. Most of the users' mobile phones are equipped with Alipay software. The registered Fu Baoxu provides the user's name and identity card number. The code, collection numbers, payment passwords and many other information, arguably its network security is relatively high. However, with the continuous development of modern network attack technology, some criminals use Alipay to find loopholes in the password function, and can find out the relevant identity information of users who leak the Alipay password before. By retrieving the password function, you can get access to Alipay's users, thus transferring the money in Alipay.

1.2 Mail attack problem

E-mail has the characteristics of easy dissemination and open account. With this feature, many lawless elements can send their own e-mail with various computer viruses to others by force through other people's e-mail account, which can directly destroy the information security of the computer system of the emailed users. Information security that borrows e-mail accounts has a negative impact.

1.3 Open computer network and free download of application software

The computer network has the characteristics of openness in the process of operation. It is precisely because of its openness that the computer network is vulnerable to some extent. In the computer network, there are not too many restrictions on the dissemination, transmission and sharing of information. The computer network is also in an open and unprotected state, which makes it easy for some illegal elements to take advantage of the openness of the network to commit illegal acts [2].

In order to popularize computer network technology, the modern network application market has launched a large number of life apps, game software and so on. The functions of these software often need to be downloaded before they can experience. In order to satisfy their curiosity, many users will download all kinds of apps at will, such as many users will download security at will. Unknown applications or pornographic video websites can destroy the security of their mobile phones or computer network systems. Although most computer network systems are equipped with tools and software to improve the quality of service and system management, there are still many illegal elements who can use these tools to collect illegal information and attack user information.

1.4 Hacker intrusion

Hacking is one of the important factors of computer network security problems. Hacker intrusion is generally an artificial security problem. Hackers invade users' computers by means of relevant means and technologies, and then attack and destroy information and data in computers, thus causing data damage and omission. This kind of man-made data destruction, attacks and so on are likely to cause the paralysis of the computer network system, and then cause tremendous losses and impact on people's production, work and life [3].

2 Computer network information security protection strategy

2.1 Strengthen account management

There are many kinds of account types in computer network. When security problems or deviations occur in network system, illegal elements often steal user's account information and password. Therefore, network users are required to increase the close complexity when setting account password, such as combining numbers, letters or other symbols to account password. Setting up, rather than using simple numbers or letters as passwords, can make its network close and not easy to be guessed or stolen by others, and try not to use the same password to set different accounts, which will lead to its multiple account passwords are easy to steal. In addition, in the process of network account registration and password login, the account information also needs to be strictly and carefully protected [4].

At present, firewall software is installed in most computer networks in our country. It can scan the network access resources within the computer system, find and deal with the hidden security problems in the system, and effectively supervise and control the access between various networks, so as to avoid the user computer system being used by other networks. Information technology attacks, such as when users use computer networks to browse relevant web pages and process some network data, can adopt relevant security strategies to protect their own information security. When the network is running, the firewall can also monitor the network information closely and automatically refuse to accept the data information with risk. Firewalls generally use the IP address of network users to find dangerous data information. Their control function can convert the IP address of users. This can ensure that they can hide accurate and real IP addresses when controlling the internal network, thus making it difficult for the external attack network to enter the internal database for destruction. When users access computer network information by themselves, they can not only intercept most virus intrusions and control many applications, but also upgrade the version of firewall in time, so that their virus prevention work is more efficient.

2.2 Strengthen the effective utilization of protective wall

Protective wall technology is an effective way to ensure the information security of computer network. Therefore, in the era of big data, the effective use of protective wall or security system should be strengthened for the operation of computer network. For example, in the enterprise computer application, the information involved

is not only large but also very important. For this reason, the enterprise should establish a perfect data information security prevention system, in order to fundamentally improve the management personnel's computer network security awareness [5]. Especially in the context of big data era, in order to effectively avoid the impact and destruction of virus and hacker intrusion on the safe operation of computer networks, it is necessary to strengthen the use of firewall technology to interfere with malignant software. Protective wall technology has an effective role in isolating viruses, and the use of topological structure can effectively improve the security and reliability of computer network operation. In addition, we need to strengthen the use of protective wall technology for regular maintenance and repair of data information, which can also greatly inhibit the invasion of viruses. Nowadays, with the continuous development of computer technology, the characteristics and styles of viruses are becoming more and more diverse, which requires relevant Internet technical managers to have a full understanding and mastery of the characteristics and performance of viruses, and to take effective preventive measures against the actual situation of viruses.

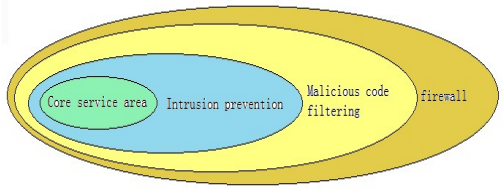

Figure 1. Firewall Network Security Protection.

2.3 Strengthen the application of antivirus software and mail recognition system

With the frequent occurrence of computer network information security problems, now more and more anti-virus software has been applied to computer operation, which plays an important role in ensuring the security of computer network operation, preventing viruses, spam messages and so on. Therefore, in the era of big data, we should strengthen the effective application of anti-virus software and email identification system. Anti-virus software can be combined with firewall technology. Anti-virus software can effectively identify viruses and malignant software intercepted by firewall, and then carry out effective anti-virus, so that the latent virus in the computer can be detected and killed. Mail identification system is mainly a security system for spam. Nowadays, many viruses and malicious software will enter the computer through mail. Mail identification system will identify the mail. If there is sensitive information in the process of mail identification, the system will automatically clear it. The application of anti-virus software and part identification system can effectively ensure the stability and security of the system [5].

2.4 Digital signature and file encryption

Digital signature is a digital information authentication method based on public key encryption technology. It can effectively guarantee the security of network information and e-mail. If there is no user key, it can not read the information. In addition, it can identify and verify electronic documents, thus effectively safeguarding the privacy and integrity of e-mail. File encryption refers to encrypting network information and data in order to prevent them from being stolen, so as to promote the improvement of confidentiality. At present, the commonly used computer network file encryption technology has two kinds of file encryption function and commercial encryption software. The commercial encryption software is mainly realized by encryption algorithm. For example, the master of encryption software is one of the most commonly used folder encryption software. Because, after the file encryption is completed, only the user can log in to the account to open the file, otherwise the re-installation system can not open the encrypted account and the established account name. In order to avoid the above problems, it is necessary to use the file encryption function carefully. Generally speaking, only the files involving confidentiality and very important are involved. When encrypting files, it's better to backup and store them elsewhere.

3 Concluding remarks

Research on how to better protect the security of computer networks plays an important role in protecting the information security and interests of network users. Because computer network information will be attacked by viruses, email attacks, open network and arbitrary download of application software, hacker intrusion and other issues in the course of operation, in order to protect network information. Security needs to strengthen the application of account management, protection wall, anti-virus software, email identification system and digital signature and document encryption.

References

1. Yang Junsheng. Application of Virus Protection Technology in Computer Network Security in Big Data Environment [J]. Computer Fan, 2018 (11): 77-78.
2. Dong Chengwu. Brief discussion on campus information network security protection and management in Higher Vocational Colleges [J]. Information recording materials, 2018, 19(11): 141-142.
3. Chen Liangliang. Analysis of the main hidden dangers and management measures of computer network security [J]. Network security technology and application, 2018 (10): 6 + 64.
4. Qiu Shichen. Preliminary study on computer network information security and protection [J]. Information Communication, 2018 (10): 137-138.
5. Liu Zhipeng. Analysis of network security issues under the Internet + new mode [J]. Computer knowledge and technology, 2018, 14 (28): 21-22.