The Safety and Preventive Measures Analysis of Computer Network Information Technology

Bo Zhao[1], Congling Huang[2]

[1]Shaanxi Costume Engineering University, Xixian, Shaanxi, China

[2]Yangling Vocational & Technical College, Yangling, Shaanxi, China

Keywords: Computer, Network information technology, Security, Prevention.

Abstract: Strengthening the security of computer network information technology has an extremely important impact on people's lives and work as well as the continuous development of society. In this paper, the computer network information security is briefly introduced, and the main security problems of current computer network information technology are pointed out in detail. Then, through summarization and analysis, the corresponding solutions are proposed and provided to improve the effective reference basis for the security of computer network technology.

1. Introduction

In the 21st century, human beings have entered the information age, and computer network technology and information technology have also achieved extremely rapid development and have begun to be widely used in various fields. With the continuous development and popularization of computer network information technology, computer network information technology has become more and more important. Whether it is people's life or work, computer network information technology is inseparable. However, although the application of computer network information technology has brought great convenience to people's life and work, it has also brought some troubles to people. Among them, the most representative one is the security problem of computer network, which is not only affecting the safety of people surfing the Internet, it also seriously threatens people's interests. Therefore, in order to effectively solve the problem of computer network security, relevant researchers have been working hard and have made great progress. Next, this paper will explore and analyze the security of computer network information technology, and propose corresponding solutions to provide a reference experience for further improving the security of computer network information technology [1].

2. Information security Computer network

Computer network information security refers to the integrity and security of various information, data, data, and equipment facilities in a network environment. At present, computer network information security in a broad sense mainly refers to two aspects, one is the security of the logical layer of the computer network, and the other is the security of the physical layer of the computer network. In these two aspects, the logic layer is mainly aimed at the integrity and security of network information, data and data, to avoid the occurrence of information, data and data loss, corruption and theft of network security issues. It is aimed at whether the equipment or facilities of the computer network information system are complete and safe whether it causes infringement or destruction, and affects its own normal operation.

In the security management of computer network information, only to ensure that system equipment and facilities will not be damaged, information, data and data will not be missing or stolen, etc., can effectively ensure the safe and reliable operation of the entire computer network information system. In order to ensure that various network services will not be interrupted. In general, ensuring the security of computer network information is to ensure the security of various network services. Therefore, ensuring the security of computer network information has an extremely important impact

DOI: 10.25236/eeems.2018.046

on ensuring the security of the entire network environment [1].

At present, computer network information security mainly includes the following four characteristics: The first type enables usability, mainly refers to the fact that users on the network can physically access network information through the Internet, and also can implement network information according to the specific needs of users. The second type of integrity mainly includes two aspects. On the one hand, without authorization, the user cannot modify or increase or decrease the network information to ensure the integrity of the network information. On the other hand, for the information accessed by the user, without the authorization of the user, other users cannot modify and increase the information accessed by the user to ensure the integrity of the user information; the third is confidentiality, which is also a computer network. The most important item in information security whether it is network information or user information, without the authorization of the sovereign, and the unauthorized users cannot access the read information, and cannot modify, increase or decrease the information to ensure the information [2]. Confidentiality; the fourth is controllability, computer networks need to use network information and Information control, to manage all the authorization information against illegal access and read for information, against hacker attacks, prevent the spread of illegal information on a computer network, control the legality of network information and user information. The above four points are the basic characteristics of computer network information security. Only when these characteristics are available and the computer network information can be better secured.

3. Security threats to computer network information technology

3.1 Computer virus.

Computer virus is the primary factor affecting the security of network information, and it is the most widely affected factor. It has the characteristics of fast propagation speed and great harm. Because of the openness of the network, the virus has obtained a fast intrusion channel, invaded into the user's computer system through various forms, tampering or deleting the user's information, and the computer virus has strong replication capability [2]. The user's computer system can be paralyzed in just a few seconds.

3.2 Hacking.

How intrusion is a kind of behavior that uses intrusion technology to enter the user's computer and steal user information. The object of hacking is usually an organization such as a company or a bank, which steals information and obtains illegal interests. The hacking methods generally have the methods of releasing Trojans and monitoring user information dissemination, which will not only cause the loss of social organization information, but if it invades the government computer, it will lead to more serious information security threats [2].

3.3 Loss of information caused by human factors.

The maintenance of network information security requires managers to strengthen their awareness of security protection. However, many users or administrators lack the awareness of network information security protection, and negligence of security vulnerabilities in computers [2]. In general, there is no anti-virus software installed on the computer, and the necessary protection and backup for important information, resulting in loss or tampering of information data, are caused by human factors.

4. The main problem of current computer network information technology security

4.1 There are loopholes in the operating system.

The computer operating system is the basis for ensuring the transmission of computer information and functions. It is also one of the most important components of a computer. It is the core of the overall structure of a computer and has a direct impact on the security of computer network information. China has continuously improved its system development, fixed many loopholes in the system, and improved the security of network information to a certain extent. At this stage, China's main application computer systems are win7, win8, win10 systems, and there are still some loopholes in the development, but there is a certain guarantee in information security. Many small and medium-sized enterprises and home users in China will choose to apply the flagship version and pirate system to install it on the computer, which will bring certain security risks. There are obvious loopholes in the programs written in the pirate system. Compared with the genuine operating system, the number of vulnerabilities will increase geometrically, which greatly reduces the system's resistance to viruses and makes the overall network operation have high security risks [3].

4.2 The core technology is relatively scarce.

The lack of core technology for computer network information security causes computer network systems to suffer from virus intrusion, resulting in information leakage and data corruption. This is caused by insufficient core technology. Network viruses have the characteristics of fast propagation and strong aggression, which will seriously damage computer systems and network information terminals. China has obvious deficiencies in technology development, which provides a viable opportunity for virus intrusion, mainly reflected in the following aspects. First, the computer system programming technology is insufficient. Second, the computer system security protection technology is insufficient. The system vulnerability will reduce the virus defense capability [3]. This is a manifestation of the lack of system development technology. In the development of security protection technology, the type of virus recognized by the protection software is limited. Many Trojan viruses are not recognized or even protected. When the virus and the protection software do not respond, the virus has been tampered with and stolen, resulting in serious security risks.

4.3 Safety awareness is generally insufficient.

When using computers, many users have insufficient awareness of security precautions. They do not take corresponding virus prevention measures when applying computers, and do not scientifically save information data, even transmission errors, accidental deletions, etc. during operation. The situation, the information cannot be retrieved. The lack of user security awareness is mainly reflected in the following aspects. First, the user does not install protection software on the computer, which causes the system protection function to decline and is vulnerable to viruses. Secondly, the user does not regularly perform anti-virus maintenance when applying the computer, which causes a large number of security risks in the system, and even there are cases where the killing software cannot identify the file. Finally, when users use the computer, they often have pop-ups, advertisements, etc. The user clicks on them for curiosity, and the website information pushed by other people is clicked without thinking [4].

4.4 The prevention mechanism is not perfect.

The inadequate prevention mechanism is one of the important reasons for the computer information security problem. Many computers in the security precautions only download a security guard, Tencent butler and other protection software to protect the user's operational behavior, and the prevention mechanism is not comprehensive enough [4]. In the protection mechanism, there is a lack of protection for terminal information, transmission information, and storage information. There are many virus intrusion channels. Imperfect prevention mechanisms will increase the possibility of viruses such as intrusion.

4.5 Manufactured damage is more frequent.

Manufactured information destruction is highly targeted, aggressive, and destructive. Hacking is a kind of espionage. Hackers refer to people with strong computer technology. They can access other users' computer systems, databases, and terminals through technology to steal the other party's data and destroy the other system. Although China has increased the intensity of hacking and strictly investigated illegal activities, many hackers still invade the computer systems of major enterprises and major institutions by means of password intrusion and Trojan horse invasion. Frequent hacking has brought huge impact on computer network security. What is familiar to everyone is the bitcoin virus incident that occurred in 2015, which has caused serious impact on major institutions, enterprises and schools. High frequency of human destruction is one of the important factors leading to computer network security problems [5].

4.6 Hardware lacks effective management.

Hardware management is the prerequisite for ensuring the safe and orderly use of computers. Many computer users in China lack the management of hardware, and often there are hard disk burnouts, system crashes, etc., resulting in information corruption or loss, resulting in certain security risks. Hardware management refers to the maintenance and maintenance of daily equipment. The hardware acts as a carrier for computer network operation and information storage [5]. Once the hardware fails, network information transmission will fail, and even information loss will occur. Lack of effective management of hardware can lead to confusion in the transmission and storage of information data, and even lead to disk burnout, affecting the normal use of computer network systems.

5. Effective countermeasures to solve the security problem of computer network information technology

5.1 Application of Security Protocols.

Security protocols are the basis for ensuring the security of computer network information. Establish a security protocol in a computer application, and after signing a security protocol, implement scientific protection against network information security. The security protocol is mainly composed of passwords, including cryptography knowledge, and is based on the message exchange protocol. It is an important part of network information security. In the application process, the security protocol can realize scientific authentication between multiple entities, perform security key distribution on the authentication entity, authenticate the operation, such as information confirmation, transmission, and reception of the computer user, and identify whether it has security risks. In the application of security protocols, scientific selection types are required to ensure the integrity and standardization of security protocol applications. Security protocols can be divided into key management protocols, security audit protocols, data information encryption protocols, security protection protocols, and data authentication protocols [6].

5.2 Application of firewall technology.

Firewall technology has software functions and hardware functions. The firewall technology is mainly used in the security information protection of local area networks, and can be applied to individual users. It sets up a gateway for the computer operating system during the application process. When the user extracts information from the network and downloads the application, the firewall will identify it and provide operational suggestions for the user. When a hacker invades, copies, or deletes computer network information, the firewall also issues a warning and organizes the corresponding operations. The firewall is mainly composed of four parts: service access policy, verification tool, gateway defense, and information filtering. The main function of the firewall is to prevent external information supply, prevent the transmission of virus files, and prompt and block the aggressive information transmission operation [6].

5.3 Application of data encryption technology.

Data encryption technology refers to the encryption processing of the network, which is converted into cipher text by means of secret key, function conversion and encryption, etc. In the process of information loading, extraction and access, all need to pass the cipher text. Unlock and restore the key to plain text. In the application of data encryption technology, only certain people, designated users, and specific network environments can operate on data. Many keys are randomly selected [7]. When the terminal transmission is about to end, the data information is decrypted, which has strong information security protection.

5.4 Promote the research of core technologies.

In the core technology research, mainly based on information encryption technology and security protection technology. In addition to increasing capital investment, special scientific research studios should be set up to improve the comprehensive and scientific nature of computer network security protection, and to provide targeted computer core information security to provide computer information security. There are two main research directions: First, the complexity of the algorithm for improving the calculation of passwords in computer information, and advanced encryption of information [4]. In China's security protection cryptographic algorithm, AES algorithm and RSA algorithm are the main ones, and relevant departments need to strengthen the algorithm. Research and build a network information security protection model.

5.5 Strengthen computer network information security management.

From the perspective of security management, relevant departments need to develop a scientific management system and formulate scientific management norms. Relevant departments should strengthen information law management, formulate relevant laws and regulations, and strengthen the important significance of legal management. In the management, we will standardize the responsibilities of various departments, strengthen the internal control of large-scale local area networks, and do a good job in relevant management [7]. In the enterprise network information security management, enterprises need to establish a computer network system application management team to repair, manage and coordinate the network system, strengthen daily inspection and supervision, establish a job responsibility system, clarify the responsibility of each department, and solve information security problems. Implemented on the individual.

5.6 Pay attention to the management of computer hardware facilities.

The management of computer hardware facilities is also the basis for ensuring the security of network information. As the basis of network information dissemination, users should maintain it regularly, clean up the computer disk, and ensure the clean and tidy information storage location [5]. In daily maintenance, maintenance of the host, peripherals, UPS and other equipment, in the process of information transmission, it is strictly forbidden to appear chaotic, unplugged, etc.

6. Summary

Overall, the issue of network information security has become a common problem, and it has also received great attention from relevant departments. In the prevention of security issues, in addition to taking relevant measures, it is also necessary to improve the security awareness of computer application populations and avoid the lack of security awareness. In the phishing website, the information data is lost, leaked, damaged, etc., causing many losses for the user. With the continuous improvement of technology, China's computer information security issues will be fully resolved, providing users with a harmonious and friendly network information environment.

References

[1] N.H. Wang, Problems and Countermeasures in China's Computer Network and Information Security, Science and Technology Information, 2010, pp.5-7.

[2] C.L. Miao, on computer network security and related security measures, computer CD software and applications, 2011, pp.13-15.

[3] Ch.Q. Du, Computer Network Information Technology Security and Preventive Countermeasures Research, Technical Discussion, 2011, pp. 9-11.

[4] X.J. Peng, Computer Network Common Attack Methods and Countermeasures, Priority Publishing, Electronic Technology and Software Engineering, 2012, vol.11, pp.77-81.

[5] L.P. Ge, Liu Yan, Research on Security Risks and Security Strategies of Postal Savings Computer

Network, Computer CD Software and Applications, 2014, vol.20, pp.99-101.

[6] Y.P. He, W.T. Wang, Computer Network Information Security and Protection Technology Research, Electronic Technology and Software Engineering, 2014, vol.3, pp.22-23.

[7] Zh.D. Zhang and L.N. Hu, Application of Computer Information Management in Network Security, SME Management and Technology (early issue), 2012, vol.13, pp.88-90.