Research on Network Security Precaution in Computer Application

Li Ping

Manzhouli Branch of Inner Mongolia University, Inner Mongolia, Manzhouli, 021400

Keywords: computer; network security; prevention

Abstract: The progress of science and technology promotes the development of computer and network technology, not only as a basic tool in people's work and life, bringing a different experience, data privacy issues and computer application, but also posing a great threat to people's property security. Computer viruses, hackers and so on are the main factors that influence the weakness and vulnerability of network environment. Therefore, it is necessary to take diversified and systematic network security protection measures to ensure that the safety experience in computer application.

The lack of secure network platform in computer applications directly affects the effect of application experience. Although network security problems in application often occur, and users also have the awareness of network security, network security issues such as makers of attack technology is also increasing, so the network security protection must be comprehensive, rigorous, in strict accordance with the construction, update the virus database firewall and other network security essentials to expand prevention, to ensure the normal operation of computer hardware and software.

1. The Present Situation of Network Security Prevention in Computer Application

At present, the operation environment of computer network is complex. Most users do not possess the awareness of environmental control in computer rooms, and do not attach importance to the maintenance of computer operation environment, which exacerbates the vulnerability of computer operation environment. In particular, commercial computers, usually with the common network of mobile devices, and the simple setting of broadband ciphers, are easy to appear in the security of computer applications.

The optimization of computer technology has led to the rapid development of the surrounding industries. At the same time, the type of computer hardware equipment is more and more diverse and has been applied gradually. Hardware is the common phenomenon of cross application of computer applications, such as mobile hard disk, mobile hard disk function, although the technology continues to mature, and convenient to use, large memory, light volume, widely favored by all computer users, this application has gradually expanded, its security problems have also been exposed. When a mobile hard disk has a virus problem, a computer device that is connected may also have a virus. When the wireless and wired equipment are used cross - use, the virus transfer will occur. Although the safety of the limited equipment data is high, it will not be stolen directly. However, the data privacy of wireless devices is poor, and the ability of system security is weak. When the two devices are connected together, they will directly reduce the security of the wired device, and create data leakage [1].

In the past, the computer operating environment is mainly a single machine environment, and the existing security problems are relatively simple. However, the network environment is complex and the security problems are widely used, and the problem of network vulnerability is more common. For example, computer software in a single machine environment, software developers are relatively ignorant of security vulnerabilities, and in general, network security will not occur. But in the network environment, computer software is vulnerable to network security vulnerabilities in operation, and users' computer software security technology is not in place, which provides opportunities for viruses and hackers. At present, all computer software is running network vulnerabilities, which directly threatens computer application security. However, the development of targeted and systematic protection measures is lagging behind the development of network software vulnerabilities [2].

Computers have become the necessities for people's life and work. With the popularity of computer technology, the problem of computer crime is increasing. With the help of computer viruses, hacker attacks or Trojan horses, users can be invaded by some abnormal channels. When the user opens some websites of compensation operation, or after the message and the message page, it gives the opportunity to the Trojan horse and the virus invasion directly. Especially in special times, hackers will transmit a lot of frontal virus software, and users' operation safety awareness is not in place, which will directly exacerbate network security problems.

2. Factors Affecting the Network Security in Computer Appliation

Computer virus is a common network security problem, which is not easy to be developed by computer maintenance staff or users, but it is not easy to be attacked by computer maintainers or users, but the attack and destructive power of computer viruses should not be underestimated. Computer viruses can tamper with internal data, data information, software programs at any time, and even lead to computer deadlock. The more mature the computer technology is, the more diverse the types of computer viruses that contain the band. The virus is not targeted, and the spread of network security is also uncertain. The most common is the computer viruses contained in web pages and e-mail, which directly affect the normal application of computers. When you open a chat software, may also be the computer virus, the computer virus is everywhere, and the different harm degree, but will affect the normal use of the computer, it should strengthen the computer virus prevention awareness, standardize the operation of computer software [3].

Hackers than the computer virus, the attack can be strong, attack range, user account password, or important organs and units of computer, targeted to stop normal use of computers, or theft of state secrets, and the extent of damage and influence far beyond the computer virus. Before the attack, hackers often need to collect a large amount of effective information, clear the security vulnerabilities of computer users, and scan the computer security through scanning. On the basis of clear vulnerability, it tries to attack the computer to control the user's computer and eventually steal the value data information. Black attack will eliminate operating records, and attacked the user computer, will directly affect the association of computer generated, [2] chain reaction.

The Trojan horse program is also a common computer virus, also known as the Troy Trojan horse. As the name implies, the virus is latent in the computer, which is reflected with the various specific operations of the user's computer. Hackers attack user computers through Trojan horse programs. After Trojan horse attacks, Trojan horses immediately occupy the system resources and steal internal resources and information. At this time, the performance of computer security is reduced or lost, and information security is seriously threatened.

3. Countermeasures for Network Security in Computer Application

The network security protection in the computer application must be comprehensive and systematic, so it is very important to build a perfect network security system. Computer security system involves a wide range of systems, including security data collection, identification, processing and other systems, to achieve full security of data information. Analysis of computer security system based on hierarchy, including business information network layer, related to the client, and the simple network management protocol, syslog information; network layer is mainly responsible for the information collection agent; network security management layer, mainly in the role of manager, information storage data investigation and analysis, and security alarm operation. The application of computer security system has realized the automation and timeliness of information security processing [4].

The computer security system, mainly on computer viruses, Trojans and other issues, to achieve the security of computer data processing, protection, but the computer data security and cannot achieve all-round protection, strengthen the network information security protection, diversified safety precautions indispensable. The role of computer network security protection rules is mainly embodied in the following aspects; first, to strengthen the security of equipment base. The security system of security group has the functions of preventing SQL injection, network monitoring, Trojan invasion and so on, and then improving the computer security. With the help of intrusion detection or firewall technology, network security can be strengthened. Secondly, it is convenient for computer safety management to be set up. With the help of network access control, security responsibility partition, or security control password, security check and security risk announcement, we can improve the level of computer safety management. Finally, the process of computer security configuration can be normalized. Through the standardization of the computer account number more delete operation, Winchk/autoup configuration and installation, network security early warning, security log and other countermeasures to achieve. The diversification of network security protection is the necessity of improving the user's computer experience.

Any computer user should have the awareness of defense against network security problems, especially the commercial computer users. We must strengthen the defensive heart to ensure that all information stored inside the computer is secure and complete. Use disk and other removable storage devices, computer connection is required to scan for viruses, safety monitoring results show that after the use of broadband network equipment; application of strengthening stolen consciousness, password cumbersome, avoid the attacker crack information. At the same time, the problem of electromagnetic wave is handled well, as far as possible to reduce the insecurity factors of the network because of the magnetoelectric problem. Do not open the website, file, mail and so on. The data information stored in the computer must be backed up and encrypted to minimize the impact of security problems.

4. Network Security Prevention Technology

At present, the common network security prevention technology is shown as follows.

Firewall technology is a widely used network security technology. Any computer device has firewall software, users can adjust and update firewall software according to their needs. The technology of firewall, mainly installed in the protected network and the external network junction, with the help of logical partition thinking, analog signal in the data through the mouth to flow over uncertain and potentially destructive and unpredictable, through a series of scanning operations, to control access to the machine number, realize the security protection for the network. When the number of file and program access exceeds the original set limit, the firewall software will scan and partition the first time, and intercepts all kinds of illegal attacks. Or by closing the port to organize the access of the external network to the computer, as well as the information transmission with the local system, to avoid the infringement of the computer. However, the isolation technology is weak in preventing the potential Trojan horse's security problems, and the firewall itself is not fully mature. When setting up the firewall, it also needs other technologies to protect the network security [5].

Data encryption technology, as its name implies, is to encrypt data and files, and to ensure the safe transmission of network data. The data encryption technology not only improves the security of data transmission, but also weakens the tampering and access times of the target data transmission. Data encryption represents the person specific to the target data access. There are various data encryption methods, and the common technology is the public key algorithm and the symmetric algorithm. The latter refers to the key that the target data transmissions and receivers have and can be accessed and interrelated. When one of the keys is known, another key can be known according to the specified rule. The public key algorithm mainly refers to the unrelated key of the target data transmissions and receivers, and can not be reckon with each other according to the specified rules. Compared to the two algorithms, the symmetric algorithm has a fast speed, but the security performance is poor. The application scope of the public key algorithm is more than that of the symmetric algorithm.

Vulnerability scanning is the main function of vulnerability lookup. By scanning the file program and other systems, the potential vulnerabilities in the system can be quickly discovered. There are many ways of scanning, including port scanning, and Simulation of the hacker scan host. The former scan mode is to scan the physical links of ports, port signal strength and open network services through ports, and compare the scanning results around the vulnerability database, then clearly identify the type and influence degree of vulnerabilities. The way of simulating the hacker scanning the computer is mainly to take all kinds of attack operations based on the hacker role and attack the target computer network to determine whether there is any security problem in the target network. Improve procedures to determine existing or potential security problems, and improve repair vulnerabilities in time. In order to ensure the effect of vulnerability scanning, it is necessary to update the vulnerability database in time to ensure that the database is rich in resources. At the same time, we should pay more attention to the new trend of loopholes in real time and repair the loopholes in time [6].

The physical prevention technology mainly involves two aspects, namely, equipment maintenance and environmental security. The security environment can ensure the normal operation of the computer and network system, and prevent the influence of the external electromagnetic interference on the system. Preventive techniques include physical device isolation, and non-compliance with network protocols. Physical isolation system mostly adopts dual power supply, UPS centralized or decentralized power supply mode. Through reasonable system layout, we can improve the computer hardware management level, and then ensure the integrity of data information.

5. Summary

The significance of network security protection is that users' privacy and property are not infringed. Privacy in computer application mainly refers to the sound and hardware data is healthy, not stolen or lost. As a computer network security guard, it is necessary to have a clear grasp of the mainstream measures of computer network security prevention, to ensure that the control of computer control is not infringed.

Acknowledgements

Fund project: The Inner Mongolia Autonomous Region Education Department 2017 annual humanities and Social Sciences general project topic "cloud environment Inner Mongolia vocational education cross border collaborative teaching research" project number: NJSY17628

References

[1] Sun X. The study on computer network security and precaution[C]// International Conference on Computer Science and Network Technology. IEEE, 2012:1695-1698.

[2] Sun Y J, Zhang H L. Study on visualization algorithm in large-scale network security precaution[J]. Computer Engineering & Applications, 2006, 43(21):115-117.

[3] Shen J, Xu J, Li K, et al. A Study on Application of Neural Networks in Assessment of Computer Network Security[C]// International Conference on Materials Engineering and Information Technology Applications. 2017.

[4] Zhang X F. Research on the Architecture of Network Monitoring Administration with Precaution[J]. Computer Science, 2003.

[5] Chen Y P, Liu D L, Guo R. Security and precaution on computer network[J]. IEEE, 2010, 1:5 - 7.

[6] Chen Y P, Liu D L, Rui G. Security and precaution on computer network[C]// International Conference on Future Information Technology and Management Engineering. IEEE, 2010:5-7.