Research on Network Security Maintenance Based on Computer Technology

Li Mei Wang1,*

1Dongying Vocational Institute, Dongying, Shandong, 257091, China

*Corresponding author e-mail: wanglimei290@dyxy.edu.cn

Abstract. With the development of computer network information technology, the Internet has popularized the entire society. The Internet makes people’s daily life more free and convenient. Of course, the emergence of the Internet has also brought people's attention to information security issues. This paper analyzes and summarizes computer network security maintenance.

Keywords: Computer, Network Security, Maintenance

1. Introduction
Network security refers to the security of information on the computer Internet. Generally, we understand it from two states of static and dynamic. Static network security means that the software and hardware of the computer interconnection system are not destroyed, and the data and information in the system are in a complete, secret and reliable state. Dynamic network security refers to a stable state in which all links including storage, processing, receiving, and use of data information are not modified, stolen, lost or destroyed during the transmission of data.

2. The concept and characteristics of computer network security
The so-called computer network security mainly refers to the personal information security on the network. In today's era, there are various security loopholes and hidden dangers in the Internet. Network security mainly includes the following aspects, namely the hardware and software of the network system, and the security issues of our data and files transmitted through the Internet. If it can resist the destruction of various factors and produce a kind of technical management and maintenance measures, through effective management and control, it can ensure that the network system is always kept in an orderly and normal state and ensure the security of network data. The computer network security features are shown in Figure 1 [1].
2.1. Confidentiality
To ensure the security of user information, in the process of file transmission and use, the information cannot be disclosed to unauthorized users or entities. Only customers with access can have the authority to use and manage. Under normal circumstances, we use encryption Technology to achieve this important feature of computer network security.

2.2. Completeness
The user's information can only be changed with authorization. Only in this way can it be ensured that the information will not be easily destroyed during the process of storage, transmission and use, which effectively prevents the unreasonable loss of information. The feature of computer network security integrity is mainly from the perspective of security, and it requires the correct generation, storage and transmission of information during use [2].

2.3. Availability
The information stored, transmitted and used via the Internet needs to be used by users with access rights, and authorized users can be allowed to use it anytime and anywhere when required by network information services. Providing services to users is the most essential and one of the most important public uses of a network system. It can be measured by the ratio of the normal use time of the system and the length of the entire working time.

2.4. Controllability
Controllability mainly refers to the security attributes of the ability to control the dissemination of information and content. It can automatically prohibit and control those unhealthy content. When file information is transmitted through public networks, computer systems are often vulnerable to attacks. And destruction, this attribute of network security at this time will automatically help the computer to restore its original state.

3. The main problems of computer network security
In recent years, with the rapid development of Internet technology, more and more Internet attacks have gradually emerged, and various new situations and new problems in the operation of computer networks have emerged one after another. Due to the diversity of attack behaviors, network security issues also present a variety of situations [3].

3.1. System access control and management
For computer network security maintenance, system access control and management are the focus and difficulty of work. The so-called system access control and management refers to the monitoring and management of computer Internet data access services. System access control includes not only the management of data information holders, but also the management of data information users. In the process of control management, Focus on controlling Internet user profile information and its security.
However, according to the survey, data and information loss caused by system access control and management loopholes or missing management entry points, and imperfect remote control occupy a dominant position in all network security issues every year, and the probability of occurrence of the problem is as high as 27.38%. % has become the main reason affecting computer network security [4].

3.2. Security monitoring of data information
Affected by many factors, all current system access control measures have varying degrees of defects. They can often only control and manage past or current problems. Due to the lag in data and information security monitoring, once the Internet system In the face of new problems within the system, fragile systems are easily destroyed in the face of powerful cyber attacks. It can be seen that security monitoring plays an important role in maintaining network security. Good security monitoring is helpful for real-time alarming of attacks on the network and taking corresponding measures to prevent them, so as to deal with vulnerabilities in the shortest time to ensure User information security in the system.

3.3. The hardware and software of the computer network are at risk
In terms of resource sharing, development, application and remote management, in order to better provide users with convenience, when designing network hardware and software systems, there are often "backdoors" or "windows", or use network communication protocols. The network port is directly connected to the network system, and the user can directly log in to the terminal or server in a variety of ways. In addition, in the process of network system design, it is impossible to achieve perfection[5]. It is inevitable that there will be more or less loopholes. If the necessary protection measures and level identification are not established for network security, hackers can easily pass. Various loopholes in the above systems invade the computer network, easily tamper with and destroy the network system, and steal important information.

3.4. Man-made malicious attacks
This type of security hazard is the biggest problem facing computer network security at present. Man-made malicious attacks can destroy user information in various ways without affecting the normal operation of the computer network to make it effective and complete. Sex is threatened. For example, a Trojan horse program can directly enter the user's computer and destroy the computer's network security without any warning. It can modify important parameters inside the computer at will, copy important files inside the computer invisibly, and more importantly It can also unscrupulously peek at all the contents of your hard drive, etc., and finally control the user's computer easily. At the same time, hacker attacks on computer information networks are not uncommon in recent years. Hackers have super-strong computer systems and network-related knowledge. Through Internet loopholes, they use illegal methods to enter users’ computer systems to obtain important information. Eventually resulting in the loss of data, and even paralysis of the entire computer system, posing a major political and economic threat to the country [6].

4. Do a good job in maintaining computer network security
A complete network security standard system structure is shown in Figure 2.
4.1. Firewall technology
Firewall technology is one of the most conventional computer network security maintenance measures. The application of this technology can block unauthorized Internet users from the system and add a protective film to the network to reduce theft of user IP addresses and attack routes. The problem arises. Its working principle is to protect the internal network by setting up a barrier between the internal network and the external network to prevent illegal invasion by hackers or criminals and protect the internal network system from damage. At the same time, the firewall technology can also set different accounts and corresponding passwords for the modules of different levels in the intranet to fight against complicated vulnerabilities. Finally, the firewall can also identify the identity of the visitor through the monitoring program records and realize instantaneous alarm to illegal users. As the most basic hardware for information security protection, firewalls play a vital role in the overall defense system. A firewall with low response and processing capabilities not only fails to protect information security, it may even cause security risks. Therefore, when using firewall technology to insure computer network security, you should carefully distinguish and choose products that are cost-effective and have brand protection [7,8].

4.2. Information encryption technology
Encryption technology is widely used in network security applications and can effectively protect data security. As the name implies, information encryption is the act of password-protecting important data, information, and files that users of computer network systems need to protect. Since the daily use of computers communicates with each other through network channels, this communication process will strip personal information off the network. After the "information encryption" operation, even if the information is stolen by hackers, attackers or criminals through network vulnerabilities, it is difficult to decrypt it. Through the application of this emergency access mode, hackers or criminals cannot obtain real data. system. However, it is worth noting that when encrypting information, the indecipherability of the password should be ensured. The encrypted user can also change the password regularly to improve the protection [9].

4.3. Intrusion detection
By collecting information from several key points in a computer network or computer system and analyzing it, the method of discovering whether there are any violations of security policies and signs of being attacked in the network or system is known as intrusion detection. It is a reasonable supplement to the firewall, helps the system deal with network attacks, expands the security management capabilities of system administrators including security auditing, monitoring, offensive identification and response,
and improves the integrity of the information security infrastructure. In addition to the above-mentioned technologies, user authentication technology and digital watermarking are also one of the main methods for maintaining computer network security. Through strict user authentication, the identity verification and message verification of Internet user visitors in the system can be carried out to prevent attackers from pretending to be legitimate users to maliciously tamper with and steal information in the system [10]. Digital watermarking is a hidden technology that embeds important information into public content using specific symbols. It can protect the privacy of the information without affecting the complete use of the original data.

4.4. Prevent the invasion of computer viruses
Virus intrusion is one of the main factors that affect computer network security, and its impact on computer network security is also extremely huge. Some viruses do not break out immediately after invading a computer system, but are lurking in it. Once affected by certain factors, the impact of the virus detonates and even paralyzes the computer. Therefore, we must do a good job of security protection against computer virus intrusion, install genuine anti-virus software, and perform anti-virus in time, and ensure that it is not installed with other software during the installation process, and update it in time during the use process. The way to install the patch to avoid the invasion of human viruses. In addition, computer users must do a good job in data backup to reduce data loss caused by virus intrusion.

5. Conclusion
With the rise of the Internet, people’s lives have become more free and convenient. This has opened up our country's economic market and improved people's quality of life. But at the same time, the problem of network security become serious and we must face and solve. Therefore, we must continue to strengthen the improvement of computer information management technology and improve network security maintenance.

References
[1] QI Bo. Research on Computer Network Technology and Network Security Management and Maintenance [J]. China Strategic Emerging Industries, 2017:93.
[2] XIONG Zhi. Research on Computer Virus and Network Security Maintenance Technology [J]. Computer Products and Circulation, 2018:67-67.
[3] ZHANG Lijia. Research on Computer Network Security Maintenance Method [J]. China Science and Technology Expo, 2013:87-87.
[4] HUANG Zhuang-yong. Research on Security Maintenance of Computer Network System [J]. Consumer Electronics, 2013:102-102.
[5] Zhan Guangpeng. Discussion on how to do a good job in computer network security maintenance [J]. Electronic Technology and Software Engineering, 2014 (27): 47.
[6] WANG Quan. Research on Security and Protecting Measures of Computer Network Communication [J]. Science and Technology Rich Guide, 2013 (35): 125+159.
[7] ChengMingXia. Discussion on Computer Local Area Network Security and Network Security [J]. China Science and Technology Information, 2013 (24): 89-90
[8] LIU Zhang. Discussion on Management and Technology of Computer Network Security [J]. China New Communications, 2013 (23): 6-7.
[9] HAN Cai-hong. Research on Computer Network Virus and Network Security Maintenance [J]. Computer Disc Software and Application, 2014:177+179.
[10] REN Guo-ying. Research on Computer Network Security Maintenance [J]. Journal of Changchun Institute of Education, 2012:84-85.