Research on Computer Network Information Security and Protection Strategy

Bu Yinglei

Shandong College of Traditional Chinese Medicine, Yantai, Shandong, China

Keywords: computer; network information; security; protection; strategy

Abstract: Computers and networks are two different topics, but they are closely related. The widespread use of computers is an important symbol of society's move towards the information age, and the Internet has become a part of people's daily lives. Through the network, you can get fresh information, query data files, leisure and entertainment, etc. Therefore, the popularity of computer networks is convenient for people's daily life, which greatly satisfies people's information acquisition and provides many channels for information acquisition. However, computer network information security has always been a topic of public concern. Due to the continuous occurrence of network information eavesdropping, theft of customer data, and the loss of important files, people are questioned about the security of computer network information. This paper analyzes the computer network information security and protection strategy and discusses the corresponding solutions.

1. Introduction

The rapid development of modern information technology has made the network security situation more complicated, the threats faced by computers are more diverse, the new forms of network security problems are constantly changing, and network security issues are becoming more and more widespread. Although the total number of virus samples captured has decreased in recent years, the number of virus data transmitted on the mobile Internet has increased a lot, and these viruses have a tendency to spread to computers. Some are because malicious websites and Trojans are constantly increasing; some are complicated by the fact that wireless devices are infected with computer devices; others are that network security barriers are getting higher and higher, and they seriously affect the working life of netizens, resulting in a high degree of attention. taller and taller.

The reason for the emergence of computer network information security is mainly due to technical problems, including computer science and technology, computer network technology, cryptography, communication technology, information security technology and other factors. The reasons for these factors are that there is no sound computer network maintenance system, a lack of a complete network security management system, and loopholes in data maintenance of software and hardware, resulting in computer networks often being attacked by malicious viruses, resulting in loss of file data. Even the system is paralyzed, which seriously affects the normal operation of the computer network and affects the security, reliability, and stability of information transmission.

2. Computer Network Overview

2.1 Computer network belongs to the service platform.

For the purpose of resource sharing, a computer network collection is formed through the connection between the computer and the network. The development of computer networks in China has gone through four stages: (1) the remote terminal online stage. (2) Computer network phase. (3) The stage of computer network interconnection. (4) International Internet and Information Highway Phases. Each stage is reformed and innovated through the application of science and technology on the original basis. Today's computer network development is in the fourth stage. The computer network includes two parts: the transmission medium and the communication device. Since the computer network carries the tasks of information exchange, information transmission, and information storage, once the network has security problems, the data

  DOI: 10.25236/scmc.2019.009

in the transmission process will be lost, resulting in the transmission of the communication device. Information disclosure.

2.2 Computer network security features

1) Computer network security has a confidentiality feature, requiring the user's private information not to be known by others, to ensure that the information in the computer is not leaked, and to ensure the privacy of the user's personal information;

2) Ensure the availability of the computer, so that the computer can perform normal operations within the normal range, not only the information can be read at any time, but also the user's needs can be realized by various software;

3) It should also have the cybersecurity interface auditability, good control of the computer, the normal and orderly dissemination of information, and the prevention of malicious tampering or loss of information.

3. The cause of computer network information security is threatened

The root cause of the threat to computer network information security lies in the security problems of the network, which are summarized as follows:

3.1 Intrinsic security vulnerabilities

Once the new operating system or application software is available, the vulnerability has been identified. No system can eliminate the existence of vulnerabilities, and it is harder to fix all the vulnerabilities than to go to the sky. From CERT (CarnegieMellon University Computer Emergency Response Team), you can find a fairly comprehensive list of program errors. Another source of news is newsgroups such as BugNet or NTBug traq. (1) Buffer overflow. This is the most vulnerable system vulnerability in an attack. Many systems receive data input of any length without checking for changes between the program and the buffer, placing the overflow on the stack, and the system executes the command as usual. This destroyer can take advantage of it. As long as he sends an instruction that exceeds the length that the buffer can handle, the system goes into an unstable state. If the vandal is specially configured with a string of characters he is prepared to use as an attack, he can even access the system root directory. (2) Refusal of service. The principle of denial of service (DenialofService, DoS) attacks is to disrupt the order of TCP/IP connections. A typical DoS attack can deplete or corrupt one or more system resources (CPU cycles, memory, and disk space) until the system cannot process legitimate programs. An example of such an attack is a Synflood attack. The destroyer who launched the Synflood attack sent a large number of illegal requests to request a connection in order to make the system overloaded. The result is that the system rejects all legitimate requests until the request waiting for an answer times out.

3.2 Abuse of legal tools

Most systems are equipped with tools to improve system management and service quality, but unfortunately, these tools are also used by destroyers to collect illegal information and enhance attacks: for example, the NBTSTAT command is used to give the system The administrator provides information about the remote node. But the destroyer also uses this command to collect information that is threatening to the system, such as the identity of the regional control software, the name of the NetBIOS, the IIS name, and even the username. This information is enough to be used by hackers to decipher passwords. Another tool that is most commonly used is the PacketSniffer. System administrators use this tool to monitor and distribute network packets to identify potential network problems. If a hacker wants to attack the network, the NIC will first become a function-promiscuous device, intercept the packets that pass through the network (including all unencrypted passwords and other sensitive information), and then run the packet sniffer for a short time to have enough information. Go attack the network.

3.3 Incorrect system maintenance measures

The inherent vulnerabilities of the system and a large number of ubiquitous destruction tools greatly facilitate the attack of hackers, but invalid security management is also an important factor causing security risks. When new vulnerabilities are discovered, managers should carefully analyze the level of hazard and take immediate remedial action. Sometimes, although we have already maintained the system and updated or upgraded the software, due to the complexity of the filtering rules of the router and firewall, new vulnerabilities may occur in the system. Therefore, timely and effective change management can greatly reduce the risk to the system.

3.4 Inefficient system design and detection capabilities

Security systems designed without regard to information protection can be very “unsafe” and cannot withstand complex attacks. Building a secure architecture must start at the bottom. This architecture should provide effective security services and be properly managed. The code design and execution of the server is also effectively managed. Recently, there have been many public vulnerability reports stating that cgi bin is very vulnerable when input checks are incomplete. Hackers can exploit this vulnerability to launch denial of service attacks, illegal access to sensitive information, or tampering with Web server content. Inefficient design will eventually lead to a loophole intrusion detection system. Such a system is very dangerous, it does not provide enough information, and even the information provided may be untrue and inaccurate.

4. Security threats to computer network information

4.1 Natural disasters

Computer network systems are very sensitive and vulnerable, and are susceptible to external natural factors. Natural factors mainly include the influence of a series of factors such as the temperature of the environment, the humidity of the environment, and the degree of pollution of the environment, resulting in the failure of the operating system of the computer. Under normal circumstances, the machine room must have basic dust-proof facilities and anti-shock facilities, and the computer room must be kept at a constant temperature. However, the computers in our daily lives do not have these configurations, so it is easy to cause the computer network system to face natural disasters without good resistance, thus reducing the defense ability of information security.

4.2 Computer virus

The virus spreads quickly and has a wide range. Every year, many computer network systems are attacked by malicious viruses, causing huge economic losses. Generally, viruses are highly aggressive, destructive, contagious, and concealed. Viruses can damage computer applications and execution programs through network data transmission, resulting in a decline in the efficiency of computer systems and loss of hardware data.

4.3 Operational errors

The operation generally means that the computer user does not have a basic understanding of the computer network security. In the process of using, there is no awareness of the insecure network, and the garbage file is cleaned and disinfected from time to time, and the password of the computer is easily falsified and formed into a network. Vulnerabilities severely restrict the normal operation of the computer.

5. Computer Network Information Security Protection Strategy

5.1 Improving the natural environment

Improving the natural environment means improving the environment in which the computer is used, including temperature, humidity, dust, and the like. Therefore, in the process of using the computer, it is necessary to strengthen the external maintenance of the computer, reduce the use of

the computer in a humid environment and high temperature, and often clean the dust of the computer to prevent the computer system from aging.

5.2 Installing Firewall and Antivirus Software

The firewall can effectively control the access rights of the computer network, automatically analyze the security of the network, and have certain defense functions against illegal websites. The firewall can prohibit the access of illegal websites, filter the messages with problems, and improve the security index of the network system. . At the same time, it is necessary to install anti-virus software, which can intercept the propagation path of the virus through software, and timely anti-virus can interrupt the spread of the virus and improve the security performance of the computer network.

5.3 Strengthen the application of computer intrusion detection technology

Intrusion detection is mainly for the operating system of data transmission security detection. Through the use of IDS (Intrusion Detection System) intrusion detection system, the abnormal phenomenon between the computer and the network can be discovered in time, and the user is prompted by the form of alarm. Intrusion detection technology must integrate the comprehensive application of a series of technologies such as statistical technology, data analysis technology and password cracking technology to ensure the smoothness of the network and timely discover loopholes and fill in loopholes.

5.4 Other measures

A series of common measures, such as installing computing vulnerability patches, strengthening computer network password settings, enhancing the application of network monitoring technologies, and improving the security management awareness of accounts, can provide security for computer network security.

6. Conclusion

In summary, there are still many problems in computer network security in China. Due to the lack of perfect network security management system and scientific emergency measures, computer network information security faces enormous challenges. Therefore, it is necessary to establish a sound network information security protection system, formulate a scientific response plan, and control the destructive factors affecting network security through effective solutions. Only by ensuring the security of network information can the service function of the network be improved. Therefore, in the process of using the computer, it is necessary to improve the awareness of security and prevention, in order to reduce the invasion of malicious hackers, and to improve the security of network information.

References

[1] Peng Nanbing. Research on computer network information security and protection strategy [J]. Electronic Technology and Software Engineering, 2013, 22

[2] Liu Dongmei. Analysis of computer network security and prevention strategies [J]. Heilongjiang Science and Technology Information, 2010 (19).