Computer Network Security Risks and Management Measures

Xiaohua Xu[1], Xiaofei Hu[2]

[1]Network Information Center, Zhaotong University, Zhaotong, Yunnan, 657000, China

[2]School of Mathematics and Statistics Zhaotong University, Zhaotong, Yunnan, 657000, China

Keywords: Computer, Network security risks, Management measures.

Abstract: With the rapid development of China's economic level and computer technology, computers have been widely used in all aspects of people's life and work, affecting people's lifestyle and work efficiency. Meanwhile, people's application requirements for computer network communication are getting increasingly high. However, computer network communication has brought a series of security issues while bringing convenience to people. Network theft and cyber fraud accidents frequently pose a great threat to people's privacy and property, which has aroused widespread concern from all walks of life. It can be seen that the security protection of computer network communication is very important, and we must pay high attention. This paper mainly discusses the importance of computer network security and the security problems faced so far, and proposes corresponding preventive measures.

1. Introduction

With the rapid development and popularization of computer network technology, big data and informationization have become the general trend of human society development. Computer network communication technology inevitably bears various risks while bringing convenience to people's lives. Once there is a problem in the computer communication network, it will threaten the communication security of the network, which will affect the security and stability of the whole society. In order to reduce the occurrence of security incidents, people have developed a lot of security software, but underestimated the technology of hackers. Security software can only maintain security for a period of time and soon loses security. Therefore, we must proceed from the source of computer network communication technology, do a good job of security protection when using computer network, and optimize the network environment.

2. The Concept and Importance of Computer Network Security

Computer network security has different connotations in different situations. For example, in the process of online chat, the network security mainly means that the user's chat information will not be leaked, to ensure the security and integrity of the information. When users conduct business operations, computer network security means that business operations will not leak data due to hackers or computer viruses. In the process of users doing online shopping or using online banking, computer network security means that the bank card password or its own finance will not be stolen and financial security is guaranteed. As a kind of information transmission system, computer network has penetrated into all aspects of people's work and life, and has become an inseparable part. In life, most people use the Internet to conduct transactions. They store personal information and bank cards in computer networks. Once the network security factor declines, criminals can extremely easily steal people's privacy and cause property losses. Computer network communication security mainly has the following characteristics. First, in the process of network communication and transportation, the first thing to ensure is the integrity of the data. In the process of information transmission, the security and integrity of such information will not be lost due to external factors. Second, network communication security is non-repudiation. Once the user's behavior has a certain impact, it is

  DOI: 10.25236/iccse.18.076

impossible for the user to deny the impact of these effects. Third, computer network communication security has a certain degree of confidentiality, which is not accessible for any user and has a certain group restrictions, which means that it can only be accessible through the authorization of the user.

According to the survey report, nearly 82% of netizens have great security risks when using online payment functions. Nearly half of netizens will frequently use WIFI in public places and forget their own browsing traces after using them, which directly leads to China's large-scale economic losses in recent years due to computer network communication security problems which even have reached as high as hundreds of billions of yuan. In addition, even national government departments will use computer network communication technology. The government departments' computers store and process confidential information and documents related to national security, military, national defense and politics. Once the computer network communication security problems occur, they will inevitably become the target of hostile forces and criminals, which will seriously threaten the country's safety and harmony; people's computer network communication systems continue to expand to industrial, aerospace, navigation, agriculture, etc., but computers are prone to failures due to environmental impacts, leading to problems in the security of computer network communications, which in turn affects the development of various undertakings in China [1]. Therefore, we are constantly seeking scientific and effective ways to maintain the security of computer communication networks, so that computer networks can improve people's work efficiency and promote the rapid development of China's economy while ensuring the security of information and resources of people and even the country.

3. Current Security Issues Computer Network Communication Technology Faces

In recent years, with the popularity of computer network applications, network security incidents are frequent and still rising. The number of cases on cyber security issues accepted by public security organs has increased by an average of 110% per year, including people inadvertently leaking during daily chats. The privacy of the bank card account is stolen; when the e-commerce uses the network transaction, the security factor of the network is low or the sudden failure of the computer affects the preservation of the data in the computer, resulting in economic losses, etc. In the case of security incidents, the most common is computer hacking and virus intrusion, accounting for 35.6% of the total amount.

3.1 Computer hackers and virus intrusion

The invasion of hackers is a relatively difficult and threatening type of security issue in the computer industry. Hackers mainly use both destructive and non-destructive attacks to achieve the purpose of attacking other people's computer communication networks. They use destructive attacks to steal private information and corrupt data in order to invade other people's computer systems. Destructive attacks can generally be divided into two types, cyber-attacks and network spy. The cyber-attack selectively destroys the integrity of the information in people's computer, causing the computer system to smash; while the network spy is to steal and decipher the confidential information without affecting the normal use of the network. Non-destructive attacks by hackers generally use information bombs or denial-service attacks. It does not affect the operation of computer network systems or steal confidential information [3]. Hacking attacks generally have the means to obtain passwords, email attacks, Trojan horse attacks and system vulnerabilities. They usually steal information from internal organizations such as governments, banks, companies, etc. to gain benefits.

The invasion of viruses is also one of the great threats faced by computer network communication systems. The spread and growth rate of computer viruses are unimaginable. They are mainly attached to external programs or files. When computer users run programs or open files, they will invade the computer system and spread. They affect the operating efficiency of the computer; worse still, they cause damage to the components of the motherboard, cause the loss of data information in the computer and affect the interests of individuals, enterprises and even the country [4]. In an open network, viruses can easily invade into personal computers through emails and attachments, and even

infect other computers in the network, causing serious security risks.

3.2 Computer software's own flaws and vulnerabilities

Network software cannot be completely free of defects and vulnerabilities. With the advancement of technology, many companies have their own computer network departments, and will also develop some system software. The technical level of software developers is the key to affect the safe operation of software. Many enterprises have problems such as: lack of mature technology, programming language restrictions, and establishment of backdoor programs, resulting in problems in the security of the entire computer communication network system [5]. However, these vulnerabilities and defects are just the entry point for hackers to attack, posing a security risk to the computer network. The hackers that have been appearing in previous years have invaded computer network incidents and caused great sensation in society. The main reason for these incidents is that flaws and vulnerabilities in the development of computer software have given hackers a chance.

3.3 Lack of systematic computer network communication security measures

Today's computer network communication systems are designed to be more functional, ignoring the setting of system security measures. When the user logs in to the computer, only the user name and password are set, and the security factor is low, which increases the loss rate of the user information and data, and also provides an opportunity for the illegal user to invade. In addition, many enterprise websites do not have a security verification mechanism. The background management and page publishing interface are open to the Internet. There is no encryption or firewall setting. Therefore, it is easy for data and web page information to be tampered with.

4. Computer Network Communication Security Precautions

4.1 Improve laws and regulations on computer network communication security

Computer network communication security accidents occur frequently. The relevant departments must do a good job in the construction and improvement of relevant laws and regulations, and kill all the factors that threaten the security of network communication in the cradle. Relevant departments should implement the requirements of *Regulations on the Protection of Computer Software* and *Provisions on Technical Measures for Internet Security Protection*, and timely update and supplement the regulations to find effective prevention methods. We will impose severe penalties on criminals who endanger the security of computer network communications and effectively safeguard the security of the national information network.

4.2 Hardware system security protection strategy

4.2.1 Physical security strategy

The physical protection strategy of network communication security is actually to take physical protection measures for physical equipment, to reduce the probability of damage to computer hardware equipment due to unexpected factors or human factors. This requires all units to develop detailed computer network usage regulations, especially to strengthen the management of the use of the computer room, put away the key of the computer room, and prohibit non-computer management personnel from entering the machine room without authorization, so as to effectively prevent the destruction of human factors.

4.2.2 Device protection strategy

People often ignore some of the security settings that come with the device during the use of computer equipment, resulting in some security incidents that could have been avoided. This requires the computer administrator to perform the necessary security settings for the software device in the future use of the computer. The software device here mainly refers to the server, the switch, and the like. By setting, it is possible to effectively prevent hackers from attacking these software devices.

Timely update some anti-virus software and firewall settings, improve the anti-virus software features, and facilitate the timely detection of some junk files and intercept.

4.3 Software system security protection strategy

4.3.1 Canceling some unwanted services and ports

Software system protection is not as simple and controllable as hardware. In order to enrich the functions of the computer, people often install many service ports, or install some unnecessary service ports without their own consciousness. As everyone knows, the more ports in the computer, the more easily the computer is attacked and the security is greatly reduced. Therefore, users should pay attention to frequently check whether there are unnecessary services and ports in the computer when using the computer network and shut them down in time. In addition, users can also install some port monitoring programs to better understand the port usage. Once a hacker attacks the computer system, the monitoring program will automatically alert you that the computer user can close the service port in time, which can effectively prevent hackers from invading.

4.3.2 Correctly hiding the computer's IP address

The IP address is a necessary condition for hacker attacks, and the hacker can only attack the user's computer system by obtaining the user's IP address. The main way for hackers to obtain IP addresses is network detection technology. After detecting IP addresses, they can implement DOS attacks and FLOOP overflow attacks. Therefore, computer users should pay attention to the hiding of their IP addresses while using the computer network. You can use the proxy server to hide the real IP address, so that the hacker only displays the IP address of the proxy server during network detection, to a certain extent. It can truly protect the security of computer communication networks.

4.3.3 Changing the user's account and password from time to time

Another means of protection for computer communication networks is the enhancement and updating of user accounts and passwords. Once the password security index is low, it is easily intercepted by hackers or other criminals. In this case, it becomes a breeze to obtain or destroy the information in the user's computer, and any security protection related to the computer system cannot function. Therefore, the user should frequently change the Administrator account and password during the process of using the computer communication network. More importantly, the complex and powerful password should be set so that the hacker cannot easily intercept or crack it. Users can also prevent hackers from invading by creating an Administrator account without any permission, so as to ensure the security of the computer communication network system.

5. Summary

All in all, computer network security and protection is a complex systematic project. In the face of various security threats, we must deeply think about and study the security of computer network communication. In order to do the relevant security protection work, hardware and software protection measures must be implemented in a two-pronged manner to prevent various potential intrusions and attacks, reduce the harm of hackers and viruses to computer network security, and avoid unnecessary losses. While doing all kinds of protective measures, we must also be good at using legal means to maintain our own privacy and property safety. Relevant departments must severely punish acts that undermine the security of network communications, and urge every member of the society to effectively maintain the security of computer network communications.

References

[1] Xiong Wenqing,Pan Dan. Application of Computer Network Security Technology in Network Security Maintenance, *Network Security Technology and Application,* 2018(10):2+17.

[2] Liu Yuanbing. Discussion on the Application of Computer Network Security Technology in Network Security Maintenance, *Computer Programming Skills & Maintenance,* 2018(09)， 159-161.

[3] Guo Baojun. Design of Campus Network Security Anti-virus System -- Taking the Campus Network of Bowen College of Lanzhou Jiaotong University as an Example, *Electronic Production,* 2018(18):51-52.

[4] Chen Feng. Problems and Maintenance Measures of Computer Network Security Risk Management, *Rural Economy and Technology,* 2017, 28(06):279.

[5] Yang Qicheng. Study on Computer Network Security Risks in Schools and Management Measures, *Journal of Cangzhou Vocational and Technical College,* 2015, 14(04):59-61.