The Strategy of Computer Network Information Security and Protection

Teng Long

Hainan College of Economics and Business, Haikou, China

Keywords: Computer, Network, Information security, Information protection.

Abstract: The problem of network information security in the information age has become the main factor leading to the leakage of user information and the security of use. It has greatly affected the security and user experience of computer network systems. Therefore, this paper is about common network vulnerabilities and computers such as network viruses. The network security problem is elaborated, and on this basis, the computer network information security protection strategy is analyzed and studied, aiming at improving the security of computer network information and avoiding the security risks such as information leakage caused by users due to network security problems.

1. Introduction

With the rapid development of computer network technology, people's demand for network information systems is becoming more and more vigorous. However, while computer network systems bring convenience to people's work and life, they also bring some security threats. Therefore, this paper believes that we must carefully analyze the specific situation of computer network information security issues as soon as possible, and propose a targeted protection strategy to enable open and extensive computer network systems to provide secure network information and ensure The computer network system can run normally [1]. It should be said that computer network information security and its protection work is a comprehensive project involving many aspects. We must ensure the security of the software and hardware of the relevant network system and the storage data, so that the computer network system can ensure the security of network information.

2. The definition and connotation of network information security

Maintaining network information security mainly uses various means to effectively protect the hardware, software and data of the network system so that the network information is not damaged or leaked due to accidental factors or malicious damage, ensuring the integrity of the network information data. Usability, confidentiality and legal are used to ensure the normal operation of the network system [1]. Network information security involves both network technology and network management. Among them, network technology is mainly to prevent attacks from external illegal users, and network management is focused on internal human factors management, which complement each other and are indispensable [2]. At present, with the development of computer technology, effective protection of network information data and improvement of computer operation security have become the focus of computer application.

3. Security threats to computer network information

There are various security threats in computer network information. The most frequent are natural disasters, the vulnerability of network systems themselves, user operations errors, man-made malicious attacks, computer viruses, spam and spyware, and computer crime.

3.1 Natural disasters.

Computer information systems are just intelligent machines that are susceptible to natural disasters and the environment (temperature, humidity, vibration, shock, pollution). At present, many of us use

DOI: 10.25236/iwmecs.2019.006

computer space without measures such as shockproof, fireproof, waterproof, lightning protection, electromagnetic leakage or interference [2]. The grounding system is also lack of thoughtful consideration, and the ability to withstand natural disasters and accidents is poor.

3.2 The vulnerability of the network system itself.

The most significant advantage of Internet technology is openness. However, this wide openness, from the perspective of security, has become a vulnerable vulnerability. In addition, the TCP/IP protocol that the Internet relies on is not high in security. The network system running the protocol has threats and attacks such as spoofing attacks, denial of service, data interception, and data tampering [2].

3.3 User operation error.

User security awareness is not strong, user password settings are simple, users will leak their own accounts, etc., will pose a threat to network security.

3.4 Man-made malicious attacks.

This type of attack is the biggest threat to computer networks. Malicious attacks can be divided into active attacks and passive attacks. Active attacks selectively destroy the validity and integrity of information in various ways. Passive attacks intercept, steal, and decipher to obtain important confidential information without affecting the normal operation of the network. Both of these attacks can cause significant harm to the computer network and lead to the leakage of important data [3]. The network software used now has more or less certain defects and vulnerabilities. Network hackers usually use the means of hacking into important information systems, eavesdropping, acquiring, attacking and infiltrating important information about sensitivity, and modifying and destroying the normal use of information networks. The state, resulting in data loss or system paralysis, has caused major political and economic losses to the country.

3.5 Computer virus.

A computer virus is an execuTable program that can be stored, executed, hidden in execuTable programs and data files without being discovered by humans, and can be acquired after being triggered [3]. It is contagious, latent, triggerable, and disruptive. Computer viruses are mainly spread by copying files, transferring files, running programs, and so on. In daily use, floppy disks, hard disks, optical disks, and networks are the main ways to spread viruses. When a computer virus runs, it may reduce the efficiency of the system. In the meantime, it may damage files or even delete files, causing data loss and damage to the system hardware, causing various unpredicTable consequences [3]. Many kinds of malignant viruses that have emerged in recent years are spread on the basis of the network.

4. The importance of computer network information security

Computer network security refers to protect data in hardware devices, software devices, and systems in a network system from being destroyed, altered, or leaked by various reasons. Network information security includes the integrity, true availability, and confidentiality of network information [4].

The computer network has the characteristics of resource sharing, which improves the efficiency of research, culture and economy, but at the same time increases the possibility of attack. Many organizations are illegal and destructive when publishing messages through the network platform. The risk of access; secondly, as e-government, e-finance and other systems involve sensitive information in various fields, it is particularly important to maintain the security of network information; finally, the security of network information is political, military, cultural, economic, and Social life and other aspects have a direct impact [4]. Now the global mobile communication network has become the main strategic goal of information warfare in various countries. The struggle for theft and anti-theft, destruction and anti-destruction on the network will become more and more fierce.

5. Threats to computer network information security

5.1 The hacker has a purposeful attack.

The hacker uses his own computer technology to purposefully attack or invade the user's computer system to obtain the information he needs. This method is the most common way of computer network information security, and its hidden threat is also the biggest. It can be easily divided into: cyber attacks and network reconnaissance [5]. The cyberattack is mainly caused by hackers using various technical means to destroy the network information. The network reconnaissance is different. It is the behavior that the hacker uses the technical means to obtain or steal the information needed by the hacker without affecting the normal operation of the network. Both network attacks and network investigations pose a security risk for network information security, which has a major impact on individuals and society [5].

5.2 Computer viruses.

Hidden in storage and execution programs are characteristics of computer viruses. They cannot be discovered in time. If they are triggered under certain circumstances, they can interfere with the operation of the computer system [4]. In severe cases, the system is paralyzed and the important information of the user is lost. It is precisely because of the contagious, destructive, and potential characteristics of computer viruses that they create conditions for the spread of computer viruses.

5.3 Computer user error.

Users in the computer, due to a variety of factors may accidentally delete certain system programs, such as: hard disk formatting processing, image restoration to the wrong partition, etc., will affect the normal operation of the computer [6]. Moreover, computer users do not pay much attention to their own information security, which may lead to security risks. It is not uncommon for hackers to crack weak passwords. There are also some users who store their important information in a shared folder or on a public network, causing information loss or exploitation by criminals for personal gain.

5.4 Spam.

Some criminals use e-mail as a means of transmission, send e-mails to the mailboxes of computer users, and obtain computer user information after the other party accepts the e-mail. There is a big difference between spam and computer viruses [4]. The former is to obtain user information or to advertise. The latter is to invade the user's computer system to obtain information and affect the normal operation of the computer system.

6. Protection strategy of computer network information security

In view of the various potential threats of computer network information security above, we must take appropriate security measures to ensure the security of network information as soon as possible. The specific protection strategies are as follows:

6.1 Further strengthen the account security of network users.

Since computer network information security first involves the problem of user accounts, it involves a wide range of applications, including system login accounts and email accounts, online bank accounts and other application accounts. Then, for network hackers, they attack Get some user accounts and passwords for the network system [6]. Therefore, for this kind of security problem, we should set a more complicated password for the account that the computer network system logs in, and try not to use the same or similar account as much as possible.

6.2 Install network protection software.

That is to say, for computer network systems, the security needs to be effectively protected by installing a network firewall. The so-called network firewall technology refers to preventing external users from obtaining legitimate network resources through illegal means by strengthening access control between networks, thereby providing a special network security protection device for computer network systems [3]. Therefore, we should install a firewall to monitor the operation of the network in the current security of computer network information.

6.3 Install the vulnerability patch.

In the computer network information security system, its vulnerability is also the reason why it is vulnerable to attack. This is because vulnerabilities in computer network systems are one of the most vulnerable to attacks, which can be manifested as software, hardware or program problems [3]. As a related study in the United States pointed out, in today's more popular computer operating systems and applications, there is no possibility of any loopholes or defects. Therefore, we must install relevant patches in time for these security vulnerabilities as soon as possible. Sometimes some software developers will release some targeted vulnerability patches for these vulnerabilities to effectively solve various security risks or problems caused by the vulnerability programs.

6.4 Do a good job in network monitoring and monitoring.

Computer network information security issues also require us to be equipped with relevant intrusion detection and network monitoring technologies. In fact, intrusion detection technology is a new network information security technology that has only begun to develop and gradually become popular in recent years. It integrates various technologies and methods such as statistical technology and network communication technology to enable computer networks [2]. Whether the system has been illegally invaded or abused for certain monitoring and monitoring.

6.5 Use file encryption and signature technology.

For the various problems existing in computer network information security, especially the network information security problem caused by the unrestricted openness of computer network systems, some legitimate user information and system information are easily stolen or misused [4]. Then, we should do file encryption and digital signature technology. It should be said that file encryption and digital signature technology is a new protection technology to improve the computer network information system and data security and confidentiality. It helps prevent some secret data from being stolen, intercepted or destroyed by the outside. .

6.6 Application of firewall technology.

To maintain computer network information security, you should try to install an effective firewall and anti-virus software. Among the existing computer network information security protection technologies, the application of firewall technology is one of the most effective means to improve network security. It can securely control network access and prevent external users from entering the internal network and accessing network resources by dangerous means [6]. Technology is an important means of protecting the internal network operating environment. In addition, firewall technology can also reasonably divide network resources. Firewall technology is usually divided into different types, including monitoring firewalls, proxy firewalls, address firewalls, and filtering firewalls.

6.7 Information encryption and digital signature technology.

Information encryption technology refers to technologies that avoid information theft, information leakage, information destruction or interception of confidential data and information. The ultimate goal is to ensure the security of computer network information and data, including symmetric encryption and asymmetric encryption. Among them, the symmetric encryption technology uses symmetric cryptographic coding technology, and the key used must ensure the consistency of encryption and decryption, that is, the encryption password can be used for decryption [6]. The application of symmetric encryption technology is relatively simple and convenient, and the difficulty of deciphering the key is high. The asymmetric encryption technology is to solve the problem of information public transmission and key management.

6.8 Network monitoring intrusion detection technology.

Intrusion detection technology is an emerging prevention technology. This technology integrates many methods and technologies, such as reasoning, cryptography, artificial intelligence, network communication, and statistical technology. The main function of intrusion detection technology is to monitor whether the computer network system is I was abused and invaded. According to the analysis technology used, it is divided into two methods of statistical analysis and signature analysis. The statistical analysis method refers to judging whether an action is in a normal orbit according to the action mode monitored under normal circumstances on the basis of statistics; and the signature analysis method refers to monitoring the weak points existing in the network system for attacking [7]. Behavior, through the attack mode can summarize its signature and add it to the IDS system, this analysis method is essentially a pattern matching operation.

6.9 Install vulnerability patches in a timely manner.

Vulnerabilities in the attack are the main weaknesses, including the unreasonable configuration or functional design, as well as the shortcomings of programs, hardware, software, and so on. To compensate for vulnerabilities in network systems, software developers should write effective patches. In order to effectively solve the network information security problem caused by the vulnerability, the vulnerability patch should be installed in time [7]. There are already a lot of host vulnerability scanners to scan for vulnerabilities, such as tiger, COPS, etc. In addition, you can use tencent butler, 360 security guards and other software to download vulnerability patches.

7. Conclusion

In short, a single method can not solve the problem of computer network information security, and should have a comprehensive defense mechanism and a comprehensive protection strategy. The computer network information industry is cumbersome and fast-changing, so its protective measures should also change with the development of network information technology. With the continuous improvement and maturity of network information security protection measures, network technology will also develop accordingly. Therefore, network information security protection strategies should be improved and improved through various channels and technologies to provide a more secure and sTable computer network information.

References

[1] C.D. Huang, Technical Research on Computer Network Information Security Issues, Software, 2018, vol.1, pp.140-142.

[2] D.F. Wang, Research on Computer Network Information Security and Protection Strategy in the Age of Big Data, Wireless Internet Technology, 2015, vol.24, pp.40-42.

[3] H.J. Tang, Computer Network Information Security Related Issues, Information Technology and Informatization, 2017, vol.2, pp.33-35.

[4] Y.B. Wang, Computer Information Security Technology and Protection Research, Computer CD Software and Applications, 2018, 01(11): 63-64.

[5] L.T. Wang, Computer Network Information Security and Protection Strategy Research, Computer Knowledge and Technology, 2016, vol.3, pp.113-115.

[6] H.M. Wang and H.J. Zong, Research on Computer Network Information Security and Protection Strategy, Value Engineering, 2017, vol.11, pp.143-145.

[7] F.W. Lin, Computer Network Information Security and Protection Strategy Research, Network Security Technology and Application, 2016, vol.1, pp.22-23.