Influencing factors and preventive measures of computer network security

He Xinzhou

Changjiang Polytechnicch, Hubei Province, Wuhan, 430074, China

hexinzhouhb@126.com

Keywords: computer; security; preventive measures.

Abstract: Computers and networks have become an indispensable part of people's lives. They have been integrated into many fields and have changed the traditional way of life. However, there are threats of hackers and viruses in current computer networks, which not only cause information security problems, but also may lead to property damage. Therefore, it is necessary to strengthen the construction of computer network security. Based on this, this paper first analyzes the significance of computer network security protection, and then explores the specific influencing factors of computer network security. Finally, it focuses on the measures to strengthen the security construction of computer network, hoping to provide some reference and direction for computer network security protection.

1. The meaning of computer network security protection

The core of computer network security is to protect the data processing system, to prevent the computer information from being leaked and destroyed. In addition, the computer network security also maintains the normal realization of the computer function. For the current society, computer networks play a vital role. It not only facilitates people's communication and communication, but also plays an economic and political role. It is also because of the increasing importance of computer networks, so often All forms of invasion have caused information leakage and property damage. Computer network security also has sudden features, causing computer paralysis, so strengthening computer network security has a very important significance, it can effectively maintain people's normal life, while protecting property security.

After entering the 21st century, computer networks have become an indispensable part of various fields. People's lifestyles have also undergone tremendous changes in computer networks, but corresponding computer intrusions have become more frequent. For individuals, computer network security issues can affect property security and life communication; for enterprises, computer network security will involve corporate confidential information and technology, and may also bring huge property losses; for the country, computer networks Security is even related to politics and the national economy. Therefore, it is necessary to continuously strengthen the construction of computer network security and build a secure information society.

2. The influencing factors of computer network security

2.1 Natural cause

The influence of natural environmental factors on computer network security is not great, but if there is a large natural disaster in the computer placement area, it may cause damage to the computer hardware facilities, which may cause network security problems. For example, lightning disasters, earthquake disasters, etc., can affect the computer itself through the environment, which not only interferes with the normal use of the computer, but also causes computer damage or the problem that the network line cannot be connected.

2.2 The problem of the computer system itself

The operating system is an integral part of the computer and the key to realizing the normal function of the computer. But computer operating systems also have security vulnerabilities that create the risk of being compromised and creating opportunities for criminals to attack computer networks. For example, the "bitcoin virus" that appeared in 2017 is to exploit the loopholes in computer systems and to attack computer networks on a large scale, causing huge losses to the society. Moreover, the scope of the problems caused by such problems is large, causing paralysis of computer systems in a short period of time, seriously affecting people's normal use.

2.3 Software problems

People use computer software to implement various functions, but there are also security vulnerabilities in computer software, which causes computer network security problems. After people buy a computer, they download and install the software according to their needs. However, some criminals will implant a virus in the software, and the user will pose a system threat when installed and used. Although the current anti-virus software and system protection are relatively mature, software security vulnerabilities are hard to prevent. Simple virus implantation can cause problems such as advertisement push. Deep-level viruses can steal computer data and even realize remote control, which brings great security risks.

2.4 Hackers and viruses

The most important factors causing computer network security problems are hackers and viruses. Hackers will invade computer networks according to their own needs, which not only destroys people's privacy and security, but also causes property loss. With the continuous development of computer technology, the current computer application is very mature, which also causes the hacker to appear younger, and the identity is very diverse, and subsequent legal supervision and arrest work is not good. The same is true of the virus problem, which can lead to a large area of computer function damage, and agglomeration contagious, causing computer shackles within the scope.

It can be seen from the above analysis that computer network security is affected by many factors, so it is difficult to prevent it. Especially for viruses and hackers, most of them are premeditated, which further increases the difficulty of network security protection and affects people's normal life and work.

3. Measures to strengthen computer network security

3.1 Protection of computer use environment

In order to reduce the impact of the natural environment on computer network security, it is necessary to strengthen the infrastructure construction of the computer use environment, such as power, network, earthquake prevention, etc., so that it can effectively improve the security and stability of computer use. In addition, in order to reduce the impact of unexpected situations on the computer network, a corresponding emergency mechanism should be set up to lock the computer after an emergency, and to protect the security of the information in the computer. At present, there is no uniform standard for the construction of server room in China. Therefore, in the subsequent improvement, this blank should be filled, unified regulations should be issued, and the construction of various types of protection should be strengthened to provide a better basic environment for the use of computer networks.

3.2 Set up the firewall

Computer firewall is an important measure to protect computer network security. It can isolate the invasion to a certain extent, and can effectively coordinate the use of computer hardware and software. Most of the current computer security problems are caused by hackers and viruses, and these are all from the network. Through the firewall technology, it can effectively control the blocking between the computer and the Internet connection, and identify the security of data information exchange. In addition, the firewall can also be personalized according to the user's needs, intercepting viruses and bad information, reducing the possibility of being hacked. Therefore, when setting up the firewall, you must fully consider the individual needs, set the firewall solution in a targeted manner, shut down the network through the firewall when the problem is discovered, and cut off the information output of the computer, effectively blocking part of the network risk. However, the firewall also has certain limitations. It cannot accurately determine the IP port. This is also a problem that needs to be continuously improved in the subsequent development.

Computer firewalls protect against most hackers and viruses, but they do not fundamentally block network security issues. In response to this phenomenon, it must be targeted when making firewall selections. Individuals, companies, governments and other departments have different needs for use, so they must be customized. For example, the enterprise's firewall is mainly to protect enterprise data and core data from leaking. Therefore, when the firewall is set up, it is more concerned with data security issues. Most companies encrypt files so that they are secure even if they are compromised, and they also set the appropriate access permissions to exclude Internet access.

3.3 Computer antivirus software

Anti-virus software plays an important role in the prevention and control of computer viruses. Therefore, in order to maintain the security of computer networks, it is necessary to improve the anti-virus system. The current anti-virus software has a variety of choices. In people's daily life, there are Jinshan drug tyrants and 360 anti-virus software. It should be noted that people should regularly use anti-virus software to detect and kill computer viruses, and set up a full-scale scan to detect vulnerabilities and viruses in time, thus reducing the possibility of virus infection and hacking. For large enterprises, even the anti-virus system will be developed independently, and the computer will be scanned regularly to strengthen the firewall and reduce the security risks of the computer network.

After the computer is infected with a network virus, there may be a problem with the system, and the anti-virus software will not work properly. However, anti-virus software is mainly used for virus prevention, and can be checked and tracked before the virus is invaded, and then effectively intercepted to protect the security of the computer network. Of course, when using computer anti-virus software, it will also be threatened by users. Many unknown links and emails are marked by anti-virus software, but customers still choose to continue browsing, which leads to virus intrusion. In addition, the anti-virus software's virus detection function is not comprehensive, mostly for existing viruses, such as the 2007 "Panda Burning Incense" virus. Because it is a completely innovative virus, it spreads rapidly across the country, causing a large number of computers. The problem. Therefore, anti-virus software should be updated regularly, and the computer should be fully scanned to minimize the hidden dangers of computer network security.

3.4 Strengthen network security management

In order to effectively protect the security of the network environment, it is necessary to strengthen the governance of the network environment, to guard against the main, severely punish all kinds of illegal and criminal activities, and purify the network environment. Therefore, the relevant departments must formulate detailed laws and regulations, severely crack down on computer intrusion, and play a warning role. In addition, professional network monitoring and evaluation can be used to strengthen the defense, and when the illegal attack is discovered, the network optimization is performed in time, and the relevant departments are used for attack tracking. In addition, we must optimize the design of computer network systems, carefully study the existing vulnerabilities and weaknesses, establish access control modules, provide first-level network protection, and then continuously detect and update, through standardization and scientific Management to improve computer network security.

3.5 Improve user awareness

Improving users' security awareness is the key to enhancing computer network security. Users should have security awareness when using the network. The settings of various accounts and passwords are as complex as possible, which can effectively reduce network attacks. In addition, not browsing unknown links and websites is an important measure to reduce virus intrusion. Therefore, the relevant departments must increase the intensity of publicity, use a variety of forms to conduct network security training, and enhance the awareness of users' network security protection. For users, the following measures can be taken to reduce network security risks:

(1) Virus killing before use of the software. Before the software is installed, the user needs to perform virus detection and killing, and initially eliminate the virus. The file download should select the official website as much as possible, which can effectively reduce the risk of virus intrusion.

(2) Firewall settings. Most of the current anti-virus software has firewall settings, users can adjust according to their own needs, do not browse the marked website and mail, can also set the access rights of data access, can also effectively improve the security of the computer network.

(3) Data backup. In order to avoid the impact of computer network security, users can back up data regularly, so that even if problems occur, the loss can be reduced. Of course, for business users. Data can also be encrypted to improve security.

3.6 Cultivation of computer network professionals

In order to improve the security management of computer networks, it is also necessary to cultivate professional talents in a targeted manner so that they can effectively solve their capabilities in the face of network intrusion. Colleges and universities can work closely with government departments to train computer network security talents and improve the level of computer network professionals through technical education. In addition, it is necessary to enhance communication and communication, provide a better learning platform, and enrich the experience of computer network talents. In the event of computer network security issues, relevant professionals need to quickly process and analyze to minimize the impact of computer network security issues. At the same time, it is necessary to strengthen the defense of computer network security and improve the difficulty of computer network intrusion. Of course, these need to be promoted by professional talents, so the relevant education and training should be improved and improved as soon as possible.

4. Conclusion

Computer networks have become an indispensable part of people's lives and work, changing people's traditional ways of working and lifestyle. However, due to the wide use of computer networks, it also increases the difficulty of computer network security. Moreover, computer network security has many influencing factors, which can be divided into hacker and virus, software problems, computer system problems, and natural problems. In response to this phenomenon, this paper proposes measures to strengthen computer network security, from the protection of computer use environment, setting up firewalls, computer anti-virus software, strengthening network security management, improving user awareness, and training of computer network professionals. Analysis, I hope to provide some reference for the prevention and optimization of computer network security in China.

Acknowledgement

Fund Project: Research on the Mode of Modern Apprenticeship Training for Computer Network Technology in Higher Vocational Education in Hubei Province in 2017 (Project No.: 591).

References

[1] Qiang Longlong. Analysis of Influencing Factors and Preventive Measures of Computer Network Security Technology [J]. Information and Computer (Theoretical Edition), 2019 (03): 206-207.

[2] Cai Zhuoxin, Guo Hui, Yan Yidan. Research on the influencing factors and preventive measures

of computer network security technology [J]. Science and Technology Innovation Guide, 2018, 15 (30): 82 + 84.

[3] Zhang Ning, Jiao Liguo. Analysis of Influencing Factors of Computer Network Security and Analysis of Effective Preventive Countermeasures [J]. Shandong Industrial Technology, 2018 (17): 143.

[4] Zhou Yafeng. Influencing factors and related preventive measures of computer network security technology [J]. Network Security Technology and Application, 2018 (02): 5+46.

[5] Qiu Xue. Analysis of Factors Affecting Information Security of Computer Network and Preventive Measures [J].Computer Fan,2017(02):26.

[6] Qin Jianhua. The current situation and preventive measures of computer information network security structure and practice [J]. Cyberspace Security, 2016, 7 (05): 94-96.