Pisco Med Publishing

Original Research Article

Research on Computer Applications Based on Management of Network Information Security Technology

Xiaofeng Ma*, Norriza Hussin

SEGI University, Kuala Lumpur 47810, Malaysia. E-mail: 599082587@qq.com

Abstract: With the rapid development of computer network, the fully opened network has greatly changed people's production and daily life and the traditional industries are no longer closed. However, there are also many network security problems. To deal with it, this article explores the computer applications based on management of network information security technology. It analyzes the main factors threatening network information security from the security problems caused by computer applications. Combining with the application practice, specific measures are put forward for reference.

Keywords: Network Information; Security Technology; Management; Computer Application

1. Introduction

While bringing convenience to the whole world, computer network causes some negative effects. These security loopholes pose a great threat to people's privacy and corporate confidential information. It is obvious that with the rapid development of information technology, the relationship between network security and people's life and financial security is getting closer and closer. Thus, the research of computer applications based on management of network information security technology has become the focus at this stage. On this basis, specific protection strategies are designed according to the corresponding factors.

2. Security problems caused by computer applications

Network information security is to ensure the normal and stable operation of the network, including protecting the data information, software and hardware systems in the network from being tampered with, destroyed or leaked[1]. The rapid development of computers has created convenient conditions for network information and data transmission, with increasing number of computer applications. However, if the security problems cannot be successfully solved, the rights and interests of users may suffer from seriously negative influence, and the hardware and software systems of computers may be damaged. At present, there is no mature management system of network information security technology in China, leaving many problems unsolved in the practical application, and further affecting the popularization of computer applications in China. Security problems in computer applications include the following aspects.

First, stealing information. The computer system itself has a certain protection function to ensure the security of information inside the application, but loopholes in the system enable criminals to steal information during information transmission or storage process. Nowa-

doi: 10.18282/jnt.v2i3.1113

days, many lawbreakers rely on intercepting customers' information or sneaking into transmission paths to steal information, which causes great losses to users and threatens security of the overall network.

Second, tampering with information. In addition to stealing information, some lawbreakers also maliciously tamper with users' information, and send it out, resulting in users sending wrong data without knowing it. Moreover, many computer applications have allowed users to change information at will with permission. Once those criminals obtain the users' permission, it will bring unimaginable consequences.

3. Main factors threatening network information security

The amount of information is rapidly increasing with a gradually expanding scope in the era of big data. There are certain hidden dangers in network information security, especially in computer applications.

First, the sharing of network resources. With the help of computer applications, the connection between data information and computer network applications is getting closer and closer, and it can be said that information is everywhere. Although it brings convenience to people, many unknown risks emerge. Even if users' information is strictly confidential, it is common for users' information to be stolen because of some potential defects in the system that a large amount of personal information is stored on the network. In severe cases, it even brings irreparable losses to the country. For instance, in March 2018, a local court heard a case of a local civil servant stealing information. The basic reason for personal data leakage is that Zhu worked in a government department where he can easily get access to citizens' information[4]. Since 2010, Zhu took advantage of his position and agreed to the request of his friends Liu and Wang to download some personal information of citizens beyond his authority. He provided the information to his friends for use, resulting in the leakage of a large number of personal data of citizens. According to statistics, Zhu provided more than 700,000 pieces of citizen personal information to Liu from April 2010 to September 2016, and more than 120,000 pieces to Wang from November 2011 to July 2016.

Second, loopholes in computers. There are many loopholes in computers themselves, which will have a negative impact on computer applications. In particular, some Trojans, viruses and hackers will attack computers with these loopholes, which will lead to information to be stolen and tampered with, resulting in incalculable losses. If enterprises' or national computers are attacked, there may be risks that commercial or state secrets will be leaked, causing enormous losses[5]. For example, an educational website in Beijing was invaded by lawbreakers. In April 2018, Zhu registered online as a member of the online shopping mall of an educational technology company in Beijing. By use of the website loophole, he entered the server background, modified the balance and started the cash withdrawal function. During the period from November 2016 to March 2017, he withdrew cash from the online mall several times, stealing more than 70,000 yuan in total.

Third, viruses in computers. Viruses, as a security risk, are born with the emergence of the network. Some potential computer viruses will be hidden in the software, data, emails, pictures and information that people download by accident. Once viruses are downloaded by the user accidentally, they will invade and capture the computer system at the first time, even destroy the firewall and attack the applications in the computer. For example, the credit card information of 40,000 consumers of a mobile phone manufacturer was stolen by unknown hackers from November 2017 to January 11, 2018. The attacker launched an attack against one of the systems and injected a malicious script into the code of the payment page so as to steal the information of credit cards input by users during payment. The malicious script can directly capture the complete information of credit cards from the consumers' browser window, including the credit card number, expiration date and security code.

4. Strategies for strengthening network information security technology management of computer applications

According to the above analysis, once computer systems are invaded, there is a great probability that information will be stolen or tampered with. Therefore, it is very important to strengthen the management of network information security technology and create a safe network environment for users.

4.1 Network information encryption technology

Encryption technology, such as encrypting databases and VPN, is the core of network security technology, which can protect personal privacy and business secrets, so as to fundamentally guarantee computer network security. Security systems of C1 and C2 levels are mainly used in computer systems, which only play a very limited role, and are the first choice for many hackers. If the security level cannot be changed, it is better to adopt encryption technology and set special access rights so as to ensure the security of network information. For instance, some cross-regional enterprises not only set up restrictive LAN, but also use routers for encryption protection. The internal information of these enterprises will become digital gibberish when it is transmitted to the external data, so that the information can be secured[6]. The following code is a common information encryption algorithm.

```
import binascii
from Cryptodome.PublicKey import RSA
from Cryptodome.Cipher import PKCS1_v1_5

class RsaCrypto():
    ’’’RSA encryption and decryption’’’

    def create_rsa_key(self):
        ’’’generate RSA key pair’’’
        try:
            key = RSA.generate(2048)
            encrypted_key = key.exportKey(pkcs=8)

            public_key = key.publickey().exportKey().decode(’utf-8’)
            private_key = encrypted_key.decode(’utf-8’)

            return {’state’: 1, ’message’: {’public_key’: public_key, ’private_key’: private_key}}
        except Exception as err:
            return {’state’: 0, ’message’: str(err)}

    def encrypt(self, public_key, plaintext):
        ’’’encryption method’’’
        try:
            recipient_key = RSA.import_key(public_key)
            cipher_rsa = PKCS1_v1_5.new(recipient_key)

            en_data = cipher_rsa.encrypt(plaintext.encode(’utf-8’))
            hex_data = binascii.hexlify(en_data).decode(’utf-8’)

            return {’state’: 1, ’message’: hex_data}
        except Exception as err:
            return {’state’: 0, ’message’: str(err)}

    def decrypt(self, private_key, hex_data):
        ’’’decryption method’’’
        try:
            private_key = RSA.import_key(private_key)
            cipher_rsa = PKCS1_v1_5.new(private_key)

            en_data = binascii.unhexlify(hex_data.encode(’utf-8’))
            data = cipher_rsa.decrypt(en_data, None).decode(’utf-8’)

            return {’state’: 1, ’message’: data}
        except Exception as err:
            return {’state’: 0, ’message’: str(err)}

if __name__ == ’__main__’:
    print(RsaCrypto().create_rsa_key())
```

4.2 Network firewall technology

Firewall technology, the most basic security means, can prevent and filter harmful information from entering the system by detecting the information transmitted into the computer. However, the traditional firewall technology can no longer meet the needs of the current system development. In particular, it can no longer prevent data-driven attacks. Although it can complete the detection through pre-designed programs, viruses and harmful information may still enter the system by using other loopholes. Therefore, firewall technology should be combined with virus protection technology, VPN or NAT technologies to achieve comprehensive protection, so that the security performance of firewall technology can be truly improved. Meanwhile, the traditional firewall technology should be updated. At present, the firewall technology can not only serve as the connection between computer and network, but also reflect the status of network information. It can ensure the quality of network security prevention and control work to the greatest extent, shield unsafe websites in time and protect personal privacy data.

4.3 Network anti-virus technology

Virus is an important factor threatening network information security, so it is necessary to optimize the configuration of computer system regularly and strengthen the network anti-virus technology comprehensively. Anti-virus technology is mainly aimed at protecting software and hardware of computer applications. The level of science and technology has been continuously improved in recent years, together with the update of protection means, such as the continually increasing types of anti-virus software on the market. However, the types and manifestations of viruses have also changed. There are many hidden viruses, which are difficult to be found, virtually attacking system loopholes, invading systems and tampering with information. Taking Boot kit/Root kit virus as an example, it randomizes its file name to avoid being detected and killed by software. In 2018, the computer manager disclosed the strong countermeasure of this virus, that it blocked the killing of anti-virus software by restarting the computer violently. Then the computer manager further updated the killing method to fight against the strong countermeasure of this virus. Anti-virus means should be constantly upgraded in the actual development process to deal with the changes of viruses. This requires users to regularly update the virus database of anti-virus software, and regularly carry out virus detection on computer systems, especially on programs and software and hardware areas vulnerable to virus attacks, so as to fundamentally avoid risks[7].

4.4 Network anti-counterfeiting technology

Network anti-counterfeiting technology, also as identity authentication technology, is to prevent criminals from tampering with or attacking the system by using users’ identity[2]. The common identity authentication technologies at present include fingerprint recognition, iris recognition, face recognition and signature recognition, most of which cannot be copied and are of high security. However, due to high cost, some identification technologies are difficult to be popularized, and are only applied in a small range. Currently, the most common authentication technology is the public key cryptosystem of certificate type, which cooperates with the hierarchical system to minimize the risk of information leakage. For example, an enterprise backs up important data and sets up an identity verification program. If the identity is wrongly verified more than three times, the important data will be destroyed from the computer immediately, and the corresponding user account will be frozen immediately, so that the data security can be protected to the greatest extent[8].

4.5 Network anti-intrusion technology

In addition to the above aspects, network anti-intrusion technology is also common in computer applications, which can prevent criminals from invading computers from the source to ensure the security of computer systems. This technology can be divided into three parts, namely, information collection, information analysis and result processing. By collecting and calculating the information of each link, it can detect harmful behaviors of the system, and carry out effective measures to prevent them from entering the system. Information in computer applications, such as security log, behavior and audit data, can provide reference, among which protocol analysis and behavior analysis are of the highest accuracy. Protocol analysis is the most common one, which uses data packets to analyze structured protocols and can also judge some unknown attack characteristics. Compared with protocol analysis, behavior analysis is more aimed at attack behaviors, such as attack to the system data area, file area and memory area. Once these behaviors are identified, the system will interfere with the equipment immediately[3]. An example is that when anti-intrusion technology detects an abnormality, it will immediately start the firewall and other protection systems; at the same time, it will send a pop-up window on the computer screen to remind users and intelligently help users shield the risks to a certain degree so that users can enjoy the convenience brought by computer applications in a safe environment.

5. Conclusion

The rapid development of the Internet industry has gradually expanded the scope of computer applications. Information security technology is the foundation of the era of big data and must be taken seriously. According to the analysis of computer applications based on the management of network information security technology, this article proposes that in order to fundamentally solve the network information security problems, it is necessary to do a good job in network security protection, implement firewall and other virus prevention technologies, thus effectively avoiding the risks brought by network loopholes, and creating a safe and healthy network environment.

References

1. Yu M, Cha Z, Zhan W, *et al.* Research on the computer applications based on management of network information security technology (in Chinese). Electronics World 2020; (13): 188–189.
2. Zhan P. Computer applications based on management of network information security technology (in Chinese). Electronics World 2020; (11): 5–6.
3. Yang S. Computer applications based on management of network information security technology (in Chinese). Computer Products and Circulation 2020; (6): 38.
4. Mo Z. Research on computer applications under the management of network information security technology (in Chinese). Technology Wind 2017; (11): 99.
5. Sun M, Cai C. Computer applications based on management of network information security technology (in Chinese). Telecom World 2017; (10): 122.
6. Wang Z, Chen J, Wang S. On Computer applications based on management of network information security technology (in Chinese). Network Security Technology & Application 2017; (4): 1+6.
7. Su X, Tang H. Computer applications based on management of network information security technology (in Chinese). PC Fan 2017; (4): 137.
8. Mao X. On Computer applications based on management of network information security technology (in Chinese). Keji Jingji Shichang 2017; (4): 40–41+107.