Analysis on Computer Application of under the Management of Network Information Security Technology

Chu Xue

Qilu Normal University, Jinan, Shandong

Keywords: network information; security technology management; computer application

Abstract: With the rapid development of the economy, the development of science and technology in China is becoming more and more rapid. Network information technology is spreading and has penetrated into people's daily life. No matter whether it is work or life, it is inseparable from the network. People get information through the network, complete daily communication, life shopping, etc., but the large-scale application of network information technology also makes people's information appear exposed. There are many hackers and lawless people who use network information technology to obtain personal information and economic information, which leads to people's property safety and personal safety being threatened. To this end, they want to give the people a comfortable living atmosphere. The excellent network environment needs to ensure network information. The use of technology is safe.

1. Introduction

The emergence of Internet computer technology has brought about tremendous changes in people's lives. The emergence of the era of big data has made information exchange more convenient, but it has become more insecure. When people use network information technology to complete their work, they need to input relevant information, which brings convenience to many unscrupulous people. They use network information technology to steal information for sale, which not only restricts the development of network information technology, but also gives People's lives bring a lot of uneasy factors, which makes people feel full of crisis in the process of applying network information technology. In order to ensure the positive development of China's network information technology, the security of the current network environment has become the top priority of the relevant departments. This paper mainly analyzes this point.

2. The role of network information security technology management

2.1 Keep your computer safe

Because the current demand for computer networks is increasing day by day, if the computers used by people at this stage are still in the same way as the traditional computers, then in the event of power outages and system failures, all the information in the computer will be lost. This is a very unacceptable thing for people who survive in the era of big data. Not only that, but problems caused by unstable voltages in the network can also pose a threat to information security. To this end, in the current network information security, relevant technical personnel send related information to the network port in order to ensure the security of the network information, thereby avoiding information loss and information damage caused by the failure of the computer itself. People must realize that in the era of big data, to ensure the importance of network information security for people's life and work development, in the process of daily application of computer network, it is necessary to start from itself, improve the awareness of network information security, and not give it to exist. Any opportunity for criminals to make it difficult for criminals to find loopholes to steal information and truly guarantee the safety of computer users.

  DOI: 10.25236/iwmecs.2019.038

2.2 Fix vulnerabilities in the system

Since the computers currently on the market are relatively diverse in terms of types and systems used by computers, the emergence of this phenomenon has also led to the need for different computer systems in the management of network information security. The problems faced are different. Technical personnel responsible for network information security management are required to make network information security management according to different systems, different problems and different vulnerabilities, and take targeted solutions to ensure the security of computer users' network information. However, there is a very serious problem in computer applications. Many software companies will leave a back door in the software in order to ensure their own operation. The meaning of this back door is to help the relevant operators to better update the software. However, once the criminals discover this backdoor, it will have a very bad impact on the security of computer users' network information, such as the current Microsoft system, UNI network information technology, etc., in order to truly ensure the security of computer users' network information, The relevant technical personnel are required to solve the problem in time and repair the problem to ensure that the network information security of the computer can be guaranteed during the actual use.

2.3 Defense against hacking

Hacking is one of the biggest problems in the security management of computer network information in China. Many hackers will enter the computer to steal computer user information through improper channels, which will not only bring losses to computer users, but also damage computer systems. . In the market, it is not uncommon to use hacker technology to steal confidential information. Whether it is a business or an individual, the economic loss caused by the invasion of hackers is very serious. To do this is one of the top tasks of the relevant departments. Strengthening the management of network information security and increasing the importance attached to network information security can truly guarantee the security of computer users.

3. Analysis of Computer Application Strategy Based on Network Information Security Technology Management

3.1 Application of firewall technology

From the analysis of current network information security technology management, it is found that the most widely used network information security protection technology is firewall technology. In the process of using this technology, it mainly targets various insecure factors existing in the network. The firewall technology inside the computer can form a barrier in the computer network, thereby effectively preventing the external network from being accessed by the computer without authorization from the computer user. In the application of actual computer network technology, the use of firewall technology can effectively prevent the occurrence of unlawful analysis of the use of illegal intrusion to steal computer user information and other related events, to maximize the security of computer network technology. The use of firewall technology in ensuring network information security can adopt different security control methods such as proxy service, state detection, etc., to ensure that the internal information of the computer used by the computer user is in a closed state, that is, a person other than the computer user. It is difficult to obtain relevant information through network technology, and the purpose of strengthening the internal information security level of the computer is achieved. In order to ensure the convenience of the computer users, in the process of actually applying the firewall technology, the internal working information can be opened inside the computer according to the requirements, so that the computer user can find and use the information, and the application of the network information security technology is ensured.

3.2 Application of authentication technology

Different from firewall technology, one of the most frequently used network information security technologies in the process of using computer network technology is identity authentication

technology. This is a new type of network information security protection technology. With this method, computers can be effective. Determine if the operator is a computer user. The authentication technology mainly uses a special identification technology to identify the computer operator. This is a specific identification method that is completed beforehand. The computer uses this identification method to judge whether the operator has its own use. Computer permissions. By using the identification of the operator's identity, the basic requirements for identity verification are compared with the data contained in the computer itself, and the operator can use the computer only after ensuring the accuracy of all the information. The most important of this kind of network information security technology is the accuracy and validity of all parameters. Applying this method to ensure the security of network information not only reflects the trust verification mechanism contained between the computer user and the computer, but also guarantees Network information security. Different from other network information security technologies, because the authentication technology adopts a one-to-one processing method, it has a very strong pertinence in use, which can largely avoid the problem of network information security and avoid Bad violations of network information, such as illegal user intrusions and malicious attacks. For computer users, application authentication technology can effectively prevent network information leakage. In the current process of using authentication technology, the main manifestation forms are computer users' own biometrics, trust objects and information secrets, etc. The information that the user knows and understands, and the most practical function in the verification of these information, and the highest safety factor is the biological feature, which is difficult to change and imitate, and the effect is also the best in practical applications, but in the application of biological One of the biggest drawbacks of the feature is that current science and technology have not universalized this approach. The cost of applying this approach is relatively high, and the operating system is relatively complex, causing most of the current The authentication technology used by computer users is still based on information secrets.

3.3 Antivirus technology application

In order to ensure the security of network information, it is necessary to install anti-virus software on the computer. This is the reason that many computer users know. When using computer network technology, the anti-virus software already installed in the computer is used to prevent illegal intrusion. One of the most common ways of managing network information security. Anti-virus technology itself is a hardware technology, which cooperates with the operating system of the computer to prevent the vulnerability of the webpage from being invaded, thereby causing the virus to appear on the computer. At the same time, the anti-virus technology can also periodically detect the computer itself. Security situation. In the current application of anti-virus technology, it mainly includes the following methods: virus prevention technology, virus detection technology and virus removal technology. The so-called virus prevention technology in computer network technology refers to the prevention of computer infection by illegally invading the computer by means of technical means in the actual network information security management, and preventing the operating system in the computer from being destroyed. Its practicality is relatively strong. The virus detection technology used in network information security refers to the use of information technology to identify computer viruses, in order to determine whether there is a virus in the system. Once the system determines that the virus is contained in the computer, it will be selected according to the type of virus present. Solution solution. In practical applications, this technology can be mainly divided into two types: the first type is the basic program for installing virus detection in a computer, that is to say, the program of the virus is tested, and the characteristics and key points existing in the virus are The words and the fixed program content are detected together. Once the virus that meets the requirements is detected, it will be automatically cleared. If this type is used, the computer virus detection technology needs to be updated regularly to ensure that the computer can do all the common viruses. Good correlation prevention; the second type is completely different from the first type. This method is to detect and save a certain data segment or information common in the computer, and calculate the existing information. Save the results after completion. Regularly or irregularly check and compare the saved data during the running of the computer. If the

information is found to be inconsistent, it can be defined as the computer being infected by the virus. The network information security management technology in the computer will automatically find it. Effective solution and complete virus removal. When using anti-virus technology to ensure network information security, relevant software producers are required to periodically update the software to ensure that the software can detect the virus existing in the computer in time and clear it. At the same time, it is necessary to remind the computer user when downloading the software. Computer users regularly update anti-virus software to ensure the security of network information. Only when the computer users' awareness of network information security is improved, can all kinds of problems in network information security be fundamentally solved.

3.4 Application of intrusion detection technology

In the security management of network information, many computer users choose intrusion detection technology. This is also a management method commonly used in the completion of network information security management. Its own effect is relatively good, to a certain extent, it can meet the current needs of people for network information security. In the process of actual operation, the security of the computer can be ensured by analyzing and calculating the internal information of the computer. In the process of operating the computer, the intrusion detection technology of the computer user can determine whether the computer has an abnormal item by analyzing various indicators in the computer, which mainly includes the audit data, the security log, and the abnormal operation behavior of the computer user. In turn, to determine whether the computer has an intrusion. In the application of intrusion detection technology, it is mainly divided into two detection modes to ensure the security of computer users' network information, which are misuse detection mode and abnormal detection mode. Once the intrusion detection technology detects the intrusion behavior of the computer in the computer operation A corresponding alarm signal will be sent to inform the computer user and to ensure the security of the network information to the utmost extent. However, the basis for the intrusion detection technology to be successfully implemented is to establish an intrusion detection system in the computer. The so-called intrusion detection system itself is composed of corresponding software. And the hardware is composed, the purpose is to detect whether there is a virus in the computer network used by the computer user, and to ensure the security of the network information. In the current network information security management, the intrusion detection technology itself has very important practical significance.

4. Conclusion

In summary, in order to ensure the security of network information technology, network information security management technology and computer management technology can be coordinated in use, and the security problems existing in the use of network information technology by computer users can be reduced as much as possible to ensure The safety of all computer users and their own rights. However, in order to truly provide a safe network environment for all computer users, it is also necessary for computer users to improve their own network security awareness, to protect themselves from being exposed, and not to disclose their information insecurely. Above the website. As a network information security management technician, it is also necessary to continuously improve the software related to network security detection in the computer, improve the network information security defense system, and ensure that people's information is not leaked out at will.

References

[1] Jing Yan. Computer application analysis based on network information security technology management [J]. Ship Vocational Education, 2018, 6 (06): 67-69.

[2] Li Yajun, Hou Guangxue, Shi Shaohua. Computer Application under the Management of Network Information Security Technology[J]. Information and Computer (Theoretical Edition), 2015(13): 115-116.