Pisco Med Publishing

Original Research Article

Network Security Protection in Computer Application

Quan Liu

Information Network Center, China University of Geosciences (Beijing), Beijing 100083, China

Abstract: In today's information age, people rely more and more on computer networks.But the network security of computers is still likely to expose users' personal information, which is likely to cause economic losses, and even affect corporate and national development.Therefore, with the development of The Times, it becomes more and more important to take network security measures combined with the actual situation of computer application.Computer technicians should strengthen the analysis of computer network security problems, help people to solve the problem of data and personal information leakage in the network environment, and formulate perfect solutions according to the specific situation.This article discusses the network security protection in computer application.

Keywords: Computer Application; Network Security; Protection

Introduction

In the Internet era, people's life, work and research are always conducted on the Internet, and network security has become the focus of social attention.Computer network security not only affects people's lives, but also has a certain impact on the development of enterprises.In complex network environments, network security problems are constantly changing, and network security includes internal and external factors.Some network security problems are caused by improper user operation, to improve the users' intention of network security.Secondly, the network security technology is constantly updated and improved, to formulate the corresponding adjustment plan according to the actual situation, improve the existing network system, pay attention to the computer network security problems, and strictly implement the relevant preventive measures.

1. The characteristics of computer network security threat

In today's information age, the diversification of the network data has promoted the diversification of the network security problems, and has brought certain problems to the network security.This network threat exists to the openness of the computer network.Computer network security threat characteristics are: (1) infectivity and sudden.A computer is usually used to connect to the network, but during normal operations, such as opening a web page, the computer is leaked without warning.If there is no rapid reaction time, after the computer infects the virus, the entire LAN computer infects other computers.(2) Lurency and concealment. Nowadays, cybersecurity issues are not traditional attack patterns.If a computer is infected with a virus, the abnormality can usually not be detected immediately.Due to the diversity of the Internet, network operation supervision can not fully grasp the theft of information, encroachment on accounts, virus viruses and other situations.To realize the security of the network operation, we must strengthen the management and early warning.

2. Factors affecting the computer network security technology

In the era of the Internet and big data, the Internet has become an important part of production and life.Paperless office business has become the mainstream, and electronic products are being used more and more frequently.While enjoying the convenience brought by the Internet, users are often subjected to external attacks.First, phishing.Phishing refers to users disguised as a source bank or government agency to send spam to users to obtain relevant information.This network security problem is partly hidden, and it is difficult for users to accurately identify.The user did not know that the information leakage caused serious consequences.Second, hacking.With the rapid development of science and technology, hacking is the main factor causing the computer network security threat.Currently, hackers destroy computer network information in a variety of ways.As the computer network runs, the hacking attack is directed against infected computers.When the computer runs, hackers will steal and intercept network information, which will seriously affect user interests.Hackers undermine the integrity of user data through a series of means, preventing users from using computer systems or their own data as usual.Or when the user uses the computer, input the account number, password, personal information, data transmission, etc., there is a danger of information leakage.However, as computer users, they are unable to accurately identify dangerous information sources, which is a reflection of external attacks.[1]

3. Prevention method of computer network security technology

3.1 Strengthen the level of security management of computer network users

Copyright © 2021 Quan Liu

doi: 10.18282/l-e.v10i6.2837

This is an open-access article distributed under the terms of the Creative Commons Attribution Non-Commercial License (http://creativecommons.org/licenses/by-nc/4.0/), which permits unrestricted non-commercial use, distribution, and reproduction in any medium, provided the original work is properly cited.

Computer network security must first strengthen self-supervision; in addition, preventive work must be done at the system supervision level. In the process of computer application, clarifying individual rights and restricting the operation of relevant personnel can effectively prevent threats to network security. Relevant personnel must strengthen network supervision, check regularly, and use anti-virus software to clear files and data. Plus, almost every user has their own email account and online banking account. The user must pay attention to the complexity of the chosen password, when setting up the account, avoid the problem of the same password for the account, and must use numbers, characters, punctuation, capitalization, etc. to combine, instead of selecting numbers and characters individually, and changing the password within time Otherwise, password leakage will lead to hackers stealing the user's entire account, which cannot ensure computer network security and user network information security. Finally, don't touch suspicious websites to prevent "phishing" from stealing information from websites. [2]

3.2 Improve the computer system and repair the loopholes

The main management measure in the security management of computer network software is usually to improve the computer system and repair the vulnerabilities.Scientific identification and prevention of risk computer network access rights, to avoid the network security problems caused by non-compliance with the law operation.Therefore, to ensure the network security of computer applications, network administrators must adopt a network access verification program combining the real-name registration system, verification code, and image verification.In addition, in order to ensure the safety of the computer, the safety inspection of the hardware equipment must be strengthened.For example, in computer chip detection and design, the hardware can be protected by setting a key and using secure password verification methods to ensure the security of the hardware features.Meanwhile, some systems need to be improved.For example, if information leakage, replication, or tampering occurs, the system can automatically exit the operation to ensure the user's information security.In addition, during the software development and design stage, designers must pay attention to software security detection, regular scanning, vulnerability discovery, and timely repair.In addition, user confidentiality must be noted when using the software.When logging in and using the software, specific authentication thresholds can be set to prevent others from logging into the software without copying and stealing user personal information without permission to maximize the security of the information of the computer.

3.3 Install a firewall to effectively prevent external attacks

Viruses will be included in big data systems, through data mining to find anti-virus methods, to avoid illegal invasion, and to ensure the security of network information.Among the many network security problems, the enterprise computer network security has the biggest impact.For many enterprises, not only need to build databases, but also computer information security management systems are constantly improving.Only by strengthening the implementation of the management system can we continuously improve the understanding and ability of the computer network security.As the era of big data evolves, many computer users use firewall and security systems technologies to eliminate malware operations, minimizing malware and virus threats.The application of firewall technology plays a very important role in the public Internet environment, enterprise and network security.Firewall technology mainly separates internal data information and external data information to ensure the relatively high security factors of internal data information structure.Prevent the firewall on the computer network, you can find the computer network vulnerabilities within a certain period of time [3]

4. Concluding remarks

In short, scientific and effective network security prevention is the basis of ensuring the safe operation of the computer network.A large number of investigations show that the root cause of many network security problems is that in the computer application process, users do not have enough network security defense ability, did not take the correct network security measures, and affect the operating status of the entire computer network.In addition, the lack of scientific and reasonable network security measures does not help in the normal operation of the computer network.People need to store, share, and send a lot of information through the network, and computer network security issues urgently need their attention.Therefore, it is very important for enterprises and individuals to protect the network security. We must analyze the network security technology in computer applications and study countermeasures to do a basic job for purifying the network environment.

References:

[1] Li Yanan.Computer network security problem and its preventive countermeasures [J].Information and Computer (Theory Edition), 2020,32 (13): 208-209.

[2] Zou Yang.The Application of Computer Network Security Technology in Network Security Maintenance [J].Shandong Industrial Technology, 2019 (4): 143.

[3] Xu Lei. Research on network security prevention strategies in computer applications [J]. Business Conditions, 2020, 000(017): 104.

About the Author:

Quan Liu (1965.12-), male, Han nationality, born in Shaoyang, Hunan, graduate degree, engineer, research direction: computer application technology/network security/network room construction.