Pisco Med Publishing

Original Research Article

Analysis of Computer Network Security Issues in Cloud Computing Environment

Zhou Fan

Lanzhou Resources&Environment Voc-Tech College, Lanzhou 730000, Gansu, China.

Abstract: Aiming at the computer network security issues in the cloud computing environment, this article outlines the great prospects of cloud computing technology and its significance, and respectively dissects the hidden dangers of computer network security problems under the use of cloud computing and the corresponding solutions. Computer network security issues in computing contribute to the smooth and long-term development of computer network security.

Keywords: Cloud Computing; Computer Network; Network Security; Prevention

1. The prospect of "cloud computing" and its security significance

In the information age, everyone has to deal with information, making computer network security problems increasingly serious. As a key topic and an important way to promote the development of network security, computer network security in the cloud computing environment has gradually been put on the topic of the discussion.

Simply speaking, computer network security in the cloud computing environment can ensure that users reduce the risk of data loss or leakage when using computer data sharing. Although the security of computer hardware and software technology has been correspondingly guaranteed, the openness inherent in the Internet network will make computer network security problems face huge challenges at any time. For this problem, people's first task is to analyze and solve the problems in computer network security and eliminate hidden dangers of computer network security in the cloud computing environment.

2. Computer network security problems in the cloud computing environment

2.1 Computer virus

For ordinary people, the network security problem that is bigger than hacker attacks is undoubtedly the infection of computer viruses, which not only reduces the efficiency of the system, but also seriously damages the computer settings. Among them, the Trojan horse virus in the network virus is one of the typical ones. This virus that exists in the running program will not be detected by the host and router even if it is run. Instead, it will actively modify the host address and attach to the computer without knowing it to block the LAN and block the network.

2.2 Hacking

As a huge repository of network information, cloud computing will undoubtedly become one of the main choices for hackers using computer technology to invade users' systems and change or steal personal information. This behavior seriously endangers the security of computer networks in the cloud computing environment.

2.3 Security issues within the cloud computing

Although it is rigidly regulated that every service company is prohibited to disclose customer personal information,

Copyright © 2020 Zhou Fan

doi: 10.18282/le.v9i6.1297

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.

the openness of the network still exposes information security to certain risks. Criminals use this gap to steal corporate information during information transmission. On the other hand, some staff within the company did not perform the principle of confidentiality of customer information well, and did not pay attention to it, and did not take it seriously, resulting in leakage of customer information and loss of privacy.

2.4 Cloud computing network technology security issues

For computer network security issues in the cloud computing environment, the technology will also become one of the hidden dangers. First of all, because everyone's life is closely related to cloud computing, people have a great dependence on cloud computing, and they are in a passive position in the relationship. Secondly, the IP protocol is a double-sided knife, which will benefit the research of core technology and also become the focus of leaking customer information. Finally, computer network security issues in the cloud computing environment are mainly manifested in websites and keywords.

3. Measures to solve computer network security problems in cloud computing environments

3.1 Computer virus protection technology

If a virus invades a running computer network, it will affect the normal work and life. The best way to prevent this is to prevent it before it happens. Use computer virus protection technology to perform regular, habitual and timely virus detection on the computer. Virus blocking is excluded from the computer. The specific steps to apply computer virus protection technology are as follows. First, install network antivirus software. The current anti-virus software is mainly after manual scanning and detection, and then destroying the virus. This makes the anti-virus too random and not timely. It is needed to give full play to the subjective initiative of the computer host. Without the need for the host to set up, the anti-virus software should be able to scan independently anytime and anywhere, to eliminate the virus as soon as possible. Secondly, for typical stubborn viruses such as Trojan horses and worms, it is necessary to use corresponding network fault detection software to troubleshoot host viruses. It is a must to have vigilant and agile thinking, and when the system network is not operating normally, it requires immediate virus scan to remove the virus.

3.2 Computer vulnerability scanning technology

Vulnerability technology is one of the common technical methods in network security prevention methods. First, the computer autonomously detects the local host and remote host in the local area network, queries the main channels through the service port of the TCP/CP protocol, and records the response of the host, and then processes them to ensure the processing and collection of data information. From the actual operating situation, vulnerability scanning technology can play a better role. Vulnerability scanning technology is mainly used for program security issues, filtering out the vulnerabilities and weaknesses that cause security risks to computer network security in a short time, and outputting the format of its operating system.

3.3 Firewall technology

Firewall technology is the most common method of computer network security protection. Firewall technology is divided into state detection technology and Web intelligence technology. The former needs to refer to the OSI working standards, namely the Network.ork and Data layers. During the operation, ensure that the data packets in the system kernel are run, check the network layer time and check the data link layer. the latter will generate the state of the conversion process during application Table, details the connection between the detection engine and the data packet, and process the non-protocol content according to the relevant intelligent standards. Before the server accepts the data, it sends a client request, and responds quickly under the port opening to ensure system security.

3.4 Network access control technology

Setting up network access control technology on the computer can reduce the risk of network security risks. Network access control technology refers to setting up user access restrictions first to ensure computer network security without the user's permission. Network access control technology can be regarded as a commonly used technology in computer network security maintenance. It can avoid computer failures caused by users' unreasonable operations. It mainly

controls network access content such as attribute control and Internet access control. The application of network access control technology can protect computer network security in the cloud computing environment.

3.5 Improve user awareness of network security

Eliminating and reducing computer network security issues should not only be reflected in the technical level, but also rooted in people's deep-seated consciousness. In today's era, everyone is inseparable from the network. Everyone trusts and relies on the network. That's why cultivating awareness of network security is important. The strengthening of computer network management capabilities and protection means is not only the right of every user to use the network and information security, but also the obligation of every user. Users should reduce or even eliminate the login of personal information on public networks or computers, ensure the complexity of passwords, regularly organize backup data information, and avoid the situation of data information loss due to unprovoked failure of the cloud computing services. The user's inner recognition of network security protection is one of the prerequisites for ensuring the realization of network security, and it is also one of the basic guarantees to prevent hackers from intruding. Furthermore, we must promote the implementation of computer network security precautions and guide users to form a good computer network security awareness, to ensure the confidentiality of personal information and the effective improvement of computer network security from the perspective of customers.

4. Conclusion

The current computer network is a contradiction, which brings us convenience on the one hand, and risks on the other. We should start with improving technical pertinence, effectiveness and increasing awareness of prevention to ensure the security of information storage and transmission in the cloud computing environment. For the long-term development of computer technology, it is also possible to formulate a complete set of network security response mechanisms to deal with the endless security risks that emerge with the development of technology. In addition to the security issues we have discovered and contained as mentioned above, there are still many hidden dangers in computer network security in the cloud computing environment. It can be seen that the research and application of computer network security issues are becoming more and more serious and should be put on the agenda as soon as possible. The rapid development of science and technology has brought great convenience to our lives, but we must remember not to pull the seedlings to promote, but step by step build a foundation steadily to eliminate hidden dangers.

References

1. Huang Z. Discussion on the security management technology of the computer network database. Science and Technology Innovation and Application 2020; (23):193-194.
2. Wang Y. Computer network security and preventive measures in the era of big data. Heilongjiang Science 2020; 11(14): 126-127.
3. Wu T. Application analysis of preventive measures for computer network security problems. Network Security Technology and Application 2020; (07): 2-3.
4. Wang G. Research on cloud computing-oriented computer laboratory network security technology. Communication World 2020; 27(07): 101-102.
5. Huang X. On the computer network security strategy in the cloud computing environment under the background of the new era. Chinese Journal of Multimedia and Network Education (Mid-term) 2020; (07): 182-183.
6. Sun C, Wu L, Ning Q, et al. Research on information security and protection strategy based on cloud computing. Journal of Jiangsu Vocational and Technical College of Economics and Trade 2020; (03): 50-52.