Construction of Computer Network Security Model Based on Virtual Technology

Dawe Gui

School of Information and Intelligent Technology, Shaanxi radio and Television University, Xian, Shaanxi, 710119, China

guidw@163.com

Keywords: Virtual Technology, Computer, Network Security, Mode.

Abstract: In recent years, the virtual technology of our country has made great progress, which plays a very important role in the construction of computer network security mode. Based on this, this paper briefly expounds the current situation of computer network security in our country, and puts forward the construction strategy of computer network security mode based on virtual technology from the aspects of creating the basis of information sharing in the remote branch of users, the application of MPLS virtual network, the construction method of authentication technology, the establishment of firewall in user and remote network control and the development mode of virtual technology in computer network security respectively.

1. Computer Network Security

In the information age, people mainly use the computer to browse the network to obtain the required data information. In recent years, the rapid development of our country's network technology and computer technology, the emergence of a number of new technologies to provide great convenience for people's lives, but in this process, the use of computers has certain security risks, a little attention will lead to the disclosure of user information, resulting in serious adverse effects, which need to be dealt with urgently.

1.1. Security Status of Hardware

The hardware problem of the computer network can easily affect the security of the network. In general, the hardware of the computer mainly includes the host computer, the network setting and the related lines, etc. It can be said that the network hardware of the computer determines the smooth operation of the computer network, and it can guarantee the smooth operation of the network system. By sorting out and analyzing the relevant data, it can be found that the hardware failure of computer network is mainly electronic radiation, and if it produces electronic radiation, it will face the risk of hacking, which will lead to the rapid disclosure of data information in a short time, and then affect the security of computer operation.[1]

1.2. Software Security Status

For the computer, software is its soul and connotation, if the lack of software will make the computer in a tangible state, so, in the design of software and development of engineering, how to improve its stability and security function is the focus of attention, figure 1 is the computer software development schematic. Moreover, software problems are also the main cause of frequent computer security problems. First, in the design or development of the relevant software, the relevant staff failed to understand the security concept and preventive measures, failed to seriously analyze the impact of software design on the security of computer network, lack of objective consideration, resulting in software after the development may appear vulnerabilities, in the future operation of the computer, vulnerable to virus entry. Second, the quality of computer software is not high, in the software development and research stage to reflect one-sided and formalized problems, will lead to a wide range of user information leakage, seriously damage the user's personal hidden. Third, the method of using software is not standardized, in the use of software, failed to carefully consider the

surrounding network environment, wanton operation, in the use of software reflects a certain degree of blindness, can not grasp the software malpractice and existing problems in time, easy to leave security risks[2].
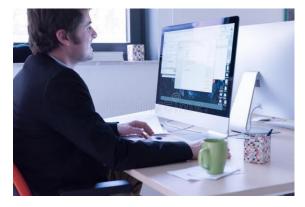

Figure 1 Computer software development

1.3. The Security Status of System Operation

The operating system of the computer is the bridge between the computer and the user, and the operating system can use the computer to carry out the corresponding operation in a relatively short time. Computer operating system has a certain lag, which is also the main cause of network security. In recent years, the software program and application technology of the computer have been improved, and the operating system has been innovated and developed. Nowadays, the big data technology and the Android system of the mobile phone have a serious impact on the operating system of the computer, which indicates that the operating system of the computer is not stable. After careful analysis, it is not difficult to see that the computer system still has problems such as low effectiveness, slow update speed and so on, network security and computer vulnerabilities occur from time to time, hackers or lawbreakers can access the computer through the system vulnerabilities, illegal access to relevant data information, resulting in the computer system facing a crash.

2. Computer Network Security Model Construction Strategy Based on Virtual Technology

2.1. Create a Basis for Information Sharing in the Remote Branch of the User

In order to ensure that the users can share the resources in the network information, the network security of the computer can be regarded as the basis, and the security of the local area network of the user can be stabilized. In this mode, users can use LAN in the virtual network, and this mode can also realize the virtual operation of international network. Using the hardware virtual technology in the virtual network, it can start the basic setting of the network security, and the application of the encryption technology can establish multiple protection for the encryption key, which can improve the practical application effect of the computer network security, as shown in figure 2.

Figure 2 Set the key to secure the computer network

2.2. Application of Mpls Virtual Network

MPLS technology can be applied in the process of IP network construction of virtual network. On the one hand, the application of this technology can realize the remote transmission of data, on the other hand, it can perfect the language of computer, and show the reliability and warm star of MPLS virtual network. When constructing the virtual network, the PE router can be loaded into the network data to maintain the stability of the CE device network connection. During this period, it is also necessary to strengthen the weight of the CE device identification code. in order to realize the effective connection and transmission of the pe router, we can use the ldp protocol to mark out the different data, and then record the flow of the whole work in detail, ensure the timeliness of the creation of the vft worksheet, and then feedback the obtained data back to the ce device, which is beneficial to further improve the stability and security of the network.

2.3. The Construction Method of Authentication Technology

The transmission environment of information data is mostly public network environment, in order to ensure the reliability of information transmission, authentication technology must be applied to VPI, in order to realize the authentication function of VPI, we need to rely on the branch of ESP protocol, AH protocol and IKEA protocol. In these protocols, AH is mainly used to authenticate the methods used to record the validity and reliability of the information. In the application protocol segment, the protocol must be authenticated, as shown in Figure 3, and the protocol can be placed in the packet. The encryption service can be targeted to achieve the addition of specific parts. In general, encrypted IP packets can ensure the effectiveness of the load, so they do not need to be encrypted data packets, can be applied separately, and the use of both AH and encrypted IP packets is the most critical method in this process, which involves a lot of content, such as the transmission form of the upper layer, the protocol way of information and the authentication of ESP, etc. The security verification of both sides of the communication can be accomplished by the key switching of IKE[3].

Figure 3 Identity authentication

2.4. Firewalls in User and Remote Network Control

The mobile network can only be operated after entering the user's interior. Using the virtual network technology can help the user to set up the firewall in the virtual network. In order to achieve this effect, it is necessary to log in to the internal network and log in directly after confirming the security. In different network environments, VNT can make the virtual network obtain firewall function in the process of information transmission and collection, ensure the security of information transmission, but also save the cost of information transmission, while ensuring the stability and security of the network, constantly optimize the network security of users, can provide a certain degree of security for the reception and transmission of information. With the continuous development of modern science and technology, the previous computer technology has been unable to meet the specific requirements of network security, virtual network technology plays a very important role in maintaining the safe operation of computers. To realize the efficient

management of computer network security is helpful to ensure the security of information transmission, facilitate the use of information data, and ensure the smooth operation of computer network system.

2.5. Development Model of Virtual Technology in Computer Network Security

In the link of maintaining computer network security, under the application of computer technology, virtual technology has also achieved a lot of innovation and development, broadband technology can provide users with safe information, and at the same time can ensure the security of information use. In the process of network security control, virtual network technology plays a very important role. With the advent of the information age, the development of enterprises need to strengthen the use of virtual technology, which is a very important part of our enterprise development process, to control the network security in a reasonable range. With the continuous maturity of virtual technology and computer technology, the security of the network has been improved effectively. The application of virtual technology can improve the security, stability and reliability of computer network. At present, virtual technology occupies a very large market share in the network security of our country, and it is gradually rising. From the point of view of computer network security, it is the key to the development of virtual technology only by constantly improving the practical value of virtual technology. In the future development of network security, virtual technology will develop in the direction of convenience and practicality, and improve the security technology of computer continuously on this basis[4].

3. Conclusion

To sum up, the problems in the hardware, software and operating system of the computer are the main factors that affect the security of the computer network, and at present, the computer still has a large lift empty in these aspects. To this end, we can fully refer to the above computer network security mode construction strategy based on virtual technology, reasonably use encryption technology and authentication technology, introduce MPLS virtual network, at the same time, add protective wall to make up for system loopholes, avoid being attacked by hackers, ensure the information security of computer network, protect the personal information of users, and improve the security protection ability of computer network in an all-round way.

Acknowledgements

References

[1] Ten, thousand. Research on security management technology of computer network database. Technology Innovation and Application , no. 04, pp. 151-152, 2020.

[2] Liu, Zhidan., Sun. Research on the present situation and defense technology of computer network security. Information and Computers (Theoretical Edition), vol. 31, no. 23, pp. 191-192, 2019.

[3] Wang, Xiao. Computer network security analysis modeling based on deep learning algorithms. Electronic Technology and Software Engineering , no. 16, pp. 195-196, 2019.

[4] Zhang. Computer network security mode construction strategy calculation based on virtual technology. Journal of Heihe College , vol. 8, no. 12, pp. 213-214, 2017.