Research on Network Security Management of University Computer Laboratory

Gong Hao

Sichuan University of Media and Communications, Chengdu, Sichuan, China

Keywords: University, Computer laboratory, Network security management

Abstract: The establishment of computer network laboratory in Colleges and universities is a teaching classroom that combines theoretical knowledge with practical experience. It is one of the most important components in college teaching. The computer network laboratory in Colleges and universities carries students' usual network learning and curriculum design. It is an important place for students to learn and a place for students to effectively combine theoretical knowledge with practice. However, with the further development of computer laboratory construction in Colleges and universities, the problem of network security has also become prominent. Therefore, how to effectively use the computer network laboratory in Colleges and universities is an issue of great concern to every university worker. This paper deeply analyzes the problems existing in the network security management of university computer laboratory, and puts forward the countermeasures to improve the network security management level of university computer laboratory from four aspects, in order to provide some reference for the network security management of university computer laboratory.

1. Introduction

Computer laboratories in Colleges and universities across the country are the main positions for the cultivation of "Internet +" talents, and undertake the important task of Cultivating College Students' curriculum practice and application ability. The teaching, practice and application of various disciplines gradually depend on the use of computers. Computer is a necessary tool to assist the construction of various disciplines and personnel training, so computer laboratory has become an important place for teaching and training in Colleges and universities.

Computer laboratories in Colleges and universities not only help the cause of higher education, but also have many hidden dangers. In each university, computer laboratories are more or less used frequently, and used with a large number of people, a miscellaneous population, a long time or a random way. Therefore, the biggest problem faced by computer laboratory network system is a variety of network security risks. For the computer laboratory with the same internal network, if one computer is infected with virus, it will quickly spread to other computers under the same network, and then affect the normal use of the whole computer laboratory. Therefore, the computer network security management of university laboratories is a very important research topic.

2. Network Security Problems in University Computer Laboratories

2.1. Insufficient Attention to Network Security

Laboratory computer network information security refers to ensuring the reliability and security of information and data during the processing, storage and transmission of information and related data in the laboratory. The concept of computer network information security is more abstract. In addition to the hardware management of networking and the application software of network control, it should also include shared resources and interactive information. The lack of attention paid by computer laboratory administrators to network security is mainly reflected in the neglect of laboratory operation and laboratory network security. As an important auxiliary tool of various disciplines, computer serves the development of education of various disciplines. The utilization

  DOI: 10.25236/iceieis.2022.021

rate of computer laboratory is very high, and the network security of laboratory is related to the personal privacy security of teachers and students and the private data security of colleges and universities, so the network security of computer laboratory is very important. However, both laboratory managers and users ignore the security problems of the laboratory and are not responsible for the security of the system, resulting in hidden dangers in the security of the network.

2.2. Poor Understanding of Network Security Regulations

The Network Security Law of the People's Republic of China is the legal guidance of China's network security work. The network security work of university computer laboratories must be carried out in accordance with the law. However, at this stage, the administrators of computer laboratories in Colleges and universities generally do not have a deep understanding of the network security laws and regulations, and believe that the computer network security laws and regulations will limit the normal use of various functions of the laboratory and increase the workload of managers. The starting point of network security laws and regulations is to ensure national security, protect the normal and safe operation of computer laboratories, and play a good role in promoting the standardized management of university computer laboratories. University computer laboratory managers should strengthen the study of network security laws and regulations, consciously act in accordance with the law, use the network and pipe network in accordance with the law, and do a good job in laboratory management and service under the premise of ensuring the network security of the laboratory, so as to provide teachers and students with safe, reliable and high-quality laboratory services.

2.3. Lack of Mastery of Network Security Technology

With the popularization of computer and network technology, information technology is everywhere. It has already been integrated into people's life, study, work and other aspects. With the expansion of computer applications, network security technology has been expanded on the basis of traditional firewall, anti-virus gateway and anti-virus software. Most of the administrators of computer laboratories in Colleges and universities are non network security professionals. Their understanding of the network security of computer laboratories generally remains at the level of computer restore cards and anti-virus software. Therefore, they still lack the mastery of new technologies, new methods and new requirements such as online real name authentication, online log retention, digital encryption backup, anti extortion and anti tampering, and the technical vision of network security is not comprehensive, which has left hidden dangers for the network security of computer laboratories.

3. Practice of Network Security Management in University Computer Laboratory

The network security management of computer laboratory is a part of the whole network security management in Colleges and universities. In order to reduce the waste of resources caused by repeated construction under the premise of maintaining the unified and standardized network security of colleges and universities, the computer laboratory of colleges and universities can formulate the network security system of computer laboratory by referring to the network security rules and regulations of colleges and universities. PDRR (Protection Detection Recovery Response) network security system consists of protection, detection, recovery and response, forming a network security closed loop (as shown in Figure 1). PDRR network security system improves the single security defense idea that the traditional network security system only pays attention to protection, emphasizing that network security is composed of four important links. None of the four is dispensable, forming an overall resultant force of network security to effectively ensure network security. Using the PDRR network security system for reference, the network specifications and application specifications of network security management in university computer laboratories can be carried out from four aspects: security protection, security detection, security response and security recovery.

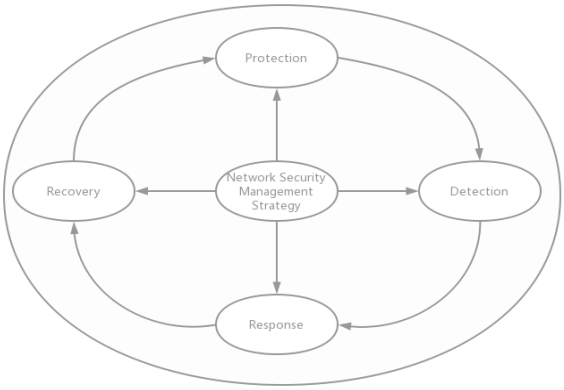

Figure 1 PDRR network security system

3.1. Network Security Protection

The separation of internal and external networks means that the computer room network is divided into two parts: the laboratory internal network and the laboratory external network. The separation of internal and external networks can realize different network security measures for the internal and external networks of the laboratory. The internal network of the laboratory, computers, servers and other equipment can be set as a trusted zone, open the required network ports and corresponding educational resources, realize the interconnection and inter-working of internal machines, and facilitate the internal system access and resource sharing. Set the external network of the laboratory, computers, servers and other devices as untrusted zones. The data from the untrusted zone must be checked and filtered by the firewall. The devices in this zone cannot directly access the devices or resources on the intranet of the laboratory. For the sake of security, computers in the laboratory can be set to be inaccessible to external network resources. Teachers and students who have external network use requirements must authenticate with their personal real name account. In addition, the network resources that teachers and students can access must be restricted, such as access to online games, online gambling, online audio, video and other resources unrelated to learning.

3.2. Network Security Detection

To ensure the security of the external services of the computer laboratory, the Webscan service provided by Qianxin free of charge can be used. Webscan service provides website vulnerability detection and website operation monitoring functions. The website vulnerability detection function can comprehensively detect the services provided by the computer laboratory, facilitate the rapid discovery of various vulnerability risks in the external services of the laboratory, and provide vulnerability repair and rectification suggestions. The website operation monitoring function can monitor the availability, black chain, hanging horse, phishing, sensitive words and sensitive information leakage of external services of the computer laboratory. The test results are sent to the manager in real time through e-mail and mobile phone SMS, which enables the manager to timely grasp the service operation status provided by the computer laboratory, and facilitate the corresponding processing in a timely manner.

3.3. Network Security Response

The network security response of computer laboratory mainly refers to the handling mechanism and emergency handling measures in case of security accidents. The network security processing mechanism of computer laboratory can be incorporated into the construction of laboratory system. The emergency treatment measures include solidifying the network security log and eliminating the network security impact. Solidifying the network security log enables the computer and server logging services, as well as the online verification and online behavior log services for teachers and students. The above logs can be backed up regularly to save the network security log for

verification by the network security agency. The emergency measures for computer laboratory network security mainly include one click off network exit and specific computer internal network. The network structure of the computer laboratory is relatively simple. Common software and hardware methods such as remote desktop and WiFi smart socket can be used to disconnect the network outlet and the computer internal network. The remote desktop can use sunflower remote control software to connect to the server. Running the corresponding management program on the server can disconnect the corresponding computer or the entire laboratory network. The use of WiFi smart socket is simpler. Just connect the laboratory network switch to the WiFi smart socket, and the socket can be connected to the laboratory WiFi network for management through the APP supporting the socket. When network security exceptions are found, turn off the socket power corresponding to the laboratory network switch through APP to disconnect all network connections and prevent further network attacks.

3.4. Network Security Recovery

At this stage, data assets have surpassed computer hardware equipment and become the most valuable assets of computer laboratories in Colleges and universities. In order to ensure the network security of the data assets of the computer laboratory, prevent the integrity of the system data and application data from being damaged, and quickly recover the functions of the computer laboratory after the hardware system is damaged, it is necessary to carefully deploy the computer laboratory from the system level and the data level. The network security recovery at the system level can be realized by adopting virtualization snapshot technology or installing software and hardware restore cards. The newly established computer laboratory can rapidly deploy the operating system and application software suitable for various disciplines through the virtual cloud desktop technology. When the system has problems, it can restore the template, quickly recover the data and restore the system. Network security recovery at the data level can be achieved by using data synchronization backup and recovery software. The database backup and recovery software includes DBSync and SQL backup and recovery assistant. File synchronization backup and recovery software includes FreeFileSync and GoodSync.

4. Conclusion

Under the trend of multi-disciplinary “Internet +” education with the help of computers and network equipment, the application and role of computer laboratories in Colleges and universities in education and research are becoming more and more important. The network security of computer laboratories is the key to ensure the information security of teachers and students. The network construction standards in computer laboratories of colleges and universities should be in strict accordance with the national requirements and regulations on network security. Taking the laboratory administrators and users as the starting point, formulate the management and use specifications of the laboratory network, customize the system for different tasks, regularly back up important data, and use the software and hardware of network security protection technology to set up security barriers for the network.

References

[1] Zhaoxuhua. Research on network security management of University Computer Laboratory[J]. China education informatization, 2021 (01): 60-65.

[2] Liaiyan. Network security problems and solutions in university computer laboratories[J]. Computer products and circulation, 2019 (12): 245.

[3] Bianhong. Research on the security management approach of University Computer Laboratory -- Taking the computer laboratory of Bian Hong Institute of normal school of Beijing Union University as an example[J]. Science and technology information, 2019,17 (19): 181-182.