Universe Scientific Publishing

DOI:10.18686/ahe.v7i9.8126

On the Network Information Security of Colleges and Universities

Kai Zhao

College of Artificial Intelligence and Big Data, Zibo Vocational Institute,Zibo,255314,China

Abstract: With the continuous development of information technology, network security has become a problem that cannot be ignored. The security of campus network is a common and complex problem, which requires all teachers and students to pay enough attention and take precautions. Campus network is an important platform for campus information transmission. An organic, intelligent, safe and stable campus network information platform is an effective guarantee for information resources, network services, information services, etc. of a university. Strengthening security construction is an important guarantee for building and making good use of campus network.

Keywords: Campus network security solution

1. Overview

With the continuous improvement of information technology, the campus network hardware facilities of all major colleges and universities have reached the initial scale, and now all have begun the promotion and development stage of information construction, especially the integration of many college application management systems and the implementation of a unified portal platform. Therefore, it is urgent to establish a university network security platform, ensure that the construction of various information infrastructure is not subject to the access and destruction of illegal users, manage the legal access of various resources, and comprehensively do a good job in the security work of university information [1].

2. Research and analysis of the current situation of campus network

At present, the campus network of major universities is large in scale and equipped with many devices. It includes many host devices such as routers, switches, servers and microcomputers. The campus network can be divided into three categories: teaching area, office area and student area. It is required to be able to access INTERNET and to access all major applications in the campus network, including office OA, mail system, teaching system, student management system, etc. Some applications must be isolated from the Internet, such as the all-in-one card system and the financial system.

3. Main security threats faced by campus network

3.1 Computer virus damage

One of the important factors that affect the security of campus network is computer virus. It affects the normal operation of the application system, easily destroys the software, hardware and data of the system, and greatly reduces the operating efficiency of the entire network, even paralyzes the entire campus network. Therefore, we must control the spread of computer viruses in the campus network. We can do the following:

First, prohibit the intrusion of computer viruses in the whole gateway, and close all the ports that are not commonly used in the campus network, especially the ports that are vulnerable to virus intrusion; Second, supervise all computers in the campus network to install virus protection software, which can greatly prevent the spread of computer viruses in the entire campus network; The third is to find the computer that has been infected with the virus, disconnect it from the network, physically isolate it, and allow it to connect to the campus network again after the user checks and kills the virus on the computer; Fourth, set up security audit in all servers to monitor the status of servers at any time, which can effectively prevent computer viruses and malicious intrusions.

3.2 Incomplete management of hardware network equipment

Colleges and universities are different from companies. Their network hardware equipment is not only distributed in office buildings, but also involves all corners of the campus, such as student dormitories, restaurants, training buildings, and campus monitoring and broadcasting. Some colleges and universities have more than one campus, which is very difficult to manage. From the level of network hardware equipment, the network level of campus network can generally be divided into core layer, convergence layer and access layer. To ensure the security of each level, the security and reliability of network equipment itself is the premise, otherwise the security strategy configured by network equipment will lose its significance. In order to facilitate the management of network hardware devices, switches and routers with remote management functions are generally purchased. In order to facilitate remote management, managers will set the remote login account and password of network devices to be identical. Once the illegal intruder obtains the remote login account and password of any network device, the entire network device will be transparent to the intruder and will pose an unimaginable threat [2].

3.3 Computer system vulnerabilities

At present, both computer systems and various application systems are not 100% secure, and there are more or less software security vulnerabilities. Intruders use these vulnerabilities to attack the server or user's computer of the campus network. Once the intruder attacks successfully, he will obtain the highest authority of the computer, and can illegally obtain the data of the target host. It is also possible to use the controlled computer to attack other computers or networks or illegally obtain data.

At present, computer vulnerabilities are mainly divided into three aspects:

One is the software vulnerability of the computer operating system. At present, the most widely used operating systems are mainly the Windows operating system released by Microsoft, as well as Linux and Apple's MAC system. These operating systems have various security vulnerabilities.

The second is the network hardware device vulnerability. Hardware devices of network infrastructure, such as routers and switches that can be managed by the network, rely on the programs in the management chip to realize a series of functions. These chip programs written by programmers will have some vulnerabilities, and these vulnerabilities provide the possibility for intruders to attack the network.

The third is the code vulnerability of websites and various network management application systems, including school websites, departments' websites, educational administration systems, student management systems, etc. The informatization construction of colleges and universities must rely on these websites and application systems. However, there are always various problems in the code of these websites and application systems in the programmer's writing process. Some problems are the defects of the code itself, and some problems are even the backdoor left intentionally by the programmer in the code, which leaves an attack path for the attacker.

3.4 User abuse of network resources

Generally speaking, the campus network will access multiple external network lines at the same time. There are many network access resources, and the network bandwidth is large. Teachers and staff can download various learning resources on the campus network. But in fact, quite a lot of Internet access has nothing to do with normal work. Many people use campus network resources to download a lot of video and software resources, and even visit some unhealthy yellow or reactionary websites. Therefore, these users have a great chance to download viruses or Trojan Horse programs from these illegal websites, resulting in their own computer being invaded, and the lesser will occupy network resources, In serious cases, it will cause traffic congestion and other problems [3].

4. Network security solutions

4.1 Identity authentication

For users accessing the campus network, identity authentication must be carried out. Identity authentication information mainly includes user name and password. The user name is bound to the MAC address and IP address of the user's commonly used computer, which can prevent personal information from being stolen to the maximum extent. Even if the user name and password of others are known, when the user name does not match the MAC address or IP address, it will not be allowed to access the campus network. It can also locate the user accurately and quickly, which is convenient for handling things.

4.2 Deploy network anti-virus strategy

Managers must set various network security policies to control and prevent the spread of computer viruses in the network. The

following points need to be done:

First, prohibit the intrusion of computer viruses in the whole gateway, and close all the ports that are not commonly used in the campus network, especially the ports that are vulnerable to virus intrusion; Second, supervise all computers in the campus network to install virus protection software, which can greatly prevent the spread of computer viruses in the entire campus network; The third is to find the computer that has been infected with the virus, disconnect it from the network, physically isolate it, and allow it to connect to the campus network again after the user checks and kills the virus on the computer; Fourth, set security policies in all servers to monitor the status of servers at any time, which can effectively prevent computer viruses and malicious intrusions.

4.3 Regularly backup and maintain the server

To prevent unexpected hardware and software system failures or user misoperation, the administrator needs to regularly back up various data on the server. For example, the database server needs to automatically back up data when the number of accesses is small. If conditions permit, you can run two servers, especially the data synchronization of various WEB servers and two servers. In case of data problems, you can quickly start another server. Monitor the use of resources on the server at any time, delete expired and useless files, and ensure the efficient operation of the server [4].

4.4 Strengthen campus management

Campus network security is not a single hardware or software guarantee, it must be an organic combination of software, hardware and personnel to form a whole, and they must complement each other. Therefore, the first thing to do is to ensure the safety of software and hardware. On the premise of software and hardware security, it is also necessary to strengthen and cultivate the technical and management capabilities of campus network managers, encourage and support network managers to participate in relevant technical training, and enhance business capabilities. On the other hand, it is necessary to formulate complete safety management rules and regulations, network system maintenance and emergency measures, and build a safety management platform.

5. Conclusion

Computer network security mainly depends on network management and security technology. At present, domestic colleges and universities have multiple campuses, and each campuses is directly scattered. There are problems in the network communication between campuses. At the same time, the campus network security problem is a relatively complex system engineering, facing external and internal network attacks. On the premise of fully understanding the current network security situation, administrators need to prevent the security of the campus network through technology and management. They need to design a reasonable security planning scheme to effectively prevent unauthorized access and various illegal attacks, prevent illegal users from stealing internal data and misappropriating network resources, so as to make the campus network construction move towards a comprehensive, open and safe direction, To provide an efficient and stable network basic platform for the development of the school's information construction.

References:

[1] Zhang Yaoxue, Wang Xiaochun, Zhao Yanbiao Computer Network and Internet Tutorial. Tsinghua University Press, 1999, (1): 89

[2] Xiao Debao Computer Network. Huazhong Publishing House. 2002, (5): 56

[3] Lin Yongjing Multi-level Campus Network Security Design. Journal of Jilin Normal University (Natural Science Edition), 2009, (10): 100

[4] Wang Rui, Lin Haibo Network Security and Firewall Technology. Tsinghua University Press, 2000, (3): 87