The campus network security hidden danger analysis and countermeasure research

Wei juan[1,a]

[1]Jiangxi Institute of Fashion Technology, Jiangxi, Nanchang, 330201

[a]251844523@qq.com

Keywords: Campus network; Safety hidden trouble; countermeasures

Abstract. With the continuous development of computer network information technology and popularization, many colleges and universities have established the campus network. The current campus network has become important in infrastructure projects in university, and the campus network information security problems will directly affect the teaching activities of the school development and implementation, and even involve students personal privacy problem. This article is in a variety of existing domestic university campus network security hidden danger as a starting point, attempts to explore the domestic colleges and universities the improvement of network information security measures and countermeasures.

The introduction

In the modern education institutions, especially universities, campus network has become a routine work, teaching, scientific research and sharing the important tool of all kinds of resources. Due to network with some of the features of its own, all kinds of leaks occur through computer networks more and more, also brought a lot of concern, so to protect the safety of the campus network, the illegal invasion, prevent the network attack, has become the key to set up and improve the campus network.

The campus network security hidden danger

In recent years, with the expansion of the institutions of mass, the new campus building or colleges merged to form the distribution between multiple campus in different areas. Therefore, the campus network in network sites scattered, increasingly complex network structure, network monitoring and management difficulties, and to run on the network management system have different security requirements, etc. All these problems make the safe hidden trouble in the network of colleges and universities in the use of further increased, the security problems existing in campus network, divided into the following categories:

The safety hidden danger of computer electromagnetic radiation. Computer is work by high frequency pulse circuit, because of the electromagnetic field changes, it must be sent outside the radiation electromagnetic waves. When the computer is running, the electromagnetic wave existed, and the electromagnetic wave by a specific device detected in a limited scope, especially use of efficient equipment can continue to run, complete detection to the computer data. Electromagnetic wave is mainly through the display, communication lines, computer host and radiation output devices in four aspects. Such as the electromagnetic radiation from the CRT, its frequency is lower than 6.5 MHZ, interpretation and it is relatively easy to receive, and has reached a higher level of technology, has been foreign intelligence is used as a kind of commonly used techniques.

The campus network own existence safe hidden trouble. One of the purposes of the campus network of colleges and universities is to use computer network data sharing function, campus staff involved in the data sharing has staff related to teachers, students and scientific research departments, the objects of data sharing is dependent on the campus network link, so many participants Shared data flow in the network link, there are many unsafe factors. For the Windows operating system, in order to realize data sharing, generally by setting the user's password to realize data sharing, in the process of the computer just by identifying the password code to identify Shared demand, so that those who were not authorized user may by pretending to be legitimate users, the use of password cracking or steal others correct password, access to the network for data access and download. Network connects the computer terminals, transmission lines were more than five classes or five types of twisted pair, the intermediate links connected by switch, an increased among lines and equipment of the network security hidden danger. Now of campus network coverage area, cable channel, or transmission of information is much larger than in the past, this is the possibility of illegal users to intercept the signal is getting higher, and intercept point is increased, the illegal users in the network of lines, intermediate nodes or other parts of the branch network can easily obtain the network information. Although the campus network, the Internet and other public information network physical isolation, due to the campus network bandwidth to rent telecom operators, at the same time it also shoulder for the maintenance and management of the network, many end users node to connect to the campus network, makes some criminals by end user nodes using the telecom operator's vulnerability to attacks on the campus network management and steal information.

The hidden trouble in security computer software. Part in the design of software, in order to facilitate debugging, there are always many "back door", together with some holes in the design is hard to avoid. Some hackers will use the operating system, Internet explorer and other security vulnerabilities that exist in the software design, a wide variety of virus Trojan program in the process of users use these software, if you do not download and install the patch in time, the attacker can use software security vulnerabilities that exist in the invasion of information systems and to steal information. Campus currently using most of the software products are foreign companies, especially in the field of operating system software almost are Windows series products, also left the campus network security hidden danger.

A computer virus attack and destroy the safe hidden trouble. To make teachers and students in the campus network files and information exchange is convenient, often use mobile storage devices, such as the U disk, which is in a computer virus spread in the network have created favorable conditions. Some teachers and students' safety consciousness is not strong, the data downloaded from the Internet directly into usb stick, and usb connected directly to the campus network computer, therefore, the rapid spread of the virus can through U disk in the campus network, the infection has been connected to campus network every computer security vulnerabilities.

The hidden trouble in security computer storage devices. Because in teaching and management on the demand, the computer in the early 90 s began to focus and use the equipment, now gradually into the frequent fault and eliminate renewal period. When computer malfunction, some classified computer hard disk is not processed or without regulation, to a repair shop or even directly into the secondary market, left a very big hidden danger to the campus network security. Even if the user deletes the sensitive data in the computer, and format the hard disk, but in the eyes of criminals, these old computer is still a sensitive information collector, using relevant data recovery software can will have been deleted data and format the hard disk data recovery effectively.

To strengthen the campus network security measures and countermeasures

Through the above analysis, the current campus network security situation is still grim. So need to develop a set of effective measures to solve the security hidden danger, accordingly to ensure the safety of campus network in colleges and universities can and healthy operation.

To strengthen the system construction, build a system of defense. In accordance with the regulation on administration of international networking of computer information system security and combined with the characteristics of each work, formulate relevant scientific rules and regulations, and substantial work, this is a significant means to ensure the safe operation of the campus network. Through establishing and perfecting the campus network management, the management of classified computer use, mobile storage devices and the use of laptops scrap custody, computer and network maintenance, network theft report and emergency plan and a series of related system, step by step to sign of the campus network security liability form, layer upon layer, inside regulation, finally promote the construction of campus network application and development in the direction of the safety and health.

To strengthen safety education, enhancing education of defence. Institutions of higher learning is an important part in teaching, scientific research is the main position, the height of the production, integration, network security, the normal work of scientific research, should cause enough attention. From home and abroad of the campus network security incidents happened in case of network security protection to get rid of the traditional concept of protection in the past, can only rely on, lock door traditional means such as files, control cabinets, but on campus data security is combined with advanced network security protection method. In addition, should strengthen the education of teachers and students and master the important network data training, make them master the necessary means of network data lost or stolen.

Strengthen supervise, enhancing supervision and defense. Schools should set up the campus network security supervision committee, respectively with the method of fixed inspection and spot check regularly, make each information network security director to perform the duties of security seriously, in order to discover the hidden trouble in all sorts of security information network, once found hidden trouble should be issued corrective book, to the serious consequences, must have the relevant person in charge of shall be investigated for responsibility.

Strengthen the technical prevention and enhancing technical line. School when buying network information product, can choose and buy as far as possible low radiation products, and give the important network terminal display device increase jammer, avoid caused by electromagnetic radiation information from eavesdroppers. Schools to use the software and hardware are strictly checks, as much as possible to purchase domestic equipment. Security vulnerabilities in computer software to download and install patch repair in time. Schools should strictly differentiate user access. With the help of virtual local area network security mechanism, can restrict user access to, or even able to lock in the Internet members of physical (MAC) address, so that users use the Internet for without the consent of the security is the limit. In view of the current campus network server generally used Windows operating system platform, make full use of its domain control function, strictly control the network client user accounts, setting all users must log on domain network operation, all the user's IP address, network card physical address and switch port for the binding, implementing strict identification and access control. So we can all sensitive to operation for safety audit and record, so that can have a mark in the wake of a security incident. Set the complex password, login password and screen saver password, as far as possible to prevent illegal personnel by stealing passwords using classified computer with access to important data. In order to prevent the virus Trojan program through the Windows operating system high dangerous network port for classified computer attack and damage, should be timely close UDP135, 139, 445 in the operating system and network port TCP137, 139, 445, etc. And install kill virus protection software, firewall, intrusion detection equipment and safety equipment.

Conclusion

The rising popularity of computer network technology increased the dependence to the network, people and generated by the computer network security hidden danger caused by the different degree of loss and damage. So, for the security of the network, more and more colleges and universities put forward higher request, the problem of campus network security is becoming more and more attention. Through the above analysis, I believe that as long as we attach great importance to in the thoughts, to strengthen the network security management, improve the information security technology, gradually establish a corresponding security system, we can build up the information security "firewall", along with the development of the network application of the university campus network security will be continuous development.

Reference

[1] Guanglin Lei, Changyi Jiao. Colleges and universities the hidden trouble of the computer network security and protection [J]. China medical education technology. 2011 (02).

[2] Guowen Yang. On the campus network information system security management [J]. Computer programming skills and maintenance. 2013, 5.

Efficient
[3] Gao Wei. University campus network configuration and security management [M]. Beijing: China light industry press. 2012, 9.