The Network Security Management Problem of Library

Li Zhao, Yun Zi
Kunming University of Science and Technology Library
Kunming University of Science and Technology
Kunming, 650000, China
E-mail：876021340@qq.com

Abstract： The application and development of computer network system bring a great convenience for library management and readers. At the same time, the security of computer network system in library is faced with all kinds of threats. How to guarantee the security of library computer network system has become the most important question for each library. This paper analyzes the factors which affect the library network security, such as network hardware, network operating system and application system, data security and so on, and puts forward corresponding security strategies and solutions.

Keywords: Library; Network Security; Safety Management

I. INTRODUCTION

With the popularization and development of the network, as well as the digitization and networking of library information resources, it gives users unprecedented convenience and a wide learning space, also leading to an increasing number of unpredicted security issues of library management. It has become an important issue of modern library management how to ensure the security of equipment, data and systems in the library networking process, in order to ensure the normal operation of the library based on network. Network security is to protect data , hardware, software and system of network systems， which is not destroyed, changed, leaked due to accidental or malicious reasons, so that the system continuously, reliably and normally run as well as the network service not interrupted. The network security of library is also using the management and control technology of network to ensure the confidentiality, integrity, availability, authenticity and controllability of data, without interrupting network operations.

II. NETWORK HARDWARE SECURITY

Under reasonable, preferably elastic network structure, we faced how to solve network security problems with network products and their security technology. The products mainly used to solve network security problems now are firewall and virtual private network (VPN). A firewall is a very effective network security devices. It is often placed on the nodes of the inside and outside the network in library. The firewall can check, screening, filtering, shielding the transmitting information from intranet or outside the network. And the information could only be transmitted via a control point to prevent someone sabotage the system and to ensure system security. VPN can mainly solve the security issues of cross-regional data transmitted between the branch libraries or different systems, in order that internal library critical data can be safely and frequently exchanged via the public network. The management of Library network device is through the development of a management system, systems of work, the registration system for network equipment and clear job responsibilities, to identify problems timely and solve the problem. There is specialized person is responsible for the maintenance of entire network and hardware, Including instructions and warranty for network equipment. And the incidental system disk should be managed by the responsible person. And to establish a registration system, including network failure handling registration, equipment Regular maintenance registration and system upgrade or patching record. Then establishing a topology map of network structure, network wiring diagrams, all types of files of network equipment and information points. With institutional guarantees and the files and types of recorded information, we can have a clear understanding of the establishment and development of entire network. It is a good opportunity to learn lessons in every treatment to deal with network security issues. Only according to the system step by step ,put responsibilities to the people, not have any fluke mind, and regularly maintenance of the equipment, can the security management of the network equipment be more scientific, standardized, and avoid the library network security issues due to network hardware problem.

III. NETWORK OPERATING SYSTEM AND APPLICATION SECURITY

Operation and control of the network hardware System also affect the security of the network. Utilize the network hardware built-in software or other software with monitoring and virtual network to Comprehensive monitor the network to prevent the network violated. Network segmentation can also be used to prevent broadcast storms. Especially the better virtual local area network (VLAN) is divided, the safer the network is. As to the security issues of WINDOWS operating system, timely install security patches of the operating system in management. As to Library security application software systems, frequently upgrade to reduce the "back door" of the application system, and use of anti-virus technology, backup and recovery technology to ensure that the system is foolproof. In the system for different users and staff, set a password and constraint permission. And strengthen management of the system administrator's password with particular attention.

Published by Atlantis Press, Paris, France.

IV. DATA SECURITY

In the library management system, a large amount of data is important as a normal network operation support. The library data security is that network information resources are not lost not modified and steal in the network transmission process. In an open network environment, the computer system would refuse to service for various reasons at any time. This reason may come from the hardware or software; may be man-made or caused by objective factors. Anyway, when this disaster comes, all that we have to is to resume the system Operation as soon as possible and provide normal services to readers. The premise is to backup data. On the premise of ensuring library application system security, the security and availability of the data can not be separated from the good data backup job. A good backup strategy can respond to a variety of security issues of the library. This is because the hardware damaged could be solved by update, system destruction could be solved by reinstalling, but incomplete data will enable us to pay immeasurable cost. For small and medium-sized library, select the server with dual hard disk backup or dual system backup, coupled with log restore function of the application system and regularly using Burning DVD equipment to do artificial full backup, and the data security can be fully ensured. For large libraries, due to the changing large amount of data, it would be better to choose the suitable backup hardware and backup software. The Mainstream of backup hardware device is still tape drive, it has good compatibility with most of the server system. The size of the tape drive is proportional to the amount of data, some large libraries would need hundreds of tape drives to consist array groups. Through the backup software to manage the backup process, not only save in the manpower, but also reduce manual backup mistakes. In addition, we still need a scientific backup plan. Example: once full backup per month, once incremental backup per day and do off-site storage and rotation reuse of the full backup media monthly.

V. USER SECURITY

For user security, the most important problem is the user's authorization. The user of library network system is nothing more than two categories, Data production staff and data utilization staff. The former library staff and the latter is a public user, who can be user to the library or a network user. Therefore, the different levels of security permissions should be set for different users or take other security authorization measures. First, set the user permissions of the library staff. Besides the system administrator with all permissions, other staff should get the appropriate permissions according to the nature of the work. For example: Book sorting and cataloging staff have the write permissions only to cataloging database, while they have only read permissions to other database or modify the permissions, but no delete permissions. Authorized Library staff do a good security work of system user password and the system administrator should also change the system password regularly to ensure the system safety. Next, the public user is also divided into two cases. For the user to the library, system either set only read access to all databases, or install a single retrieval module on the user computers, then set up a public account, also have only read permissions without write permissions. For network users, Library store data separately for data security, as well as to the security of the LAN server. The data for network users and the digital library website should be on one server, while the Library LAN server and the external network is isolated, run separately. And regularly update to ensure that the data on the maximum degree of synchronization with LAN server according to the needs extranet users. So that a public Internet users can query the library data like browsing web pages. However, it is insufficient to prevent staff and public user caused damage to the hardware and software lead to unsafety of the network data only on the technical level alone. We should process the user computer security education while making the necessary permissions setting at the same time. So the staff education is a top priority as fort is most easily compromised internally. Library staff must enforce the rules and the management system and be educated about the computer operating system work, education and anti-virus and other skills training.

VI. ENVIRONMENTAL SECURITY

The environmental security is disasters, accidents in macro terms; The environmental security objectively is whether the placement environment of library network center room and working equipment and network structure design is scientifically, whether the voltage is stable, whether the room temperature, humidity standards, whether there are anti-static, leakproof, anti-theft measures ; The environmental security subjectively is whether Improper use, security checks in place or cause data loss or system damage because of the low quality of the internal personnel; And it externally is that Hacker intrusion and computer viruses. Therefore, to ensure the security of the network, close attention should be paid from design construction of buildings, the wire routing to find out what environmental factors will lead the unsafe network. Any natural disasters, accidents which can be prevented is necessary to take precautions in management. For example, when thunder weather, if there is no lightning protection equipment in the buildings, it is necessary to turn off all network equipment to ensure security; In another example, the long-range backup of the data is to prevent theft and fire and other accidents leading to data security issues.

VII. VIRUS PREVENTION

If the library information system if not taken viruses prevention measures, Once computer viruses spread in the system, at least destroy the workstation operating system, or attack server entire information system leading to data loss, suspend service and system breakdown. Modern Library rely on computer applications from procurement to the acceptance, collection, from sorting and cataloging to circulation. If network security problems caused due to a virus, not only day-to-day business work of the library can not be carried out, may also cause the loss of data besides the economic and human losses. The consequences could be disastrous. Therefore, prevention of the virus is an important part to ensure the library network security. First of all, physically isolate the Library LAN network, which can minimize the intrusion of viruses. Meanwhile, install the anti-virus software with firewall on the server in the library. Then ensure timely updates, and run a virus scan on a regular basis, removing hidden dangers of virus infection and spread. In addition, each workstation is best not easily use unknown-origin floppy. If you want to use, conduct a virus scan before opening. Often virus in the library LAN and the workstation is because that user inadvertently use the media with virus into the system, and quickly and automatically copy propagation in network. Second, the virus come out always before of the anti-virus software updates, so the library must guarantee the security way of data backup. If the system is damaged beyond normal work, then just reinstall the system, everything can be back to normal.

In a word, the library network security is the most important work of the Library Management. We can not hold fluke mind, must adhere to start from the system, use the technical means and fight with advanced awareness. We only continue to improve the security level of hardware and software systems, do all the backup data, strengthen management, education and training. So that we can change from passive to active in network security, carry out library information services better and provide users with a stable and reliable system environment.

REFERENCES

[1] H.B. Chen, Network security threat and Countermeasures, Sci-Tech Information Development & Economy, 2005, Vol.12 pp:219-220

[2] Y.H. Zhao, Development and management of public management information system, 2007

[3] G.L. Wang, J. Yang, Information retrieval and utilization , 2005.08

[4] S.Z. Niu and W.Q. Jiang, Network attacks and prevention theory and Practice, 2006

[5] L.S. An Technology of Network security, 2010.04