Analysis of Computer Network Security Strategy in the Library

Changjin Guo

Chongqing University of Science & Technology, Chongqing, 401331

Keywords: Analysis, Computer, Network Security, Strategy, Library

Abstract: The operation and management of the modern library cannot be separated from the computer network. With the development of network technology, new services such as multi-library search and interlibrary loan are constantly emerging. Therefore, the library computer network security issues have become increasingly prominent. This paper analyzes the main factors that affect the security of computer network in libraries and puts forward some strategies that should be followed to strengthen the security management of library computer networks in view of these problems.

1. Introduction

With the rapid development of computer network technology, library operations management has undergone tremendous changes compared with the traditional model. Not only the readers inquired about the collection of bibliographies, reservation books, readers and bibliographic information management through the network, but also with the library digitalization, the continuous development of information technology, multi-library inter-library search, interlibrary loan and other new business constantly Appears depend on the computer network. It can be said that a modern library cannot be separated from a computer network for a moment, and if the computer network fails, the entire library will be paralyzed. With the construction of the modern digital library, the library database resources become more and more huge, how to ensure the safe operation of the computer network and to ensure the safety of the massive data resources has become an important issue.

2. The main threat to computer network security library

There are many factors that affect the security of library computer network. One or several kinds of network security technologies cannot meet the network security needs of libraries. The problem should be solved in many ways and in various ways. From a holistic point of view, the threats to library computer network security are both equipments and technology, as well as system management and personnel quality factors, as well as the underlying network information resource resources themselves. To sum up, the main threats to library computer network security include the following aspects.

Such as security vulnerabilities caused by improper operator configuration security, user security awareness is not strong, the user password choice is not careful, users will be free to own account or share with others and other network security threats. This is the biggest threat to the library computer network, and adversary attacks and computer crimes fall into this category. Such attacks can be divided into two types: one is active attack, which selectively destroys the validity and integrity of information in various ways; the other is passive attack, which is without affecting the normal operation of the network, Intercepted, stolen, deciphered to obtain important confidential information. Both of these attacks can be extremely damaging to computer networks and result in the disclosure of confidential data. Computer virus is man-made latent information that interferes with the normal operation of a computer system and spreads and spreads with strong contagion. Once an attack occurs, the system and data are destroyed, resulting in serious losses and adverse consequences. Software data security is not strong. Library computer network system uses the database, data transmission technology and the database itself loopholes will endanger the safety of

Copyright © (2018) Francis Academic Press, UK

data. Mainly in the unit of the network completely ignored, resulting in the unit network management system, anti-virus systems and measures that are not perfect, or the implementation of ineffective supervision, are endangering the safety of computer networks an important factor.

3. Library computer network security strategy implementation purposes

Library computer network system is to provide services to users and collect information tools and network security strategy is to protect the integrity and accuracy of these information resources, and to resist the threat of network hackers and all kinds of computer network virus attacks. The main purpose of library computer network system security strategy implementation includes the following aspects.

When a library user needs information, the library computer network system and the information it holds must provide timely, reliable service to the user.

Library computer system and its information is to serve a specific user, the library computer system to ensure its practicality, effectively solve the actual needs of information users.

To ensure that the library computer network system and the information it possesses, the information provided must be complete and reliable. The library computer information network system owns and provides the complete and reliable information, which is an extension of the traditional library and provides the high assurance rate and accuracy of document information under the new environment. It is an important goal of the library business.

Some of the information in a library is private information about the user and related individuals. Some are non-public information that is confidential within a library. Libraries and librarians must ensure the security of such information and prevent the malicious use of bad information.

Human factors affecting the computer network security of the library mainly include human-operated errors and malicious attacks by network hackers. Such as improper operation of the administrator or improper security configuration, leading to network security vulnerabilities or misoperation of the administrator resulting in data loss. The improper operation of the user also easily leads to network security problems. For example, if the user sets the password too simple or the user safety awareness is not strong, Account lending others, etc., will pose a threat to network security. Network hacking malicious attacks to the library computer network security threat is greatest, network hackers often use network security vulnerabilities to attack the library network, the purpose is to steal confidential information or undermine the integrity and validity of the database. Malicious attacks can be divided into two types of active attacks and passive attacks. Active attack means that hackers take various measures to destroy the network firewall, attack the library database system, selective destruction of information content. Passive attacks are more subtle, is to steal, copy, monitor confidential information without damaging the network, will result in the leakage of confidential information.

Poor software security can also cause library computer network security problems. For example, the database system and data transmission technology itself loopholes will lead to the loss of database content or data transmission errors, which will threaten the integrity of the network database. Another aspect of the network security failures caused by software factors is reflected in the invasion of computer viruses. Computer virus is latent and highly contagious and its existence will interfere with the normal operation of the system, and even cause data destruction and loss.

Hardware failures also affect the security of the library's computer network, which can result in significant data loss if the data server hardware fails without good data backup. Although the probability of a hardware failure during operation is small from a single component, the probability of failure is large due to the complexity of the library network, the amount of hardware that needs to be used, and how long the server does not shut down Increase in amplitude.

4. Library computer network security strategy

Hardware protection against network data security mainly refers to the measure of increasing security by adding hardware usually refers to the computer hardware, such as CPU, data memory,

cache, input / output channels and external devices to take appropriate security Measures to prevent data damage, to protect the integrity of the database. Securing security through hardware is more reliable than software protection. For important systems and data, you must adopt a combination of software protection and hardware protection to ensure data security. Common hardware protection methods are memory data protection, virtual memory protection, input / output channel control protection.

Data loss is also the biggest problem facing library computer network security. The most effective way to reduce the heavy losses caused by data loss is to back up data regularly. The use of redundant array of independent disks (RAID) technology is to achieve redundant data backup and improve data system performance is one of the important ways. The principle of RAID is to make use of an array of disk groups, with data decentralized design, improve data security. It treats a disk system composed of multiple disk drives as a single disk that can be expanded on a RAID stripe set for simultaneous multi-head read and write. As a result, the security of enhanced data realizes the parallel operation of data and improves the overall performance of the database system.

Network data encryption is mainly to prevent criminals in the data transmission process through the interception of data tampering with the data, stealing and copying and other operations. Network data encryption technology is a basic computer network security technology, there are many kinds of data encryption methods, according to the different stages of data transmission, storage, can be summarized as the following aspects: ① data transmission encryption: data transmission encryption transmission line Encryption and end-to-end encryption of two methods, transmission line encryption refers to different transmission lines using different encryption algorithms, have different keys; and end-to-end encryption refers to the data before sending the whole data subcontracting and Encryption, using the unified key in the transmission process, after arriving at the destination need to be in accordance with the sub-package information to decrypt the data before reading. ② data storage encryption: Even if the data transmission process is safe, but in the process of data storage, the information may still be stolen, which is the need to use data storage encryption. Storage encryption can be through a specific algorithm, the stored data itself is encrypted, it can be for visitors access control, that is, only have specific permissions and specific identification of visitors to access the data area.

User management should include user access control and user rights management. The former refers to the control of users of network resources, and only legitimate users log in to the server to access network resources, network access control mainly through the network registration and landing system that users want to use network resources, you need to register now on the library website and authentication, and the site assigned a unique identity and access password, after the user is required to visit the site login verification. User rights management is a kind of protection measures taken for the illegal operation of the network. The registered users of the library are divided into different levels, such as administrators, advanced users and ordinary users, and make specific resources accessible to clients with different identities. For administrators, you can assign permission to modify or delete data to maintain database resources. Library computer networks are usually not independent, but through the TCP / IP protocol connected to the Internet, so that users can access the library home page through the Internet. However, this also brings a lot of hidden dangers and threats to the computer network security of the library. Therefore, firewalls and anti-virus software must be used to protect the library network. The firewall, composed of software and hardware, is located at the interface between the external network and the internal network and recommends a security barrier between the internal network and the external network. The main function of the firewall is to implement packet filtering, proxy services and monitoring network status. The anti-virus software is mainly for computer viruses, anti-virus software is usually provided by a professional anti-virus software provider, library computer administrators need to upgrade services, timely killing of computer viruses.

5. Conclusions

Library computer networks contain a large amount of data and clients, which require high network security. On the one hand, we should adopt a security strategy to ensure the safety of computer networks. On the other hand, we should realize that there is no absolute security. The higher the security cost is, the higher the cost of capital is and the less convenient it is to use. Therefore, we should fully understand the importance of analyzing the computer network security in the library, and adopt different security protection strategies according to different systems and requirements in order to achieve both security and suitability.

References

[1] Liu Jia. Library Computer Network Security Management Issues [J]. Shanxi University of Finance and Economics, 2012, (2): 237.

[2] Jin Wenxin. Design and Implementation of Computer Network System Security Strategy in University Library [J]. Library Forum, 2009, (3): 80-83.

[3] Yin Di. Talking about the Current Situation and Countermeasures of Library Computer Network Information System Security [J]. Network and Information Engineering, 2014, (18): 43-44.

[4] Han Zijun. On the construction of multi-layered network security system [J]. Library Tribune, 2003, (6).80

[5] Guo Jiuyu, Deng Xian'e Library Network Security Problems and Countermeasures [J]. Library, 2005, (1). 59.