

Research and Implementation of Security Policy of Library Digital Information

Wang Haixia

Jilin Agricultural Science and Technology College

Abstract

This paper put forward a general discussion on the digital library security from the perspectives of management risk, security demand and target, the security architecture and model of library digital information. The specific solution for implementation is presented for the information security of library digital information in the aspects of hardware infrastructure security, firewall technology, encroachment test, access control, virus protection, data backup and security management.

Keywords: digital library; information security, digitalized information, information security technology

1. Introduction of digital information security theory

1.1. Concept of library digital information security¹

Generally speaking, the library digital information security means that the hardware equipment, network communication and software system of digital library network will not be lost, destroyed, manipulated or leaked, which

ensure the normal operation of the library digital information system with the ultimate target of maintaining the confidentiality, integrity, availability and controllability in the processing and transferring of library digital documents.

1.2. Demand analysis of library digital information security

Macroscopically speaking, the demand of library digital information security is simple, that is to say, the substantial digital information owned or purchased by the library is conveniently and quickly provided for the proper usage of the authorized users. According to this demand, the library provides the service for readers with the digital information resources, which requires the assurance of security, the seemingly simple demand of library digital information can be reduced to the following security requirements:

- The normal operation of hardware equipment and network equipment
- The sound security of operating system and database system
- The security of application system
- The information security (data security)

If the above requirements can be assured, the service system of library digital information resources can normally

¹ Wang Haixia, Female, MA, Jilin, Jilin, Research Orientation: Construction and Management of Digital Library.

provide the service for the users with developing service quality.

1.3. Risk analysis of library digital information security

With the library digital resources sharing further strengthened, the insecure factors become more outstanding. The threats for the security of library digital information can basically be summed up as the following:

1.3.1. Risk analysis of physical security

The physical security refers to the safety of different hardware equipment, such as server, switchboard, router, and communication line. The possible security risks may come from many accidents, such as fire, thunder, and long-time blackout. The threat of physical security may directly cause the damage of equipment, collapse of network or system, or the direct damage or loss of data, such damage will bring the disastrous results.

1.3.2. Risk analysis of network security

a. Risk analysis of data transfer

The platform of library digital information service is open in the environment of internet. The TCP/IP protocol is applied in transferring the data, if the rogue elements carry out the attacks, such as the forgery, deletion, steal, or manipulation, there will be massive impact and damage.

b. Risk analysis of open ports

The library digital information is usually open to the outside in the form of web site, and some service ports have to be opened with the system server stored in the specific server center. The attendants need to carry out the basic operation on the server through remote control, which also has to open some service ports and access permissions. The account

information may be detected, cracked in the normal data exchange, which can bring security threats.

c. Risk analysis of system security

The system security risks usually come from the operating system and database system. The system of the library digital information service is generally Windows server 2003 or 2008, and the SQL sever series is widely used as the database system. As there are various leaks in the aspects of the security of these systems, if some of the leaks are discovered and used by attackers, there will be massive scanning, which will become a great security risk of the whole system.

d. Risk analysis of application security

The service system of library digital information is always independently developed according to the requirements of the library itself. As the system is not widely employed as the operating system, the hacker will be reluctant to attack its application, and the security measures are relatively short, so there will be system leaks which are easy to be cracked. The existing risks are as follows:

- Risk of identification verification
- Leaks of Web service
- Leaks of DNS service
- Virus attack

e. Risk analysis of management security

People management is always involved in the security of equipment, network and system, so management is the most important part of the whole network security, especially for a large and complex security system designed for the network. Therefore, it is necessary to carry out the corresponding security measures caused by the risk of management.

1.4. System structure of library digital information security

According to the network reference model of OSI, the system structure of library digital information security should be built on the full model, which covers different levels and combines the various protection technologies and factors to provide a comprehensive protection. The protection of each level is added up to greatly increase the difficulty and cost of attacking. Based on such thought, the solution established on the corresponding model of different levels is shown in table 1-1.

Table 1.1 Laminated protection technology

OSI reference level	Security leaks	Threats	Solutions
7-Application level	Data acquisition Malicious algorithm Data damage	virus fabricated, damaged data malicious program illegal users file lost	Virus protection System protection Access control Identification verification Intrusion test
6-Expression level			
5-Conversation level			
4-Transmission level	exchange, router data addressing	Router damage Service rejection Data interception	Encryption algorithm Rooting update
3-Network Level			
2-Data chain level	Communication lines Hardware working environment	Electronic attacks Relay damage	Restriction, Management Security boundary
1-Physical level			

2. Security measures at the system level of library digital information

2.1. Configuration scheme of security protection of server system

As the server systems employed by the library are based on Windows server 2000 or 2003, the security protection configuration should be established for the servers to ensure the normal operation of the library digital information platform. The server of library digital information resources will be configured as the following.

2.1.1. Basic information of the server

The server platform of library digital information is configured with operating system of Windows server 2003, intranet static IP address of 10.0.0.2, and the reflection method is applied to access the internet with a static IP. As the web service is enough to provide the digital resources for the internet, the port 80 of server is the only opened one to provide the service for the outside.

2.1.2. The TCP/IP filtering is implemented on the intranet

The local connection-properties-internet protocol (TCP/IP)-advanced-options-TCP/IP filtering –properties, the TCP/IP filtering is initiated with the 80 and 3389 of TCP port available for transferring the information.

The IP segment, hereby, is the configuration of the library intranet, i.e., even I myself want to control the server remotely, the campus intranet have to be accessed in the physical space of this library, because only this network segment meets the access control configured. The above configuration can prevent the intranet server from simple attacks to a large extent. Any connection attempts will be rejected, and the ping order will not get the feedback. The configuration is then tested, and only mstsc remote connection can be used to access the remote server with no feedback for any other links. The test results are shown in figure 2-1 and 2-2.

```

Connection-specific DNS Suffix . : 
Description . . . . . : Marvell Yukon 88E8022 PCI-E Gigabit Ethernet Controller
Physical Address. . . . . : 18-09-05-86-5F-8C
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . : Yes
IP Address. . . . . : 10.21.63.6
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 10.21.63.254
DHCP Server . . . . . : 10.21.5.100
DNS Servers . . . . . : 10.12.8.58
                          10.122.5.101
                          202.96.104.19
  
```

Fig. 2-1: The specific description of local computer IP.

```
C:\Documents and Settings\Administrator>ping 10.0.0.2
Pinging 10.0.0.2 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 10.0.0.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Fig. 2-2: The feedback after the ping order is sent to the server.

2.1.3. The necessary group policy is opened according to the security requirements and intrusion detection.

The closed services are as follows: Computer Browser, Task scheduler, Messenger, Distributed File System, Distributed linktracking client, Error reporting service, NTLM Security support provider, PrintSpooler. The necessary group policy is opened.

2.1.4. The configuration of user and disk access

The user jlnku with administrator access should be established first, and then any irrelevant users, including the administrator, are prohibited. The disk C can only be accessed by Jlnku and system, and other directory will be configured as the same way. The directory of Windows will be added with the default access of users, or the programs, such as ASP and ASPX, cannot be operated.

2.1.5. Other configurations

The registry can be changed to fully hide the important directory or files, and the operating system and database system software can be amended with patches regularly; the C\$ share is cancelled; the Guest account is disabled, and the administrator account and password are changed; the tools, such as ftp.exe, telnet.exe are deleted; the unopened ports are disabled.

2.2. Configuration scheme of SQL database system security protection

The system configuration of the library digital document resource is the Windows server system with SQL database, so the operating system and database system should be prepared with the correspondent configuration and protection measures before the web application service.

2.2.1. The configuration thought of SQL security

As there are various leaks on the SQL system, the priority step is to ensure the basic security of the system with operation and configuration, which are as follows:

- Download the latest and secure leak patches for SQL Server
- Change the default port 1433 of SQL server
- Restrict the users' access to the SQL with the lowest access
- Change the in-built stored process of SQL Server

2.2.2. SQL Injection and prevention measures

SQL Injection is used with the outside ports of database to inject the user data into the actual database operating language with the aim of intruding the database or controlling the operating system. Based on the experiments, the three effective judgments and countermeasures are concluded.

- If the injection action of user is detected, the directory will jump to other page.
- Any injection action will be deemed as the outside links and be rejected.

- The injection of user will jump to certain website or page.

2.2.3. The detection of potential leaks with MBSA

3. Other implementation scheme of library digital information security

3.1. Configuration scheme of firewall

Based on the digital document resource library and network architecture and the network environment of the college itself, the firewall needs the installation of hardware firewall, which is targeted at the threats from the internet, and software firewall, which is targeted at the threats from intranet.

3.1.1. The hardware firewall is located between the network center room and the internet with the installation of Cisco Firewall Pix 525, and the specific configuration, based on the requirements, is as follows: The Console port of firewall is connected to a spare serial port of laptop computer with a serial line equipped for the firewall, the port 80, as the major part of configuration, is employed to open the web for the internet at the reflected IP address of local server.

3.1.2. The Windows firewall is usually taken as the software firewall, which is

mainly used to prevent the unauthorized users from accessing the local computer through Ping order or illegal methods. Such configuration is mainly applied to the operating system.

3.2. Virus protection scheme

The Symantec Antivirus system is employed as the library digital information service system. The system administrator may force the clients to implement the uniform configuration and the network virus protection strategy through Symantec System Center (SSC), the clients cannot be changed, and even be deprived of virus protection software. The update can be carried out through the internet to prevent the new virus. Certainly, the system security cannot be guaranteed only with only firewall and antivirus software to ensure the safety of information, some other methods, such as the implementation of intrusion detection technology, has to be employed.

3.3. Data backup scheme

According to the present conditions of the library, the equipment investment cannot meet the requirements of the data security, and the human backup has to be combined with the auto backup. As there are no specific backup servers or online storage, the data backup and database auto backup, without using the network storage, are temperately applied to back-up the data, which will be transferred to the present mobile memory for storage by human.

3.4. Security system for digitalized information management of library

The implementation of technology is not enough for the information security, which requires other methods besides the technology. As the full information security protection cannot be provided only with the technology, the proper approaches should be applied in the aspects of education and personnel management to adapt to the demands of library digital information security.

4. Conclusion and Outlook

The information security is a large and complex system, through the study on the existing threats, security technology and management in the field of information security, this paper presents the basic technologies and methods which can meet the requirements of security for a higher education digital library, and provide the practical guidance for the construction of digital library.

In the meantime, it is a complex and long-term task for the development and construction of digital library. With the development of computer technology and network communication technology, the widely developed “mobile library” requests a new environment demands for the storage, search and usage of the digital document resources. Along with the fast development of the information security technology, the threats for information security will be diversified and the demands increase, which request

the development and improvement of the information security system for digital libraries. The information security demands for digitalized documents will meet more challenges.

5. References

- [1] Zhang Weizhen. Discussion on the Development History and Development Tactics of Chinese Digital Library [J]. *Sci-tech Information Development & Economy*, 2008, 09: 10-11.
- [2] Zhang Jianbiao. *Information Security Architecture* [M]. Beijing: Beijing University of Technology Press, 2011.
- [3] Zhai Jianhong. *Introduction to Information Security* [M]. Beijing: Science Press, 2011.
- [4] Ma Xiaoting. Study on Cloud Computing Security Analysis and Management Strategy for Digital Library [J]. *Information Science*, 2011, 08: 1186-1191.
- [5] Zhang Hongliang. *New Security Strategies for Digital Library* [D]. Changchun: Northeast Normal University, 2008.
- [6] Kuo-Hsiung Liao, Hao-En Chueh. Medical Organization Information Security Management Based on ISO27001 Information Security Standard [J]. *Journal of Software*, 2012, 74: 32-35.
- [7] Ross Anderson. *Security Engineering: A Guide to Building Dependable Distributed Systems (Second Edition)*[M]. Beijing: Tsinghua University Press, 2012.
- [8] Allan Cho, Yu Li. Libraries in a Digital Frontier: Preserving Chinese Canadian Cultural Heritage[C]. *Digital Libraries*. 2011: 35-38.

- [9] Chen Chen. A Study of Information Security and its Strategy in Digital Library Based on Cloud Computing [J].Library Work in Colleges and Universities, 2011, 31: 58-60.
- [10] Liu Chao. Information Security Analysis of Digital Library [J]. Modern Information, 2009, 29: 72-75.
- [11] Wu Jiali. Information Security and Risk Management of China's Digital Library [J].Fujian Computer, 2011, 27: 60, 150.