Risk and Preventive Strategy of Network Security in University Digital Library

Yuying Liu

Shenyang Aerospace University Library, Liaoning, 110136

835184286@qq.com

Keywords: University Library; Digital Library; Network Security

Abstract: With the advent of the era of big data, university library have gradually changed from traditional document centers to digital library.Faced with new ubiquitous network and the rapid development of the “Internet + library ”, the secure information network environment provides a reliable guarantee for the data and information security of university digital library.This paper analyzes the status situation of network security in university library, and puts forward some suggestions on how to strengthen the security of library information networks.

With the rapid development of digitalization and networking, university libraries are constantly introducing digital resources for information navigation, enriching the library's collection resources. At the same time, the problems of digital and networked libraries in network information security are becoming increasingly prominent. According to the 28th "China Internet Development Status Report" issued by China Internet Network Information Center (CNNIC), by the end of 2018, the number of Internet users in China had reached 829 million, and the proportion of Internet users who had encountered network security problems was as high as 50.8%. Cyber security issues have gradually become the focus of the information society. As one of the three pillars of colleges and universities, the library is a documentary information center for learning. It is responsible for providing information resources and information services for cultivating high-level talents. With the influx of network information, computer viruses and hackers are on the Internet. The attacks are becoming more and more fierce, so the information network security of university libraries is also particularly important.

1. The Meaning of Library Information Network Security

The network information security of digital library refers to the guarantee that the hardware, software and data in the system will not be leaked, damaged or changed due to external reasons during the operation of the library system, so as to guarantee the normal operation of the library system and ensure the integrity and confidentiality of information transmission[1].

Network information security is a very complex problem, it is not only a technical problem, but also involves human psychology, social environment and legal content. The network information security of digital libraries is a system concept, including equipment security, automatic management system security, various data security, network communication security, personnel management security, environmental security and so on. Digital library network information security has the following three objectives: integrity, ensuring that unauthorized operations cannot be modified, adding or deleting data; Validity, ensuring that unauthorized operation cannot destroy various data; Confidentiality, ensuring that unauthorized operations cannot access protected information resources[2].

2. Analysis of the Status Situation of Library Information Network Security

2.1 Attacks on External Networks

Since the digital resources of university libraries need to be directly connected to the external network (ie. the Internet), anyone on the external network can access the internal network of the

  DOI: 10.25236/meici.2019.026

library, which can easily cause the internal network system of the library to be attacked by external network hackers,Such as the release of viruses, illegally stealing user accounts, destroying resource data, etc.,resulting in network congestion, server defects, loss of user data, etc., making the library unable to carry out normal information services. Due to the fragility and complexity of computer network, the possibility of network attack is increased, and the communication cables, switches, routers, hosts and terminals used in the process of network communication are often the targets of attack[3].The library's various network information resources are abundant. Therefore, once individual users access the library network through illegal means and steal all kinds of information resources of the library, it will cause immeasurable loss to the information network security inside the university library.

2.2 Internal Network Security Threats

Modern library management is inseparable from the network, and it is inseparable from the computer. The removable media devices (mobile hard disks, CDs, etc.) used by users will be the breeding ground for computer virus introduction, illegal software operation, system information leakage, etc. The computer network of the university library is huge, and there are many users on the network and the level of difference is large. Therefore, the security management in the internal network is very difficult.

2.3 System and Software Factors

Software security mainly includes three parts of the operating system, database system, and application system.At present, the university libraries mainly use Microsoft's Windows operating system, Linux and Unix.Among them, Linux and Unix systems are more complicated to operate, but they are more resistant to computer viruses. Windows operating system is simple to operate and easy to configure, but it has many loopholes and is vulnerable to computer viruses or human factors.In terms of database, both SQL Server and Sybase database have some security vulnerabilities. These vulnerabilities will become the door of hacker attacks; errors in the settings of the database itself, permissions, etc. will also enable unauthorized users to directly obtain user data.In terms of application software, software cannot be perfect. Software vulnerabilities and defects are the first targets of hackers[4].The management systems used by libraries are different from each other, and the level of development is also high or low. If the system development level is high and the prevention methods are advanced, the security is higher. On the contrary, the application software itself may also have security risks.

2.4 Information Security Awareness is Weak

In the construction of library network information, many university libraries are constantly introducing electronic resources in order to strengthen their digital construction. Due to the blind construction and light maintenance, the network information security issues are not well considered.Managers don't know how to protect information security, how to properly choose and use network security products, and how to deal with system problems.Statistics from many security agencies at domestic and abroad indicate that about 70% to 80% of security incidents are caused entirely or mostly due to poor internal management.The management system of library network security is not perfect or the implementation is not in place, and the implementation is not in place. As a result, the existing management mechanisms and security measures are ineffective.In fact, deep security issues such as the integrity and consistency of information data have not yet attracted the attention of library network managers, which also poses hidden dangers for library information network security.

3. Measures to Strengthen Library Digital Network Security

3.1 Strengthen the Awareness of Network Security of all Librarians

The ambiguity of information network security is a major difficulty in information security management in the library community. Therefore, strengthening management and training of staff

members is of great significance for ensuring the security of library network information.

3.1.1 Establish and Improve Library Network Security Management System

Digital library network information security is a sophisticated network system project, which must have systematic management and emergency measures[5]. According to the requirements of library computer network systems and data resource security, strengthen safety awareness education, establish and improve relevant safety management systems and formulate operational procedures for each position. For example, establish a safety management system, standardize the operational procedures of various businesses, clarify the responsibilities of management personnel and operators, and conscientiously implement daily data backup, remote backup, real-time backup of important data, password setting and storage system, and do a good job in computer virus monitoring and prevention. Strictly implement various safety precautions, improve the sense of responsibility of technical personnel, strengthen responsibility supervision, and follow the principle of "pre-existing prevention, in-process control, and post-event auditing" [6], do a good job in the safety of computer network systems, and truly use the system to standardize behavior, implement management according to responsibilities, and protect according to standards.

3.1.2 Strengthen Coordination among various Departments of the Library

Network security is a systematic project. In addition to the technical work system, other staff members of the library should actively understand the network security knowledge, participate in relevant technical training and learning, and enrich their knowledge of network security. Do not install foreign software at will. Seriously do the anti-virus work of mobile devices to ensure the security of the entire network system of the library.

3.2 Strengthen the Construction of Software and Hardware Environment

3.2.1 Hardware Environment Construction

Strengthen the establishment of basic settings for network information security, enhance the reliability of communication lines and the security of hardware and software equipment, back up equipment, improve the disaster prevention capability of equipment, prevent electromagnetic radiation leakage and anti-electromagnetic interference, and prevent equipment theft. Loss and damage. Regularly maintain the equipment to prevent the entire network from being damaged due to equipment components.

The firewall is an important infrastructure to protect information security. It can separate the internal network of the library from the external network and protect the operation between the internal network and the external network[7]. In the network construction of the library, firewall equipment should be deployed between the intranet and the intranet between the intranet and the intranet.

3.2.2 Software Environment Security and Protection

Choose a higher security operating system, a properly certified application, and database security software.Timely patch the system, do a good job of system vulnerability repair[8]; keep the server automatically updated; do not install other applications that are not related to the system service on the server; block unnecessary service components; periodically check system log files, and find problems in time.In addition, security inspection tool software should be used to regularly check system security issues in order to promptly fix system security vulnerabilities.

3.3 Establish a Comprehensive Security System

3.3.1 Rational Planning of the Network Using Virtual Local Area Network Technology

University libraries use virtual local area network (VLAN) technology to group corresponding servers, users and other network objects located in different geographical locations, and set corresponding security and access rights [9]. Computers form corresponding virtual network working groups according to automatic configuration.

3.3.2 Access Control

By establishing an access control system for specific network segments and services, most attacks are blocked before reaching the target.

3.3.3 Checking for Security Vulnerabilities

Through periodic inspection of security vulnerabilities, even if an attack can reach the target, most attacks can be invalidated.

3.3.4 Intrusion Detection Technology

Intrusion detection technology is an active security protection technology. It not only enables system managers to keep abreast of the security status of the system, but also provides security policies and guidance for managers. The digital library system can prevent security attacks , virus intrusion, hacker malicious attacks, and network operation monitoring, all through intrusion detection technology. Through the attack monitoring system established for specific network segments and services, most of the external attacks are detected in real time, and corresponding actions are taken (such as disconnecting the network, recording the attack process, and tracking the attack source, etc.).

3.3.5 Certification System

A good certification system prevents attackers from impersonating legitimate users.

3.3.6 Data Disaster Recovery Technology

Data disaster recovery security strategy refers to disaster recovery strategy and backup strategy of library service resources[10]. Good backup and recovery mechanism can restore data and system service as soon as possible in case of loss caused by attack.

3.3.7 Setting up a Security Monitoring Center

Provide safety system management, monitoring, drainage protection and emergency services for information systems.

3.3.8 Establish an Emergency Response Mechanism

First, do a good job in network information security risk assessment, and secondly, establish an emergency plan for information security emergencies, and finally deal with information security emergencies[11].

4. Conclusion

Due to the complex and versatile network environment and the vulnerability of information systems, the objective existence of security threats in library information networks is determined. Today, with the rapid development of digital and networked libraries, it is indispensable to strengthen security supervision and establish a protective barrier. The network has no absolute security. It is only a relative security. The higher the security factor, the higher the cost. It will inevitably consume network resources or limit the use of network resources. Only by combining security technologies and measures effectively, rationally and flexibly, to find the best balance between network security and the reader's comprehensive information needs.

References

[1] LiangChao Wang. Discussion on Network Information Security of Digital Library[J]. Modern Communication.2019 (6):136-137.

[2] WenYuan Li.The Network Information Security of Digital library[J]. Library Tribune.2003 (2):54-56.

[3] ShouWu Yu. Analysis of Network Security Construction of Digital Library in Colleges and Universities [J]. Computer and Information Technology.2018 (10):54-57.

[4] Li Jing. Analysis on Network Security in University Library[J]. Sci-Tech Information Development & Economy.2010 (12).22-24.

[5] Tao Ran. Zhang Ying. Su Ning. Shuwen Wang. Research on Network Information Security of Digital Library [J]. Information Recording Materials.2019 (2):50-51.

[6] Chen Li. Zhumei Cheng. Fang Hong. Research on information security and management of Digital Library[J]. Journal of Hunan City University (Natural Science).2016(7):97-98.

[7] ShiFen Tan. The Construction of Network Information Security System in University Libraries——Taking the Library of Hebei Medical University as an Example [J].Industrial & Science Tribune.2014 (8):229-230.

[8] ZhangLin Tang. Network Security of Digital Library under Network Environment [J].Library World.2007 (2):60-63.

[9] ChangMao Yan.Yinjian Zhou.Li Peng. Construction of Network Security System of University Library [J]. Information Research.2014(1):108-111.

[10] Ni Ping.WenBing Wang.Ni Jun.Research on the Security Policy Framework of Digital Libraries under Ubiquitous Network Environment [J]. Journal of Academic Library and Information Science.2018 (4):10-16.

[11] Peng Huan. Current situation and countermeasures of network information security in digital library [J].Software Guide.2015 (6):167-170.