Discussion on Safety Planning of Information Campus

Wei Li[1] and Jianfeng Xiong[2]
[1]College of Computer, Wuhan Vocational College of Software and Engineering, Wuhan Hubei 430205, China
[2]The first secondary vocational school in Zhuhai, Guang Dong, 519000, China

***Abstract*—Aiming factors that affect the information technology campus safety, we design and plan the campus security information application, from the host system security, data security, application level security, application classification system permissions and other aspects, in order to achieve information on the campus to provide security protection.**

Keywords-information campus; access control; log; data backup overview

I. INTRODUCTION

With the rapid development of network-centric information technologies, methods of information dissemination has undergone a major change, Information campus development has provided conditions for information technology on campus ,it also can provide information timely access, automation, networking, digital management. In the information technology campus construction process, due to the shared computer network and the distributed wide area, it is easy to appear all sorts of information destruction in the information resources[1]. At the same time, due to the hardware failure which may arise, software failures, operational errors and staff, are likely to bring data destruction, along with the ongoing campus information technology, security issues will become increasingly prominent, sharing data and resources contradictions between the network security will also become increasingly prominent, it is very important to guarantee the safe operation of the campus network information system.

II. SAFETY SYSTEM DESIGN

Information Campus bring a variety of convenience, but also bring a lot of security issues such as hacking, virus outbreaks, unauthorized users invasion, we need to ensure information security under the premise, to provide users with high-quality network information services[2]. Good information security management on the premise that campus security threats and problems have a full understanding and predictability. The design of campus security system information, including physical security, software security, data security, must be fully considered in the design of economic security system, so we must firstly consider all kinds of security risks from the internal and external networks for analysis, and then formulate appropriate safety objectives and security policies, and establish a security model, and finally form a rational, comprehensive information security system as the system configuration, basic management and application security framework. On this basis, the access control, encryption and authentication technologies and other will be applied on the system[3].

III. PHYSICAL SECURITY DESIGN

The basic structure of Information Campus is the physical condition of equipment, such as computers, network equipment and so on. The physical security equipment include safety and security environment.

A. Environmental Safety

Environmental impacts need to be considered in the integrated design. The first environmental safety is the environmental safety room, safety items include site selection, fire, power supply and distribution systems, fire alarm and fire-fighting equipment. Secondly, UPS is essential, because there may be power instability, unexpected power outages. Then taking into account the mutual influence of the wiring between the lines, at this time it must be well shielded, including the line in which the shield tube will be used[4].

B. Device Security

Safety equipment includes anti-theft devices, anti-destruction, anti-electromagnetic interference. The equipment safety mainly includes the equipment security, the anti - destruction, the anti electromagnetic interference and so on. For lightning, earthquakes, fires and other natural disasters caused by equipment failure is also the focus of equipment safety. Server is the key to a secure system. In server business-critical systems , fault-tolerant disaster recovery and load balancing techniques should be used to improve the reliability and security of the system. Server has redundancy, the best backup server, when the problem is appeared in the main server, backup server can provide services at any time. When the server to read and write operating frequency is much more than ordinary desktop, we must use a dedicated server hard disk.

IV. SOFTWARE SECURITY DESIGN

The factor of software security is one important factor restricting information campus security[5]. The software reliability is the probability that the software does not cause the failure in the specified time, and the failure of the software is the basic reason for the poor reliability of the software. Software security design should also consider the fault-tolerance and anti-virus infected systems.

A. Software Selection

On the operating system, the stability and security of UNIX is greatly more than Windows, the Oracle database system stability is also better than SQL Server, under the conditions permit, as far as possible the choice of UNIX + Oracle configuration[6].

B. System Status Check

Before the end of each working day and off, in addition to the data, files of the day should be backup, you also need to record the main data files and program files of the system. These data include: file name, file size, last modification date, time, etc., which should be checked at each start-up.

C. The system Logging Mechanism

System logging mechanism is used to record the whole process of system operation. System log files are generated automatically and is transparent to users, which include: date, time, user name, file name, operation, operation mode, the operation content, the system runs its supervision, maintenance analysis, fault recovery, can play a very important role[9]. To prevent unauthorized users from legitimate users access to data or systems in order to avoid operation of the supervisory system log data obtained for the system to take important data is stored in an encrypted format. Enable system account functions in the computer system, which set a record file system running on the system in which each user can enter the system time user registration and login times, accurately recorded and automatically record the user number, terminal number , switch time and frequency[7].

D. Software Maintenance

For a number of risks present in the system, it should take appropriate measures to maintain security.

Timely installation of the operating system and server software , the latest version and patches. Some loopholes in the system are continuously found, the software vendor will typically release a new version or patch to patch security holes to keep using the latest version of security ,so the threats can be minimized.

Necessary security configuration , shut down a security risk or unnecessary services, such as system configuration: FTP, Telnet, login, shell, TFTP, etc. Some security risks exist in these protocols. R prohibit certain commands, such as: rsh and so on.

Restricted key system files (such as password UNIX under, shadow, group, etc.) using permissions.

Establish the computer virus prevention measures, strengthen management, and constantly update anti-virus software version[8].

Strengthen the authentication login process, set up the complex login password which is difficult to guess, tightly protect the account password and frequently change to prevent the unauthorized users easily guessed passwords, ensure the legitimacy of users, restrict unauthorized users from accessing the server.

V. DATA SECURITY DESIGN

Information Campus involved in the data including object data storage layer, metadata, and a computer system, the data security including confidentiality, integrity, availability, controllability and non-repudiation of data. Data security is the main contents of database security and data backup and recovery.

A. Database Security

1) Basic Access database: Provided by the database system privileges, object privileges (query, modify, delete, insert, etc.) to control, and the use of the appropriate role of classification authority, so the authority management will be more flexible.

2) Data-level permissions: Data-level permissions achieve by controlling the domain. Firstly, through the definition of the data domain, data will be divided into different ranges according to different domain, when an operator is assigned to the domain, the operation staff won the authority of the operation of the data of the data domain, the operator not to other data in the domain of data operation.

3) Database Encryption: To encrypt some sensitive table only after verification by the order of the table read and write operations, so operation on these tables or malicious changes will be avoided.

4) The database log: By using archive log analysis tools which are provided by Oracle, the database can analyze the whole process of data manipulation, and find safety problems and timely solutions[9].

5) The database audit: Through the security audit records and tracking user operation of the database, denied responsibility for security to prevent the database.

B. Data Backup and Recovery

To ensure data security, to ensure that emergency treatment in case of emergency, it is necessary to use data backup and recovery mechanisms, methods include local backup and remote backup. Taking into account cost factors, local backup is a good choice, send the backup data to the remote equipment after the backup locally, which effectively solves the influence of spontaneous combustion of disasters. When some problems appear in the system data, the data recovery system for corrupted data recovery. All sectors and databases at all levels need to take regular database backups, off-site backup and other measures. For different business needs, we alternatively take synchronous and asynchronous replication on the off-site backup regularly. It should be ensured security of the database mirroring technology to the key database system. Keys and other critical security parameters security system is an important safety equipment, which should also be treated as a backup to avoid key or critical security parameters affect the security device loses its normal business[10].

C. Error Log and Run Log

Log data security is an important means to promote unity Log format and handling mechanism, the provisions of the following basic principles:

Log format unified, clear, legible and strong;

Log level in the development and operation of the adjustment period, in order to prevent a lot of unnecessary run-log information storage medium is full;

Log in the recording process, we should try to avoid too much competition for business systems and I / O resources;

Log output device can be flexibly configured, common are: files, databases and so on. In the Cluster environment, the database is a good choice.

VI. Application Level Security

A. Authentication

Authentication involve in the database authentication, application certification, CA certification, etc., only legitimate users can log in to the application system[11].

B. Multi-Level Access Control

There are many functional modules in applications, even the legitimate users can not operate all of the modules, the appropriate function module will be granted according to the user's department. The same data can be set different operating authority: authority to query, entry permissions, auditing authority, the approval authority.

C. Application of the System Log

Information log management track record user login system, the business module operation as well as libraries and tables of information operations, including user name, operating modules, important library table type of operation (add, delete, change), field operations before and once the value of the operation[12]. Through log management, in the event of malfunction can be easily rolled back process.

D. The module-Level Permissions

Module-level permissions can be realized through the role of the superior access control, lower privileges need to obtain permission from the superior authority. When adjusting the higher authority, system will automatically adjust the lower authority, in other words that is canceled when a permission from the parent permissions, the lower permissions also canceled the same permissions.

VII. Conclusion

Campus safety information is comprehensive, is a perennial need for complex system engineering implementation, which requires a holistic, multi-level security policies. System security policies must complement each other in order to truly play a role[13]. The establishment of a campus information system security, security information for the promotion of campus network and information security is of great significance.

References

[1] Muhammad Khurram Khan, Khaled Alghathbar, Cryptanalysis and Security Improvements of 'Two-Factor User Authentication in Wireless Sensor Networks', Sensors (IF 1.953), 2010, Vol.10 (3), pp.2450.

[2] Hyunsung Kim, Privacy Preserving Security Framework for Cognitive Radio, IETE Technical Review (IF 0.705), 2013, Vol.30 (2), pp.142-148.

[3] Alina Olteanu, Network security: Design, analysis and tradeoff evaluation, The University of Alabama 2009CNKI.

[4] Haiyan Cai. Information security and virus protection methods institution local area network [J] Electronics and Software Engineering, 2016,11: 237-238.

[5] Xinke Ma , Wu Shuang. Large university network security information security concept construction [J] China Science and Technology Information, 2016,12: 111-113.

[6] Liu Jie, Yuanyuan Chen. Campus network security Higher Colleges and Prevention Strategies Thinking [J] e-commerce, 2016,07: 43 + 62.

[7] Tang Yu. Construction of Government Portal security system [J] Science and Innovation, 2016,14: 39-40.

[8] Fengni Zheng. University information and cost [J] Computer and Modernization, 2016,07: 124-126.

[9] Libo Wang, Zhang Wei , Wentao Deng. University information system analysis of the evolution [J] Henan University of Technology (Social Science Edition), 2016,02: 148-153.

[10] Zhang Jian, Wang Qi .Necessity of management information systems security in the [J] information network security, 2012,06: 1-2.

[11] Guoyong Zhou, Chen Lei. Information system security inspection system designed study [J] information network security, 2012,08: 167-169.

[12] Zhang Kun, Ma Li, Yafei Xu. Scythians non-research complex information system security system [J]. Chinese Journal of Management Science, 2000, S1:.. 336-346.

[13] Guangfeng Xia. Research campus network security system design and deployment of [D]. Hefei University of Technology, 2008.