International Journal of Economics, Finance and Management Sciences
2022; 10(6): 340-347
http://www.sciencepublishinggroup.com/j/ijefm
doi: 10.11648/j.ijefm.20221006.15
ISSN: 2326-9553 (Print); ISSN: 2326-9561 (Online)

Research on the Architecture of Information System Security Management Platform of Real Estate Management Center

Jie Zhang

Department of Business Administration, Chaohu University, Hefei, China

Email address:

jiejie.0927@163.com

To cite this article:

Jie Zhang. Research on the Architecture of Information System Security Management Platform of Real Estate Management Center. *International Journal of Economics, Finance and Management Sciences*. Vol. 10, No. 6, 2022, pp. 340-347. doi: 10.11648/j.ijefm.20221006.15

Received: September 19, 2022; **Accepted**: November 9, 2022; **Published**: November 14, 2022

Abstract: In recent years, with the continuous development of social economy, the scale of the network and the amount of information have increased dramatically, and network information security has been paid more and more attention. The promotion of "Internet + real estate registration" and the application of registration information sharing have brought great challenges to the security management of real estate registration information. How to strengthen the security management of relevant systems has become a practical consideration for local registration authorities. The implementation of the new mode of real estate registration brings great challenges to information security management. This research mainly refers to the domestic mainstream management system architecture, the requirements of the National Computer Information System Security Protection Classification Criteria (GB 17859-1999), and the advantages and disadvantages of the existing management platform through the hierarchical classification analysis method of the management system. The future oriented flat management platform architecture is proposed according to the business system interface, which not only meets the existing business needs, but also has the ability to dynamically expand capacity. The overall management platform architecture is characterized by scientificity, advancement and expandability, which fundamentally solves the hidden danger of information system security management and realizes the controllable whole process of the management platform.

Keywords: Information Security, Architecture, Management Platform, Flat

1. Introduction

On July 31, 2018, the Ministry of Natural Resources issued a notice on comprehensively promoting the convenience of real estate registration for the People. The circular called for deepening "Internet plus government services", changing "people running errands" to "data running errands", continuously expanding online affairs, and comprehensively promoting the convenience of real estate registration for the people. The provinces continued to deepen the reform of "releasing regulation and service", and made it easier for people to handle affairs through the interactive sharing of data information system management. However, while bringing great convenience to the public, great changes have been made to the management and operation environment of the original real estate registration information system and the requirements for interaction and sharing. The security risks of real estate registration information are gradually increasing. How to strengthen the security management of relevant systems is becoming a practical consideration for local registration agencies [1].

On the one hand, the promotion of "Internet + real estate registration" information system management has broken the original independent operation environment. At present, all localities actively promote the new mode of "Internet + real estate registration", and the physical office hall is gradually extended to the online office hall, and the online service matters such as reservation, pre-application, pre-acceptance, inquiry, payment, e-certificate, and even real-time file checking are gradually popularized. Under the new management mode, the original environment of the real estate registration operating in the physical isolation of the land and resources private network is gradually broken, and the real estate information system management operating in the land and resources private network is gradually connected with the external network of government affairs and the Internet.

On the other hand, the office to submit data simplification, real estate information sharing scope is broader. According to the documents of The General Office of the State Council, no one shall be required to submit the materials that can be obtained by departmental information sharing through administrative means. Local governments have made great efforts to streamline their work and submission materials, and have realized the review of their work through data sharing. There are many cases in which the registration of real estate requires the submission of the real estate ownership certificate or filing materials, such as the court to freeze assets, the bank loans, to buy a house, school, starting a business, as well as water, electricity, gas, open an account or change, etc., all need to share real estate management information system of real-time query, real estate management information system in real time Shared with great demand is high, the scope, object, Its information security risk also becomes big accordingly.

2. Demand Analysis

The management principles of "Internet plus government services" are resource integration, data sharing, process optimization and service innovation. We will adhere to the principle of building a management system based on the Internet and general offices, make it a principle for government service management platforms to access the Internet, and an exception for them not to [2]. We will strengthen cross-level, regional, system, department, and business connectivity and collaborative sharing of government information resources. We will make use of information technologies such as the Internet, big data and artificial intelligence, and enhance our comprehensive service capacity through management technology innovation and process reengineering to further improve the efficiency of government services.

In order to meet the needs of information technology in the new era, it is urgent to strengthen the security of the existing real estate registration information system. The data sharing area is planned and designed for the "Internet +" business scenario. Implement data backup for core data services and remote disaster recovery for service systems. The main contents of the construction include the following four points.

2.1. The System Network Management Capability Is Strengthened

In view of the existing management system, involves the network equipment parts, according to the current situation, network equipment is single node equipment scenario, this part is the network security hidden danger (single equipment failure can cause entire network business interruption), needs to be the part of the network into a "1 + 1" double node equipment, implement equipment main equipment protection ability, promote private network management system reliability.

2.2. Real Estate Registration Management System Security Reinforcement

In order to improve the security capability of real estate registration information system, intrusion prevention, anti-virus, fortress machine, log audit, database audit, vulnerability scanning and other capabilities [3]. As a result, the real estate registration information system has completed the equal protection evaluation and obtained the "Three-level protection Record Certificate of the Real Estate Registration Information System", thus realizing the core competence of the information system security management platform.

2.3. Data Sharing

In order to meet the demand of "Internet + real estate registration" construction, comply with the relevant national policies, the need to build data sharing management area, in order to satisfy the government affairs, taxation, industry and commerce, public security, civil affairs, court, finance and other departments of information sharing, data sharing and exchange, custom service, information service interface functions.

2.4. Data Security

To ensure the security of core data, it is necessary to build remote data backup capability. To ensure the stable running of system applications and reduce the impact of services in the production environment due to irreversible factors such as service breakdown, a remote Dr System must be set up to take over services when the production environment is interrupted.

3. Security Management Platform Architecture

The security management platform of the information system of the Real estate management center is designed according to the core management module. The overall architecture planning is divided into Intranet and extranet. The Intranet is divided into outreach area, operation and maintenance area, server area, and disaster area.

The overall security scheme topology is shown in Figure 1.

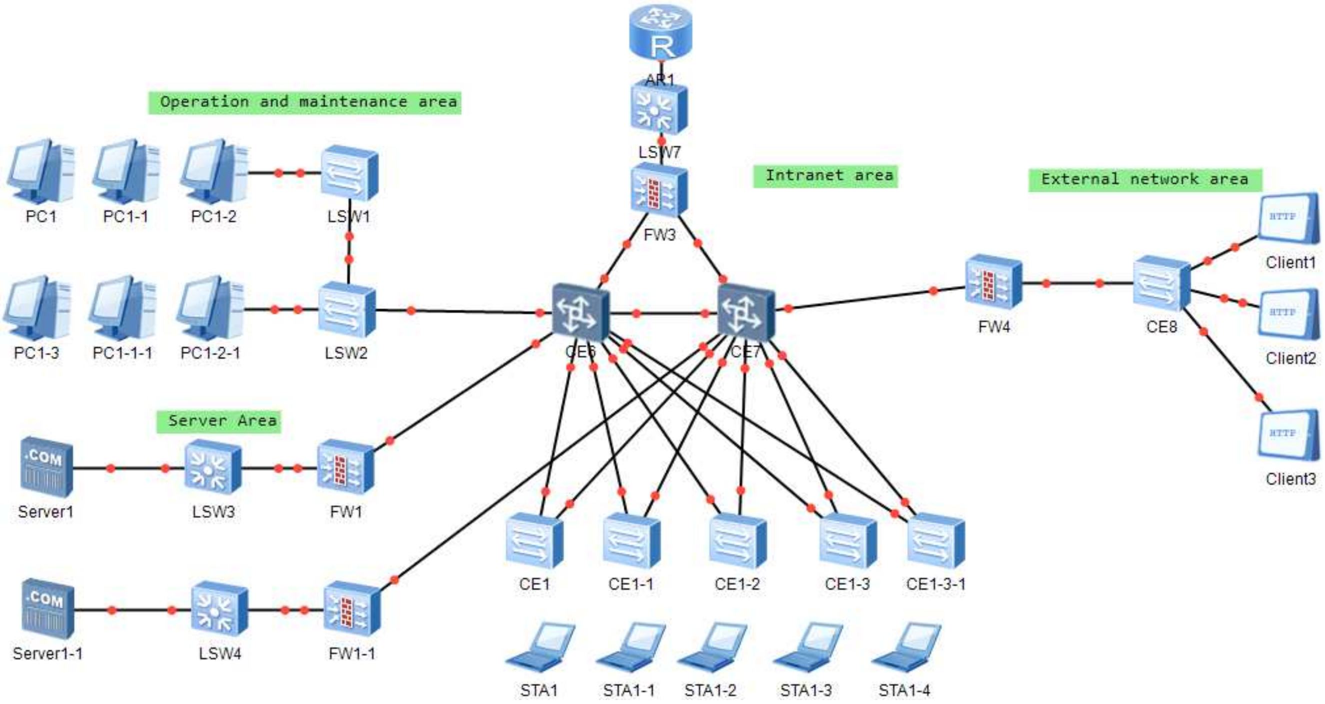

Figure 1. *Security solution topology.*

This architecture refers to the level 3 national standard of protection. The Intranet is constructed from the following aspects.

3.1. Information Security Level Protection Management System

The existing core network is in a single operation state. When the real estate registration and digital city services go online, the stability of the network will affect the security of the entire information technology. This scheme firstly suggests that the internal and external networks simultaneously adopt switch stacking to improve the stability of the network. Firewalls are deployed in each security zone on the Intranet to improve the security of the security zone boundary. Data ferry products are deployed on the Intranet to improve the security of data exchange. The terminal security management product is deployed on the Intranet to improve the security of Intranet terminals. Network antivirus products are deployed on the Intranet [4] to improve the defense capability against Intranet viruses. Deploy log audit products to improve the ability to collect and analyze security events. Deploy O&M audit products to improve O&M efficiency and safety, especially to reduce security risks of external O&M personnel.

3.2. Deployment of the Integrated Network Management Platform

Improves the monitoring and management capability of all network devices, servers, and storage resources, so that what you see is what you get. Network gates and intrusion prevention devices are deployed between the Intranet and extranet to improve the security of data transmission between the Intranet and extranet. Terminal security management software is deployed on Intranet and extranet terminals to improve the security of USB flash drive and wireless interconnection.

3.3. Data Protection Management System

The network gate is deployed between the Intranet and the extranet to improve the security of data transmission between the Intranet and extranet. Data exchange devices are deployed on the Intranet to improve the security of data exchange between the Intranet and the extranet.

In a word, deploy ORACLE RAC environment for real estate registration system to achieve high availability of database; Provide backup scheme for local data and remote backup scheme at the same time; Firewalls and intrusion prevention devices are available in the Internet zone. Based on the Level 3 standards, it is recommended to strengthen the firewalls in the Internet zone in the following ways: Add a network gate to connect the Intranet and the extranet, and add a firewall product in the front end.

4. Security Management Platform Implementation

4.1. Construction of Identity Authentication Management System

The security of terminals in the network can be effectively controlled through unified identity authentication and admission control. The identity authentication management system can be divided into two aspects: host identity authentication and application identity authentication [5].

4.1.1. Managing Host Identity Authentication

To improve the security of the host management system and ensure the normal running of various applications, a series of hardening measures are required for the host management system. The measures include: Identifying and authenticating users who log in to the operating system and database system, and ensuring the uniqueness of user names; Configure the user name and password based on the basic requirements; The password must be of at least 3 characters, at least 8 characters in length and changed periodically; Enable the login failure handling function. After a login failure, take measures such as ending the session, limiting the number of illegal logins, and automatically exiting. During remote management, you need to enable SSH to encrypt management data and prevent network eavesdropping. The two-factor authentication mode is adopted for host administrator login, and the USB key and password are used for identity authentication [6].

4.1.2. Applying Identity Authentication

In order to improve the security of the application system, the application system needs to take a series of hardening measures, including: identifying and authenticating the login user and ensuring the uniqueness of the user name; The user name and password must be complex according to the basic requirements; The password must be of at least 3 characters, at least 8 characters in length and changed periodically; Enable the login failure handling function, after a login failure, take measures such as ending the session, limiting the number of illegal logins, and automatically exiting. If the application system has the above functions, it needs to be opened for use, if not, it needs to carry out corresponding function development, and the use effect should meet the above requirements.

For a three-tier management system, two or more authentication technologies are required. Therefore, you can use two-factor authentication (USB key+ password) or build a PKI system and use CA certificates to authenticate users.

4.2. Access Control Management (ACL)

An important requirement of the three-level system is to implement autonomous access control and mandatory access control. Autonomous access control implementation: Within the scope of security policy control, the user has a variety of access operation permissions to the object created by himself, and can grant some or all of these permissions to other users; The granularity of the subject of autonomous access control should be user level, and the granularity of the object should be file or database table level; Autonomous access operations should include creating, reading, writing, modifying and deleting objects. Implementation of mandatory access control: on the basis of strict identity authentication and permission control for the security administrator, the security administrator carries out security marks for the host and object through a specific operation interface; The operation of determining the subject's access to the object should be controlled according to the security mark and mandatory access control rules; The granularity of the mandatory access control principal should be at the user level, and the granularity of the object should be at the file or database table level [7].

In this way, access to resources such as files and databases of the application system is controlled to avoid unauthorized use. The measures include: Enabling access control: Formulate strict access control security policies to control users' access to the application system, especially file operations and database access, based on the policies. The subject of the control granularity is at the user level and the object is at the file or database table level. Permission control: The access control rules must clearly cover the subjects and objects related to resource access and the operations between them. The principle of authorization for different users is to minimize the authorization to complete the work, avoid excessive authorization scope, and form a mutually restrictive relationship between them. Account management: Strictly restrict the access rights of the default account, rename the default account, and change the default password. Delete unnecessary and expired accounts in a timely manner to avoid sharing accounts. The implementation of access control mainly adopts two ways: using a secure operating system, or security enhancement of the operating system, and the use of the effect to meet the above requirements.

4.3. Managing System Audits

Management system audit includes host audit and application audit.

Host management audit: Deploy the terminal security management system and enable the host audit function, or deploy the host audit system to monitor, audit, and manage hosts. The audit scope covers each operating system user and database user on the server. The audit content should include important security events in the system, such as important user behaviors, abnormal use of system resources, and use of important system commands [8]. The audit record shall include the date, time, type, subject identification, object identification and result of the event.

Application management audit: Application-layer security audit audits the behaviors of the service application system and must be closely integrated with the application system. This audit function should be developed in a unified manner with the application system. Use the system audit function to record the date, time, initiator information, type, description, and result of major security events, and protect the audit results to prevent unauthorized deletion, modification, or overwriting of audit records. At the same time to record data statistics, query, analysis and generate audit reports. Deploy the database audit system to audit user behavior, user events and system status, so as to grasp the overall security of the database system.

4.4. Managing System Intrusion Prevention

Management system intrusion prevention is mainly implemented at the host and network levels.

4.4.1. Intrusion Prevention Against Hosts

The intrusion prevention against host can be handled from many perspectives: intrusion detection system can prevent the intrusion against host; Deploy vulnerability scanning for system security detection; Deploy the terminal security management system and enable patch distribution to upgrade system patches in a timely manner.

Install only required components and applications, and stop unnecessary services. In addition, harden other security configurations based on the system type. To prevent network intrusion, it can be realized by deploying network intrusion detection system. The network intrusion detection system is located on the network with sensitive data to be protected [9], and it searches for network violation patterns and unauthorized network access attempts by listening to the network data flow in real time. When a network violation or unauthorized network access is detected, the network monitoring system can respond according to the system security policy, including real-time alarm, event login, or user-defined security policy.

Intrusion detection systems can be deployed in the core and main server areas. It is recommended to deploy intrusion detection systems on switches in these areas to monitor and record all access behaviors and operations on the network to effectively prevent illegal operations and malicious attacks. At the same time, the intrusion detection system can also vividly reproduce the operation process, which can help the security administrator to find the hidden dangers of network security. It should be noted that IPS is a necessary addition to firewalls rather than a simple supplement. As the second line of defense of network security system, intrusion detection system can minimize the corresponding loss when the firewall system fails to block the attack. Therefore, the IPS must have more detection capabilities and can interwork with other security products, such as border firewalls and Intranet security management software. All kinds of malicious codes, especially viruses, trojans, etc., are serious hazards [10]. When viruses break out, they will make the performance of gateway devices such as routers, layer 3 switches and firewalls rapidly decline, and occupy the bandwidth of the entire network.

In view of the risk of the virus, the recommendation focuses on eliminating or blocking the virus at the source of the terminal. For example, the network antivirus system can be deployed on all terminal hosts and servers to enhance the antivirus capability of terminal hosts and timely upgrade the malicious code software version and malicious code base.

In the safety management of security domain, which can be deployed antivirus server, is responsible for the formulation and terminal host antivirus strategy, trying to establish a consolidated tech-oriented level upgrade the server, and in the lower nodes to establish secondary to upgrade the server, the management center to upgrade the server via the Internet or the manual way to get the latest virus signature files, distributing to each terminal, data center node And deliver to each secondary server. The filtering control based on the communication port, bandwidth and connection quantity through the firewall at the network boundary can avoid the heavy traffic impact caused by the worm outbreak to a certain extent. At the same time, the anti-virus system can provide the security management platform with monitoring and auditing logs about virus threats and events, and provide necessary information for the whole network virus protection management.

Resources must be controlled to ensure that the application system can properly provide services for users. Otherwise, resources may be exhausted, service quality may be degraded, or services may be interrupted. The application system can be developed or configured to achieve the following control objectives: Automatic session termination: When one of the two communication parties in the application system does not make any response within a period of time, the other party can detect and automatically end the session to release resources. Session limit: Limits the maximum number of concurrent session connections in an application system, the number of concurrent session connections that can be allowed within a time range, and the number of concurrent sessions that can be allowed for a single account. The related threshold is set to ensure system availability. Login conditions: restrict terminal login by setting conditions such as terminal access mode and network address range. Timeout lock: Sets the terminal login timeout lock based on the security policy. Available resource threshold: limits the maximum or minimum usage of system resources by a single user to ensure proper resource usage. Monitor the resources of critical servers, including CPU, hard disk, memory, etc. Detect and alarm when the service level of the system decreases to the minimum specified in advance. The system provides the service priority setting function, and sets the priority of access accounts or request processes based on the security policy after the installation, and allocates system resources based on the priority. If the application management system has the above functions, it needs to be opened to use, if not, it needs to carry out corresponding function development, and the use effect should meet the above requirements.

Backup and recovery mainly include two aspects, the first is data backup and recovery, on the other hand is the redundancy of key network equipment, lines, servers and other hardware devices. Data is the most important system resource [11]. Data loss will prevent the system from continuously working properly. Data errors will mean inaccurate transaction processing. A reliable system requires immediate access to accurate information. Implementing a comprehensive storage strategy as part of the computer information system infrastructure is no longer an option, but an inevitable trend. The data backup system should follow the principles of stability, comprehensiveness, automation, high performance, simple operation and real-time performance. Advanced features of the backup system provide enhanced performance, ease of management, broad device compatibility, and high reliability to ensure data integrity. A wide range of options and agents extend data protection to the entire system and provide enhanced capabilities, including online backup of application systems and data files, advanced device and media management, fast and smooth disaster recovery, and support for Fiber-channel storage area Networks (SAN). Local full data backup requires a complete backup policy [12], and backup media must be stored off-site. Provides remote data backup function, and uses the communication network to transmit the key data to the remote standby site in batches. The core switching devices, external access links, and system servers are designed with dual-node and dual-line redundancy to meet the requirements of uninterrupted system operation in terms of network structure and hardware configuration.

4.4.2. Network Management Architecture Security

The security of the network management architecture and the rationality of the network structure directly affect whether it can effectively carry the business needs. Therefore, the network structure needs to have some redundancy. In general, when selecting the main network equipment, it is necessary to consider the peak data flow of the business processing capacity, and consider that the redundant space meets the needs of the business peak; The bandwidth of each part of the network should ensure that the access network and the core network meet the needs of the business peak; Define the priority of bandwidth allocation according to the importance order of business system services, and give priority to important hosts in case of network congestion [13]; Reasonably plan the route, and establish a safe path between the service terminal and the service server; Draw the network topology diagram consistent with the current operation; Different network segments or VLANs are divided according to the work functions and importance of each department and the importance of the information involved. The important network segments that contain important business systems and data cannot be directly connected to external systems. They need to be isolated from other network segments and divided into separate regions.

At present, although there are generally two core switches in the network management of the prefecture-level real estate management center, the physical structure does not realize the redundancy function, which needs to be adjusted. In addition, the information center also needs to be connected with the new office building and the administrative office building, so the design of high reliability is needed to ensure the redundancy and bandwidth.

Network access control Through regular network boundary risk identification and demand analysis, firewall and access products need to be deployed for access control at the network layer. All data packets flowing through the firewall can be filtered according to strict security rules, and all data packets that are unsafe or do not conform to the security rules are shielded to prevent unauthorized access and illegal attacks. At the same time, it can conduct security linkage with the intranet security management system and network intrusion detection system to create a comprehensive and in-depth security defense system for the network [14]. The firewall has been deployed in the current network, and the network is not strictly divided into regions. It is recommended to divide regions for management in the later stage.

The network security audit system is mainly used to monitor and record various operations in the network, detect existing and potential threats in the system, and comprehensively analyze security events occurring in the network in real time, including various external events and internal events. The network behavior monitoring and auditing system is deployed in parallel at the switch to form the flow monitoring of the whole network data and carry out the corresponding security audit. At the same time, it provides monitoring data for analysis and detection together with other network security devices for centralized security management. The network behavior monitoring and auditing system connects the independent network sensor hardware components to the data aggregation point devices in the network, analyzes, matches, and counts the data packets in the network, and implements network auditing functions such as intrusion detection and information restoration through specific protocol algorithms, and generates detailed audit reports according to records [15]. The network behavior monitoring and auditing system adopts bypass technology, without installing any components in the target host. At the same time, the network audit system can link with other network security devices, send their monitoring records to the security management server in the security management security domain, and focus on analyzing and detecting network exceptions, attacks and viruses. In addition to behavior audit, audit events in the network can be collected through log audit, IDS, etc., so as to improve network security.

Boundary integrity check The core of boundary integrity check is to check the behavior of internal users who are not allowed to connect to the external network in order to maintain the integrity of the network boundary. This goal can be achieved through the network access control module integrated in the IT integrated service management platform. One of the important functions of the network access control module is illegal outreach control to detect computers illegally accessing the network in the Intranet. Illegal outreach monitoring mainly solves the problem of discovering and managing the behaviors that users illegally establish their own channels to connect to unauthorized networks. The management of illegal outgoing monitoring can prevent users from accessing untrusted network resources and prevent security risks or information leaks caused by accessing untrusted network resources.

The monitoring of illegal outgoing behaviors of terminals can detect the behaviors of terminals that attempt to access non-credit network resources, such as trying to communicate with terminals that are not authorized by the system or trying to connect to the Internet through dial-up. Logs can be recorded and alarm messages can be generated for illegal outreach activities found. Unauthorized outgoing behavior management of terminals prevents terminals from communicating with terminals that are not authorized by the system and prevents dial-up Internet access. Network intrusion prevention At the boundary of each area in the network, the firewall plays the main role of protocol filtering, according to the security policy in the network layer to judge the legitimate flow of data packets. However, in the face of more and more attacks based on application layer content, firewall is not good at processing application layer data.

Firewalls have been designed and deployed at the network boundary and in the security zone of the main server area to strictly control access to each security zone. In view of the above analysis of the core role of the firewall, it is necessary to cooperate with other devices capable of detecting and defending new hybrid attacks and firewalls to jointly defend against various types of attacks from the application layer to the network layer, establish a complete set of security protection system, and carry out multi-level and multi-means detection and protection. The intrusion prevention system (IPS) is an important part of the security protection system. It can timely identify the intrusion behaviors in the network and make real-time alarm and effective interception and protection.

IPS is a future-oriented new security technology following traditional security protection methods such as firewall and information encryption. It monitors events occurring in a computer system or network and analyzes them to find and effectively intercept intrusions that compromise the confidentiality, integrity, availability of information or attempt to bypass security mechanisms. IPS is a hardware product that automatically performs this monitoring and analysis process and also performs blocking. After the IPS is connected to the firewall in series, the firewall will implement access control to ensure the legitimacy of the access. After that, the IPS dynamically protects the intrusion behavior, detects the access status, communication protocols, and application protocols, and performs in-depth detection on the content. Blocking internal data attacks and spam data flow. For Internet borders, UTM must provide complete online behavior management functions to manage Intranet access applications to the Internet. It can identify various types of known network application software, such as IM, VoIP, P2P, and FTP, and formulate different management policies based on various conditions, such as IP group and VLAN ID, to restrict Intranet users from using the following: Internet applications, such as IM software, P2P software, and online games, regulate online behaviors through technical means, prevent bandwidth abuse, and prevent Intranet leaks. Because IPS detects access in depth, IPS products need advanced hardware architecture, software architecture, and processing engine to fully ensure processing power.

5. Conclusion

Through the above system management platform construction, the system can form an overall hierarchical security system, and at the same time according to the security information system security management technology construction, to ensure the overall security of the system. Management level protection is a continuous cycle process, so through the implementation of the whole safety management project, the whole system can achieve continuous safety with the change of the environment. At present, this set of management system architecture runs stably on the platform, fully meets the design requirements of the information system security management of the real estate management center, and can achieve the level L7 management capability requirements from the physical layer to the application layer. In the future, it will provide a flat, simplified and innovative idea for the information system security management platform architecture research, and achieve a low investment, high value model. It has the significance of promotion and replication.

Acknowledgements

This study was supported by 2021 Outstanding Young Talents Support Program in Colleges and Universities (Item number: gxyq2021019); 2021 Humanities and Social Science Research Key project of Anhui Universities in China: Study on performance Evaluation System of Transformation of Scientific and technological Achievements in Anhui Free Trade Zone (Item number: SK2021A0608); Pilot project for basic teaching and research units in Anhui Province in China (Item Number: 2018jyssf039); Chaohu University Business Administration School level Key Construction Discipline (Item number: kj20zdjsxk01).

References

[1] Feng Ying, “Analysis of Computer Network Information Security of Public Institutions,” China Management Informatization, vol. 25, no. 10, 2022, pp. 189-191.

[2] Wang Wei, “Information Security Risk Assessment Based on Orderly Weighting and Entropy Weight,” Project Management Technology, vol. 20, no. 5, 2022, pp. 55-59.

[3] Zhao Qing, “Analysis of Enterprise Information Security Guarantee Strategy in the Age of Big Data,” China Management Informatization, vol. 25, no. 7, 2022, pp. 110-112.

[4] Ren Jiawei, “Analysis on Management and Protection of Traffic Comprehensive Information Platform under the Standard of Equal Protection 2.0,” Management and Technology of Small and Medium Enterprises (First Ten Days), no. 8, 2021, pp. 171-172.

[5] Liu Yilin, “Discussion on Computer Network Information Security and Protection Countermeasures,” Metallurgical Management, no. 23, 2021, pp. 187-188.

[6] Du Kexun, “Technical Analysis on Improving the Security of Enterprise Computer Network Information,” China Management Informatization, vol. 24, no. 22, 2021, pp. 86-87.

[7] Li Jie, “Enterprise Social Insurance Management Information System Management and Protection,” China Management Informatization, vol. 24, no. 16, 2021, pp. 129-131.

[8] Zhang Li, Peng Jianfen, Du Yuge, et al, "Overview of comprehensive assessment methods for information security risk assessment," Journal of Tsinghua University (Natural Science Edition), vol. 52, no. 10, 2012, pp. 1364-1369.

[9] Tong Ying, Yao Huanzhang, Liang Jian, "Research on threats to computer network information security and data encryption technology," Network Security Technology and Application, no. 4, 2021, pp. 20-21.

[10] Wang Jingjing, "Research on Computer Network Information Security in the Age of Big Data," Electronic test, no. 4, 2021, pp. 123-124.

[11] Gu Feng, Yan Bing, Zhang Yuan, "Analysis of the importance of computer information management in the network security of government agencies and institutions," Journal of Chifeng University, vol. 35, no. 6, 2019, pp. 74-75.

[12] Zhang Jiangang, "Effective ways to improve network information security management," Decision making exploration (middle), no. 4, 2020, pp. 4-5.

[13] Hu Baiyao, "Exploring the way of information security management in the context of smart city construction," Intelligent buildings and smart cities, no. 5, 2022, pp. 106-108.

[14] Jin Ting, "Design and Implementation of Real Estate Unit Management System -- Taking Beijing Real Estate Registration as an Example," Surveying and Mapping and Spatial Geographic Information, vol. 44, no. 9, 2021, pp. 128-131.

[15] Shen Jian, "Research and design of real estate registration information security architecture covering the whole life cycle," Land and Resources Informatization, no. 4, 2019, pp. 44-48.