Design Thought and Planning Method of Information Security System

Lei Ao, Cheng Zhang, Yuchen Wei

City Institute, Dalian University of Technology, Dalian, China

E-mail: 154001958@qq.com

Keywords: Network system platform, Information Security, Information Security Guarantee System

Abstract: Through the analysis of the current situation of the communication platform system and the overall design idea of the security system, the information security technology system and the security management system will be established to ensure that the communication platform network is controllable, safe and unimpeded, and that the business systems on the network are safe, accurate and correct. In the communication platform information system, effective security protection ability, hidden danger discovery ability, emergency response ability and system recovery ability are formed, which can provide a safe network operation environment and application security support for the operation of the communication platform information system, and ensure the safe and reliable connection, data exchange and information sharing of the communication platform information system, so as to realize the security of business and security of use. The aim of promoting business is to lay a foundation for the further development of information security construction of communication platform.

1. Principles of Safety System Design

According to the security requirements for preventing security incidents, the security objectives to be achieved and the security services required for corresponding security mechanisms, and according to the hierarchical protection standards and referring to international standards such as SSE-CMM and ISO17799, the security system of the communication platform comprehensively considers the implementability, manageability, extensibility, comprehensive completeness and system balance of information security. The following four principles will be followed in the overall design process:

Firstly, the principle of hierarchical protection refers to the appropriate protection of different protected areas according to actual needs. Communication platform system should be classified into different levels according to national hierarchical protection standards and actual business, including classifying the degree of information confidentiality, user operation authority, network security level (security subnet and security area), and hierarchizing the system structure (application layer, network layer, link layer, etc.), so as to provide different levels of security objects. Comprehensive and optional security algorithm and security system to meet the actual needs of different levels of the network.

Secondly, the principle of active defense refers to adequate protection before security incidents occur. This can not be accomplished only by a single tool-based product or technology, but requires a more comprehensive protection system for in-depth defense, which contains a series of active safety protection technology, safety management strategy and safety management system. For the communication platform system, it is necessary to integrate security technology, strategy, people and services, establish or restructure a set of security management processes to meet the security needs of the communication platform system[1].

Thirdly, the security system is an organic whole, and each component needs effective linkage to play its greatest role. We can build a solution by choosing excellent products and services, but if each product, service and other links are isolated from each other, the security strategies of each product and service link are relatively isolated, and the overall security strategy can not be formed. This will inevitably form security loopholes and give intruders a chance. Network security is

dynamic. If every excellent product, service and other links are isolated, it is impossible to fully understand the overall security situation of the network, of course, it is impossible to dynamically adjust the security strategy according to the network and application situation. Therefore, the communication platform system needs a unified and dynamic security strategy, but also needs to consider the overall security solution from the perspective of linkage and efficiency.

Finally, in order to effectively guarantee the safe and stable operation of the communication platform system, it is necessary to establish a network-wide security monitoring system to comprehensively manage the security products and host servers deployed throughout the network. By aggregating, filtering, collecting and correlating a large number of single security events in different locations and different security systems, we can get security risk events from a global perspective, and form a unified security decision to respond to and deal with security events. Through comprehensive management, it can provide assistant decision-making at the macro level, system construction at the meso level and monitoring and management of system equipment at the micro level[2]. The project will involve a large number of business systems, network devices, security devices and operating system hosts. The management and maintenance of many of the above-mentioned equipment will be enormous, so comprehensive management must be considered from the beginning of construction, and the authorization, certification, authentication, auditing, logging and performance monitoring of all equipment and applications should be considered in a unified way.

2. Security Architecture Model of Communication Platform

According to the framework requirements of the above-mentioned communication platform system security integrated defense system, the following information security system model is adopted to design the system[3].

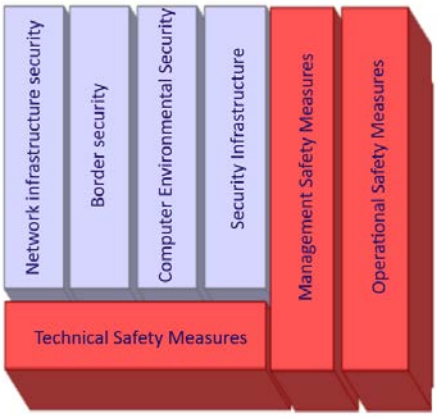

Fig. 1 Information Security Guarantee System Model of Communication Platform

The information security guarantee system of communication platform is a three-dimensional defense system in depth. The system consists of technical safety measures, management safety and operation safety measures. Technical security measures are composed of four aspects: network infrastructure security, computing environment security, border security and security infrastructure system (so-called "three security support": network infrastructure security, computing environment security, border security and supporting security infrastructure).

The security mechanism of communication platform system security guarantee system will be implemented in the design and implementation of network infrastructure security, boundary security, computing environment security and security infrastructure, according to different protocol levels and system units.

The emphasis of information security implementation of business system of communication platform system is to configure security equipment and technology according to computing environment security and boundary security, while network infrastructure security and security infrastructure provide unified security infrastructure support for different businesses.

In the aspect of management and operation security, we mainly form a long-term security control mechanism based on the requirements of information system services, from the point of view of management and operation, and combined with the technical framework.

In the security of network infrastructure, we will adopt three measures: reasonable design of network architecture, security guarantee of wide area transmission and security guarantee of local transmission to realize security services such as data confidentiality, data integrity, availability and reliability under the transmission layer of communication platform system, and to realize unified security management under the transmission layer.

In the aspect of border security, security domain partition, border access control, border intrusion detection and other measures are adopted comprehensively to realize information security services such as border access control, domain separation, illegal intrusion behavior monitoring and so on in the communication platform system. In the aspect of computing environment security, anti-virus, host intrusion detection, security configuration and reinforcement, patch management, security audit, vulnerability scanning evaluation and other measures are adopted to realize the security of computing environment system in communication platform system.

In the security infrastructure, independent safety management network design, integrated virus prevention and control, security assessment and patch management system, safety management center and other measures are adopted to achieve data integrity protection, anti-denial of denial, availability and reliability of security services in the communication platform system[4].

3. Planning for Technical Safety

3.1. Network Infrastructure Security

Core layer, convergence layer equipment and important access layer equipment should be dual hot standby. Redundant fault-tolerant structure is adopted in the interconnection of core layer network devices; redundant fault-tolerant structure should be adopted in the interconnection of convergence layer network devices; and redundant fault-tolerant structure should be adopted in the interconnection of core layer, convergence layer and access layer. In view of the link security of WAN, the network communication mode of backup of lines of different telecommunication operators should be adopted.

The key application servers use two special switches backed up each other as access switches of the server cluster.

3.2. Boundary Definition (Secure Domain Division)

Access control is one of the main strategies of communication platform system security prevention and protection. Its main task is to ensure that the resources of communication platform subsystems are not illegally used. It is an important means to maintain the security of communication platform system and protect network resources. It is a security protection measure for illegal operation of network.

The precondition of secure access control is to establish security domain reasonably and establish different security domain according to different security requirements. The establishment of security domain can be divided into physical and logical security domains. Physically, the information system is separated from the region and divided into different physical regions. Logically grouping information systems or users to specify different access rights.

The definition of the boundary of security domain is very important for the safe operation of the communication platform system at present and in the future, and it is also the basic measure to establish the security guarantee system such as the communication platform system. Only by reasonably dividing the security domain, can we effectively adopt technical means to ensure the security of the communication platform system.

Through a thorough understanding of the communication platform system, it is found that the whole network has not implemented security domain division and clear area division. The following security domain partitions are planned:

Set up a server area where important server assets are located;

Set up terminal access area, terminal access area;

Set up Establishment of safety management area and deployment area of safety operation and maintenance management system;

Set up the deployment area of interconnection domain, switching, routing and gateway equipment.

3.3. Computational Environmental Safety

Firewall control focuses on the pre-control of security incidents, intrusion detection focuses on the monitoring of security incidents, and system security audit focuses on the post-analysis and recording of security incidents.

In each network system of communication platform, the establishment of system security audit mechanism is an important part of the system security guarantee system of communication platform.

Through the system security audit mechanism, we can make a complete record of the operation of each system of the communication platform in order to effectively track down the responsibility and analyze the reasons for the violation of network security rules, and provide necessary technical evidence for punishing malicious attacks when necessary. If combined with the alarm function, it can stop and remedy in time after the occurrence of the violation of network security rules, or when the important operation threatening network security is in progress, so as to avoid the loss expansion.

There are two levels of audit for each system of communication platform: network level and database level. The audit function at the network level is to analyze and restore the data flowing through the network in real time, to record the various violations in the monitored network, and to determine the cause of the accident and the basis for the event person after the occurrence of a security accident.

The audit system at the database level can monitor the direct operation of the database in the network, record important and irregular data operations, provide monitoring means for data security, and provide evidence for irregular operations. It can audit and record the operations of adding, deleting, modifying and querying the database using standard SQL language. It will not affect users'normal access to the database, users do not even know the existence of the system, but once it finds that suspicious users are violating the rules of sensitive data, it will take immediate measures, or record, or alarm, if necessary, directly cut off the connection between users and the database. Through system security audit measures, the network and important servers of communication platform system can be protected, and the event process can be restored immediately after security incidents are found, which provides reference for the definition and tracing of event sources.

Through in-depth understanding, the current communication platform system still lacks the mechanism of security audit. It is suggested that the network-based and database-based security audit system be implemented in the near future to meet the security audit requirements of the communication platform system.

3.4. Security Infrastructure

Security infrastructure includes security operation center and security service system.

The security operation center mainly realizes the following functions: it realizes the management of the state of security equipment, including the good state, configuration information, flow of security equipment, etc. Further implementation of security incident management, centralized processing of important alarm events including firewall, intrusion detection, anti-virus, security audit, important server operating system, log alarm of important network switching equipment, and important computer room physical environment;

Implement a knowledge base of security incidents to support patch management and emergency response. According to the actual situation, the safety operation center can be used as a part of the later security construction. Through the evaluation, we can see that the communication platform has a variety of information assets, and with the development of future business applications, the types

and quantities of operating systems, network devices and application systems in the network will be more and more.

In this case, it is unrealistic to require network administrators to manage and apply all information systems from a security point of view. At present, owing to the limitation of personnel themselves, it is impossible for staff to do some basic maintenance work, requiring them to deal with various security problems of information assets. Therefore, it is necessary to establish a special information security service team and a complete information security service system to ensure the normal and efficient operation of the network information system of the communication platform[5].

The security service system of communication platform should include: security risk assessment, security system reinforcement, security emergency response, engineer presence and so on.

Information security service teams can come from internal, specialized security service providers or an organic combination of both. Therefore, it is suggested that the communication platform can periodically carry out information security risk assessment or self-assessment according to the actual situation.

4. Conclusions

Through the analysis of the current situation of the communication platform system and the overall design idea of the security system, the information security technology system and the security management system will be established to ensure that the communication platform network is controllable, safe and unimpeded, and that the business systems on the network are safe, accurate and correct. In the communication platform information system, effective security protection ability, hidden danger discovery ability, emergency response ability and system recovery ability are formed, which can provide a safe network operation environment and application security support for the operation of the communication platform information system, and ensure the safe and reliable connection, data exchange and information sharing of the communication platform information system, so as to realize the security of business and security of use. The aim of promoting business is to lay a foundation for the further development of information security construction of communication platform.

References

[1] Jiang Jianchun et al. Overview of network security intrusion detection research [J]. Journal of Software, 2018.02

[2] He Jianhong, Bai Xiaoying, Li Runling, Cui Zhishe. Service-oriented infrastructure based on SLA [J]. Telecommunication Technology, 2011, 51 (9)

[3] Xiao Renovation, Ma Jiaqi. Design and Practice of Data Center Storage System. [J]. Information Network Security, 2012, 17 (02)

[4] EricMaiwald, Wi1liEducation, Security Planning&Disaster Recovery, 2003, Posts& Telecommunications Press, PP.86-94

[5] Yang Guang, Li Feifei and Yang Yang. Brief analysis of computer network security precautions [J]. Science and technology information, 2011 (19)