The Design of Enterprise Network Information Sharing Scheme Based on Security Technology

Jun Ji[1, a *], Fei-Fei Xing[2, b], Yu-Qing Zang[1, c]

[1]Beijing Polytechnic, Beijing 100176, China

[2] BMEI CO., LTD., Beijing 100027, China

[a]ji_jun2000@sina.com,[b]xingfeifei@126.com,[c]sunny_zyq@sina.com

Keywords: Information sharing; Information security; Firewall

Abstract. According to the characteristics of enterprise network system, the paper designs the network information protection system of security technology and divides network system. All kinds of safety equipments are applied to system, which forms full protection system architecture.

Introduction

With the rapid development of information construction in our country, information security is gradually becoming a hot problem, in which the importance of network information security is especially; the ultimate goal of security management is security transmission in network and the authenticity of stored data in the system by user [1]. Meanwhile, in the process of information, information security is the most fundamental guarantee of the information effectiveness. In the content of information construction, information security protection system and the construction of emergency response measures should be paid attention from two aspects of technology and management. The management level should strengthen the system construction and understanding for information security of staffs. The technology levels should provide multi-level and multi-angle information protection measure. What's more, when the dangerous of information security breaks out, the effective measures should be taken to minimize the damage [2-3].

The security threat of network information sharing and the target of security system

The division of network information sharing system is complexity, which involves secret network, enterprise intranet, enterprise extra-net and internet. There are many network equipments, including server and terminal. Because of the variety of business system data and service staff, overall network is attacked easily and produces information leak. The analysis of security threat is as following [4-7].

1) Divulge the secret

Stealing confidential information is the important security threat for internet. In the process of producing, storage, disposal, exchange file information, the goal of invader is finding chance to obtain confidential information.

2) Counterfeit

Counterfeit is creating false data to deceive someone or software system. The aims of counterfeit are counterfeit authentication of user, counterfeit application system to obtain the user account and authentication information.

3) Abuse

Abusing of working station and terminal equipment is one of important reason for information leak. Working station or mobile computer with external linking the internet illegal causes sensitive information leak of network or terminal.

4) Tamper

Tamper is one of important security threat in the network. Illegal user achieves advanced access permissions by the tamper to steal confidential information, deceives information receiver.

5) Denial

Denial refers to user denial behavior and operation in the system.

6) Unauthorized

Unauthorized access refers to access to the system data information without being authorized. Unauthorized access includes system the leak of effective authorization and access control measures; tamper permission data to obtain advanced permission, illegal access to information resources; avoiding access to control components, access to business data from the background.

The target of information sharing system network is providing overall security for data authenticity, confidentiality, integrity, availability, non-repudiation. Details are as follows. when business data needs to eternal service, therefore, system can provide protection for the information authenticity, determine the source of business data, identify counterfeit information, provide the integrity of business, ensure the consistency of the data, prevent data being tampered by illegal user, provide the availability guarantee for network, ensure information system to be refused by wrong uses of legal users. The availability guarantee should include redundancy, backup, restore and response.

The four network systems of network information security sharing

Enterprise network provides resources sharing service for different access object. Access objects include enterprise departments at all levels, enterprise eternal network and internet users. According to different kinds of data information security level for each network, enterprise application intranet is often defined as classified information network, and the other two networks are named as non-classified information network. Therefore, the enterprise network is divided into four different networks, classified private network, enterprise network and the internet areas respectively. Network topology diagram is shown in Fig.1.

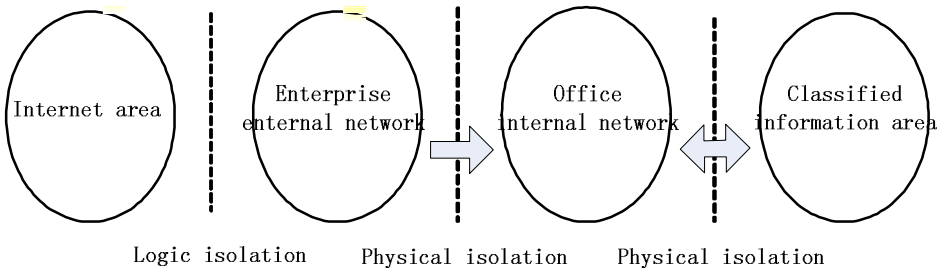

Fig.1. Network topology information sharing platform

The layout of security technology product

In office intranet network, the types and quantity of equipment and software are as shown in the Fig.2.

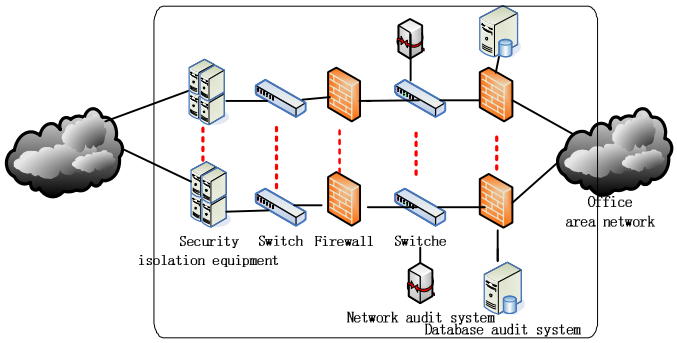

Fig.2. The equipment and software of enterprise intranet and of enterprise eternal network

Office intranet area security product deployment list is as shown in Table 1.

Table1 Security product deployment list

ID	Device type and designation	Deployment and location	Defensive level
1	Firewall	Network access area outside	The outer defense
2	Network audit system	Network access area outside	The outer defense
3	Security isolation and information exchange system	Network access area outside	The outer defense
4	Database audit system	Office intranet area network	The inner control

Product deployment of internet area is as shown in Fig.3.

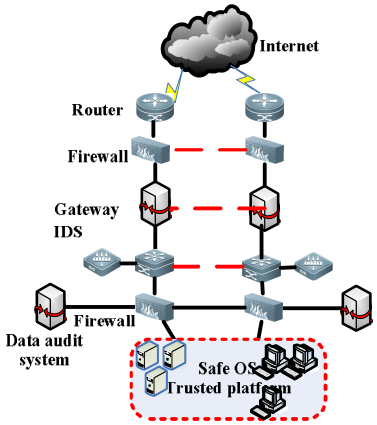

Fig.3. Product deployment of internet area

Product deployment of internet area lists in Table 2.

Table2 Product deployment of internet area list

ID	Device type and designation	Deployment area and location	Defensive system
1	Firewall	Network access area outside, server area, terminal maintenance, safety management area	The outer defense
2	Gateway	Network access area outside	The outer defense
3	Flow control equipment	Network access area outside	The outer defense
4	Intrusion detection system	Network access area outside	The outer defense
5	Database audit system	Server area	The inner control
6	Security operation system	Server area, terminal maintenance	The core to control
7	Trusted platform	Server area, terminal maintenance	The core to control

Conclusions

According to the characteristics of enterprise network, the paper designs a protection system for network information sharing. The research can be applied to specific enterprise network system to realize security management of enterprise intranet information, and promote the healthy development of the construction of information sharing system.

References

1 Kaufman C, Perlman R, Speciner. Network Security–Private Communication in a Public World. Peentice Hall(2005).

2 Alec Yasitaner,Tanet Manzano,Policies to Enhance Computer and Network Forensics.Proceedings of the IEEE(2001).

3 S Foresti, J Agutter, Y Livnat. Visual correlation of network alerts. Computer Graphics and Applications, 26(2): 48-59(2006).

4 C.A.Costa,J.&Harding,R,I.Young.The application of UML and an open distributed process framework to information system design.Computers in Industry 46(2008).

5 Lists.In:Proceedings of the 46m IEEE International Midwest Symposium on Circuits and Systems, Dec, 512-515(2003).

6 A Hassan.Algorithms for Verifying Firewall and Router Access Lists[C].In:Proceedings of the 46m IEEE International Midwest Symposium on Circuits and Systems, 512-515(2003).

7 Andrew H.Gross.Analyzing Computer Intrusions. PhD Thesis.University of California.San Diego,San Diego,CA(1997).