Research on Network Information Security Analysis and Prevention Strategies of Campus Network in Xinjiang Uygur Medical College

Alimujiang·Paiziaihemaiti [1, a] Ablimit arxiden[2*, b]

[1]College of Xinjiang Uygur Medical, Hotan, Xinjiang, China, 848000
[2]School of Mathematics and Information, Teachers Collage of Hotan, XinJiang 848000, P.R. China

[a]email

Keywords: Network Information Security, Prevention Strategies, Campus Network, Xinjiang Uygur Medical College

Abstract. With the improving of information technology of Xinjiang Uygur Medical, there are more and more applications and network node, the structure has become increasingly large and the network systems has become increasingly complex. Generated in the course of business operations in a large number of data requiring protection, the development of the organization's dependence on information is also growing and important part of information security management has become the Xinjiang Uygur Medical information development and construction. How to build an effective information security defense system and give an effective protection of the Xinjiang Uygur Medical College information assets is an important issue in Xinjiang Uygur Medical College.

Introduction

With the rapid development of Internet technology, led to the rapid development of the campus network. Our university campus network has entered a rapid development stage. But under the influence of subjective or objective factors, the campus network occurred during the construction of some deviation, some schools focus only on the size of the campus network is strong enough to possess the function is comprehensive, the system can support some common run in this case, ignore the campus network of the most important aspect, and that is building the information security system. Many campus network will also put information security apparatus, but only focus on the hardware parameters of competition, without considering the comprehensive information security management and information systems, security problems caused by information systems have become increasingly prominent, a single defense structure to the information security of campus network It posed a serious challenge.

The Formation and Status of Campus Network in Xinjiang Uygur Medical College

Today's society, economy and science and technology high-speed, under this social context, building on each campus network has also put forward higher requirements, size and construction of a school campus network directly affects the level of information a school, this also represents the strength of modern teaching school, so the construction of the campus network has become an indispensable part of a school.

Xinjiang Uygur Medical College campus network also experienced a scratch, from small to large development process. Now the school's campus network is a collection of school news release, sharing of teaching resources, teacher-student interaction platform, the students asked questions, release of employment information such as the role as one of a network resource platform, and the platform for teachers teaching and students learning provided convenient conditions, with the updated school development and network technology, called for the construction of the school network corresponding reforms to ensure the campus network security, availability, timeliness and other aspects can be further improved, so that the campus web become a powerful assistant school construction and development.

Currently, the school has been completed on the campus network hardware engineering construction, the school administration building, teaching building, laboratory building and student

apartments Internet connectivity, and also supports educational management system, on-line enrollment and employment system, information distribution system operation.

At this stage, for use in schools is P2DR such a two-tier model of information security defense system, in order to maintain the development of the system, the daily management of the system and the development of the implementation of measures, including security policy, program management, risk management, security, system lifecycle management, are lagging behind, that is incomplete, imperfect. In addition, the lack of schools in the system operation and use of the process were a complete development, use, maintenance mechanisms, and lack of training in the use of personnel, in terms of staff responsibilities is not very clear, there is still a school identification and authentication way single, logical access control is not tight, there is no complete audit log storage, encryption strength is not enough.

The Firewall Technology of Network Information Security

Network information security is a matter of national security and sovereignty, social stability, national cultural inheritance and development of important issues. From a technical perspective, the network information security is a matter of marginal multidisciplinary computer science, network technology, communication technology, cryptography, information security technology, applied mathematics, number theory, information theory, and other disciplines.

Most firewall using several technologies combined form to protect the network from attacks, the basic technology is usually divided into network packet filtering and network service agents.

Packet Filter. Packet filtering technology at the network layer packet analysis, select. Based on selected filtering logic within the system is set up by checking the data stream for each packet source address, destination address, the port number, protocol status with other factors, or a combination thereof to determine whether to allow the data.

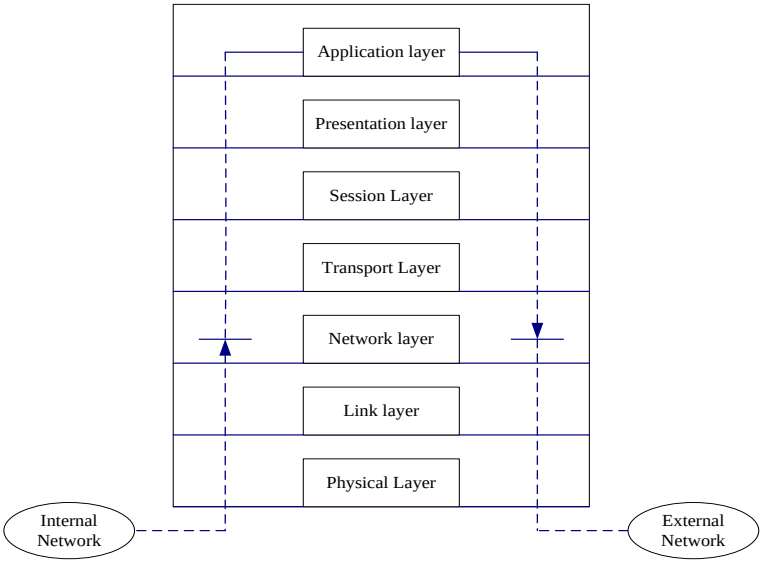

Fig.1 The implementation mechanism of data filtering firewall

Users can set a series of rules that specify allowed to flow into or out of the internal network packet types, as well as the transmission of packet types need to intercept. IP packet filtering rules based on packet information, the source IP address, destination address, and encapsulation protocol, and port number for screening. These operations can be performed on the router can also be carried out on the bridge and a separate host. Packet filtering for TCP or UDP applications rejected in IP network access layer is very effective.

Application Layer Gateway. Application Layer Gateway technology is protocol filtering and forwarding on the network application layer. It uses for specific network applications services agreement specified data filter logic and filtering packets while the necessary analysis, records and statistics, generate reports.

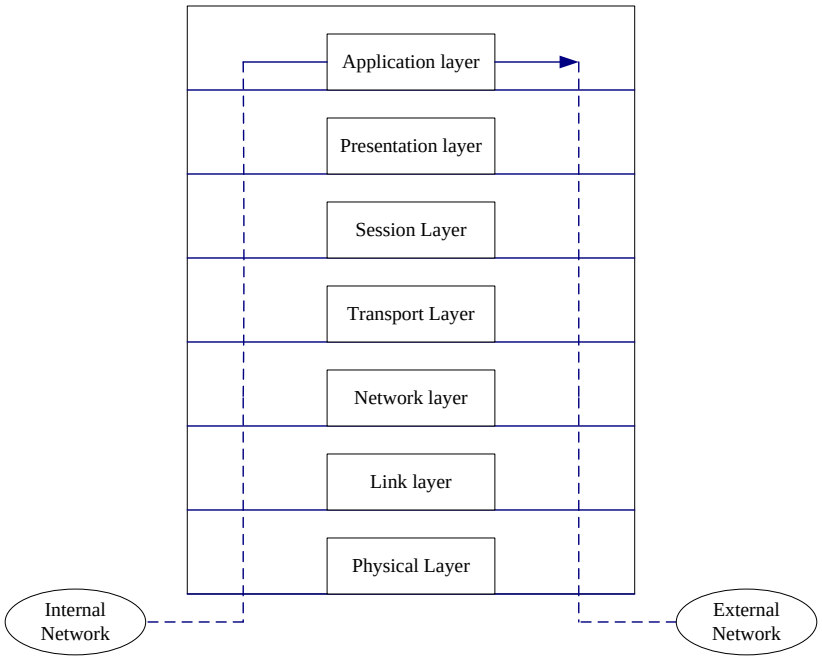

Fig.2 Implementation mechanism of application layer gateway firewall

Application layer gateway can work in any layer of the OSI model up check incoming and outgoing packets, copy and transfer data through the gateway, preventing direct contact between the establishment and the host.

Proxy Service. Agent services are handles on behalf of internal network users outside of the server. Client proxy server and proxy dialogue, verify the user requests it, and then sent to the real server, the proxy server to an internal network application services played a role in the middle of the external network adapter.

Internal network only receives a service request made by a proxy server, refused direct requests from other nodes on the external network. When the external network to apply a service node in the internal network, first proxy server receives, and according to their server type, service content, the service object and scope of the applicant's domain name, IP address and other factors to determine whether to accept the service . If accepted by the proxy server forwards the request to the internal network and the response back to the applicant; otherwise, reject the request.

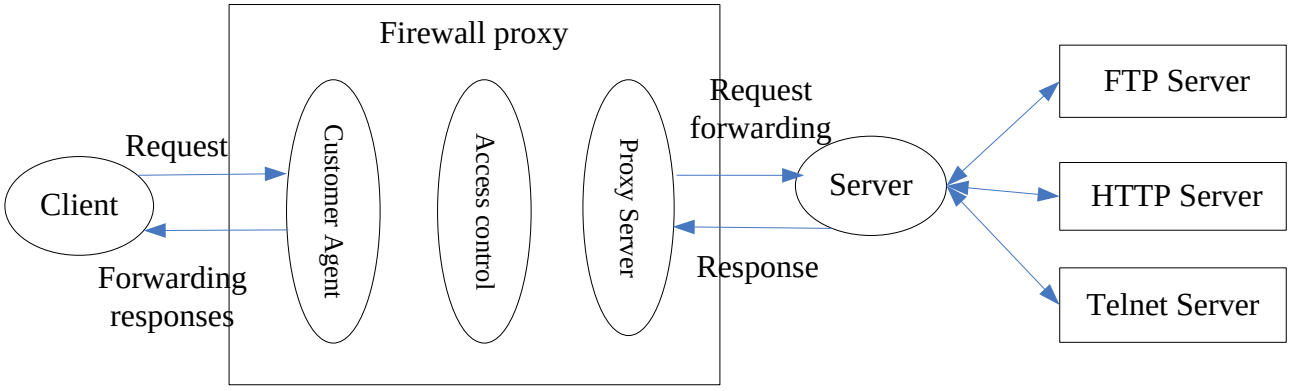

Fig.3 The proxy firewall application layer data control and transmission

The Security Risks of Campus Network

Risk from the External Network. Internal campus network environment is relatively simple, in the face of external threat is very fragile. In general, the safety valve will set up a network of campus outreach, but how to identify hacking is an important issue. In order to achieve campus network research and teaching functions in the interior is relatively open, inside the switch links have relatively large risk, various types of information within the campus network if the user is in

one way or another internal purposes, it is not impossible to steal thing. With the popularity of the Internet, more and more people to master the more advanced Internet technology, the Internet and campus activities precisely the most intensive areas, and related technologies popularity also makes public university students access to these technologies is very easy. Such user groups in the use of the Internet are inevitable that individual tempted curious people, using a variety of Internet technology for secure campus network trouble.

Moreover, the university campus as a teaching and research institutions has a lot of information resources, some resources have some commercial value, lawless elements in society are likely to steal those resources into the campus network sabotage, students and even disclose personal information, tampering with school educational administration data. Or carry out large-scale attacks make the carrying capacity of the campus network to the limit in order to paralyze the entire campus network. It will not only bring economic losses for the school, but also threatens to undermine the image of the school.

Risk from Hardware Facilities. Carrying the hardware to run the entire campus network, if a hardware problem, the campus network, it is fatal. Many schools of communication cable, power supply facilities and the absence of proper protection of servers and storage resulting in too large or small problem. Typically, hardware problems, the entire school will be caught without network state. In the face of extreme weather disasters, hardware facilities may also receive rain and snow, cold, lightning and other natural phenomena, malfunction or damage.

Limited Technical Level. Current network technology still has traffic information for transmission to greater restrictions, very high frequency of College Students' Internet activities, especially in the evening peak period. A lot of information exchange is likely to exceed the carrying capacity of the campus network. In addition, the computer's own system vulnerabilities and limitations are restricting the further upgrading of the campus network. Internet professional quality school maintenance staff also determines the campus network to deal with security issues in the face of the adequacy of .

Limited School Management Level. Some schools campus network security issues for lack of attention, lack of campus network security policy support. For some leaders do not have enough knowledge of technical issues, do not pay attention do not even know the meaning of the campus network security, resulting in deletion of the campus network management or security system implementation was not in place.

Implementation of Information Security Defense System Model

Basic domestic information security defense system is to establish a model using P2DR, P2DR model is based on the security model of the time, it is important to form the two levels: the first level is the core of security policy, the second level is protection and detection mechanism, protection and detection mechanism is by the protective equipment, means of detection, response measures constitute.

In this paper, a more perfect security system model, namely P-POT-PDRR three-tier model, which is the core of information security mechanism and P2DR together the basic form of the model. In addition to protection and detection mechanism P2DR outside, P-POT-PDRR model biggest feature is the integration of information security mechanisms among the "people, technology and operations," the three main elements, and it was added to the model of recovery mechanism, the information security management philosophy is reflected as highlights. Paper for the establishment of Xinjiang Uygur Medical information security defense system is used in the core of this information security management focus on P-POT-PDRR model, the model is part of the security policy, the expression is kind of how schools need information security, to how the protection of information resources, the level is the implementation of information security defense system guidance and programmatic document. Mid-level model reflects the configuration information security defense system to protect the mechanism, that is, by the initiative of people, technology, and running in the composition of the three operations, information security is explained basically who do, do what, how do the problems, the three basic elements are the

backbone of the entire security system. Simply, P-POT-PDRR three-layer model is under the unified command of the core security strategy, personnel, technology, operating the three complement each other closely, and as a support, protection, detection security defense system, in response, restore four links alternately, thereby forming a viable operating procedures for the completion of specific information security defense work.

The importance of the three levels in the order of the security policy, security mechanism, protective mechanisms.

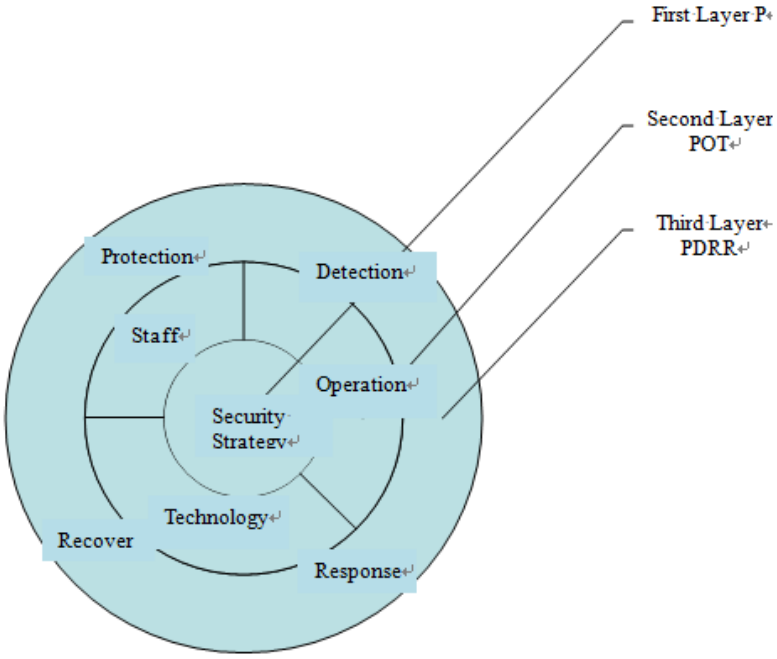

Fig.4 The P-POT-PDRR three-layer model

The Implementation of the Network Information Security Policy in Campus Network

Security Policy. Defense system security policy is the most important part of the content is the core of security defense system. Main function is capable of protection, detection, recovery, and normative behavior guidance documents. To carry out the implementation of all activities can be separated from the framework of security policy. P-POT-PDRR security policy security policy is different from other models, it is more focused on information security management should be as heavy, not a single security and defense rely on expensive equipment, perfect technology to achieve. Security policy formulated they fit directly affects the structure and operation of the effect of information security defense system. A good security policy should have availability, regulatory, safety, long-term sexual characteristics. Therefore, when considering the development of security policy must be comprehensive, detailed, and to meet the actual situation of the school in this process not only to consider the full information security defense system, available at the same time but also to achieve the goal of protecting the Xinjiang Uygur Medical information resources, in addition, laws and regulations, the use of funds, etc. should also be considered as a content focus. For schools, the security policy information system security defense system should contain the following:

The security policy should be consistent with legal and regulatory requirements. Information security and defense policy to be consistent with national laws, administrative regulations and local regulations and normative documents, the security policy established by the law cannot violate, nor violate the relevant laws and regulations, which is the most basic point. The security policy should within this basic framework to develop, although there may be conducive to any school of information security defenses, but violated state law, contrary to regulations, measures and technologies must not appear in the security policy, cannot be more protective mechanism It has been implemented.

Risk assessment is to make the school a comprehensive information security assessment. Only information security status with complete understanding, in order to make the right response measures to protect information resources. Risk assessment is in front of a security policy must do the most important work by the threat of the assets of the school may face its own weaknesses and other factors analysis and testing, we can draw the entire school of information security problems and inadequate for the construction of information security defense system, its basic work is risk assessment.

Security Mechanism. Use of personnel security mechanisms embodied technology, to complete the operation on the need to protect the information infrastructure for all-round protection of ideas, it is a kind of information security management as an important ideological mechanism that uphold content security policy, will after its information security management and the concept of integration, and then used to drive a protective mechanism to form a complete, effective information security defense system.

Information security technology at different stages of the development process of information security also exhibit different characteristics. Now more information security technology is embodied in information security, building a system, no longer rely on a single device, technology and measures to protect information resources. Information security mechanism is that with the rapid development of information security technology developed to manage the weight of the system. It is focused on people, technology, operating three mutual collaboration, use of technology by the staff to complete the operation of information security protection work, again the three human subjects, the effect of the security mechanisms and ultimately by the people to decide.

Conclusion:

With the rapid development and popularization of the Internet, the new network threats Xinjiang Uygur Medical College Campus Network attendant, data leaks and the risk of fraud. Medical education system you want to get a truly comprehensive platform support network, security is a top priority. And how to effectively prevent a growing number of security risks in the relevant technical level higher demands at the same time, how to build a better Xinjiang Uygur Medical their information security defense system has become the Xinjiang Uygur Medical yen gain attention It focuses.

References

[1] Jia Xinzhang, Li Jingyuan. Information Security Engineering, Vol. 6 (2012) No 53, p.25-26

[2] Wang Qunyong. Computer Operation and Applications, Vol. 12 (2010) No 27, p.74-76

[3] Jing Jianfen, Hou XuSiem. Computer Engineering, Vol. 30 (2011) No 19, p.144-145

[4] Wang Kuailiang. Computer Operation and Applications, Vol. 29 (2008) No 27, p.21-23

[5] Zhang Gongxu, Sun Jing. New Quality Management, Vol. 8 (2013) No 27, p.57-60

[6] LI Yang. Microcomputer Applications, Vol. 4 (2011) No 27, p. 51-56

[7] Wang Jun. Discussion on Science and Technology, Vol. 10 (2015) No 7, p.87-89

[8] Wang Yan. Computer Engineering and Applications, Vol. 9 (2010) No 27, p.122-125

[9] Hu Qiliang. Safety Technology, Vol. 12 (2013) No 17, p. 28-29

[10] Ding Ling. Discussion on Science and Technology, Vol. 4 (2010) No 24, p. 35-40

[11] Peng Miaoyu. Computer Engineering and Applications, Vol. 7 (2011) No 12, p. 81-89

[12] Tan Kunpeng. Information Security Engineering, Vol. 6 (2012) No 23, p.82-87

[13] Han Lei. Computer Operation and Applications, Vol. 12 (2010) No 27, p.74-76

[14] Hou Xuyang. Computer Science and Information Technology, Vol. 30 (2011) No 19, p.48-50

[15] Wang Mingming. Changchun Normal University, Vol. 29 (2008) No 27, p.26-28

新疆和田北京东路 98 号昌龙大夏第一单元 1803 室 18099053919 海日古丽