Advances in Educational Technology and Psychology (2021)
Clausius Scientific Press, Canada

DOI: 10.23977/aetp.2021.051011
ISSN 2371-9400 Vol. 5 Num. 10

On the Current Situation and Solutions of Campus Network Security in Colleges and Universities

Yi Shen[1], Haoming Yan[2]

1. Department of Computer Science, San Francisco State University, San Francisco, Ca 94132, USA

2. Aerospace engineering, University of Arizona, Tucson, AZ 85719, USA

Keywords: University campus network, Network security, Firewall, Intrusion detection

Abstract: with the university campus network playing a more and more important role in university teaching, scientific research and administrative office, how to rely on the existing network infrastructure, integrate and build the university network, support the operation of various business systems, support cross departmental and cross regional information resource sharing, and promote the improvement of University teaching ability and informatization level, It has become a priority for colleges and universities. Build a network security protection system, network trust system, security management system and a unified technical standard system in Colleges and universities to ensure the reliable operation and effective application of college business system.

1. Introduction

Taking the LAN security project of a secondary college of a university as an example, this paper discusses the security status of the campus network and some more effective solutions. Before the implementation of the security project scheme proposed by us, although the college has established an information network, it has not taken any security measures. In order to ensure the security of the network, the college has been looking for various appropriate security equipment to strengthen network security protection, hoping to strengthen the security of the existing network, so as to ensure the stability, reliability and security of various business systems and network infrastructure in information construction. The main problems existing in the college's network before the implementation are also common problems in many college campus LANs, including the following three aspects:

1.1 The Investment in Network Security Being Seriously Insufficient

There is no systematic network security facilities, network construction funds are seriously insufficient, and the limited funds are mainly invested in network equipment. There has been no systematic investment in network security construction. The network is still basically in an open state, lacking effective security early warning means and preventive measures.

1.2 Internal Internet Access is Chaotic without Any Means of Safety Management and Monitoring

The internal IP management is chaotic, which can not limit users' access to the Internet, and there is no means of security management and monitoring. The switch is unable to manage and respond to network events.

1.3 The Awareness of Network Securitybeing Weak

There is no perfect network security management system,attacks on the network, intrusion into other people's machines, misappropriation of other people's accounts, illegal use of the network, illegal acquisition of unauthorized documents, harassment and personal attacks by e-mail are common. Thus, in order to trace the source of the attack, the system should have effective tools to record the whole process of the attack, provide a basis for the investigation, and effectively deter illegal intruders. In addition, due to the limited manpower, some staff often have multiple duties, violating the principles of the security system and posing a serious threat to the security of the system[1]. Therefore, we should strengthen management and monitoring from various channels such as technology and management to eliminate security problems at this level.

2. Some Effective Network Security Solutions Often Being Used

Firstly, configuring firewall is not only the first step to ensure the security of campus network system, but also the primary consideration in system construction. Firewall can protect the network system from external attacks by monitoring, limiting and changing the data flow through the firewall. The author recommends the deployment of a network firewall system for the basic security protection measures of the border.

In terms of Firewall deployment, it is recommended to install the firewall at the boundary of the internal and external network, so as to avoid the exposure of the internal network to the external network, effectively isolate the internal and external networks, and shield the internal information, structure and operation status of the network. At the same time, by setting access control rules on the firewall, we can make conditional mutual visits between internal and external networks, filter out illegal access requests, greatly reduce the opportunity of external attacks on the internal server / host of the network, and solve the security problem of the network boundary.

Some common firewall products on the market can basically realize the following functions: (1) through source address filtering, reject external illegal IP addresses, and effectively avoid unauthorized access of hosts unrelated to business on the external network. (2) Firewall can restrict the network access behavior of internal users, such as restricting game websites and movies during working hours, restricting internal users from bad websites, etc. (3) Firewall can restrict the network access behavior of internal users, such as restricting game websites and movies during working hours, restricting internal users from bad websites, etc. (4) The firewall can formulate access policies to restrict specific internal hosts from accessing the external network. At the same time, only authorized external hosts can access only the limited IP address of the internal network, so as to ensure that the external network can only access the necessary resources in the internal network, and the operations irrelevant to the business will be rejected. (5) After the firewall is installed, the network security policy is centrally managed by the firewall. Therefore, hackers cannot control the access rights of other resources by changing the security

policy of a host, and it is almost impossible to attack the firewall directly[2]. (6) The firewall identity authentication module is used to authenticate the identity of each user accessing the Internet to ensure that each user using the Internet can correspond to specific personnel, effectively solve the network access audit problems caused by IP / Mac embezzlement and sharing computers by multiple people, realize the “real name system” of network access, and avoid the loss of productivity caused by anonymous network access, Legal consequences. (7) Through various functional modules of firewall, effective access control mechanism is realized. Such as P2P software restriction, traffic bandwidth control, concurrency control, etc.

It is necessary to focus on the use of firewall identity authentication module. Take the black Shield firewall used by the college in the above project as an example. The firewall identity authentication module consists of firewall identity authentication server and intranet user client, and works together with Heidun log system: (see Figure 2 for specific deployment)

(1) Firewall identity authentication server is responsible for uniformly configuring user database and user authorization access rules; Collect and analyze data; And send the data to the log system; (2) The intranet user client is responsible for sending the authentication request to the server, and the authentication communication is completed through the encrypted channel[3]; (3) The log system is responsible for storing, sorting and analyzing data.

Secondly, in addition to the firewall, the deployment of network intrusion detection is also very important for the security of campus LAN. In the above project, the college's network outlet connected to the Internet can effectively prevent harmful information from entering from the Internet by using black Shield firewall as the security protection equipment at the network boundary. However, if only the firewall is used as security protection in the network, it is not enough[4]. The main weaknesses are as follows: (1) the firewall is powerless to launch attacks against the Internet from the Intranet; (2) Launch attacks against the intranet from the intranet, and the firewall is powerless; (3) The firewall can't do anything about the attack of using legal ways to enter the network. Based on the above network security status and requirements, the following scheme is proposed.

In view of the existing network situation of the college, we suggest connecting the detection engine of the network intrusion detection system on the core switch and configuring the port image on the switch to monitor the network traffic of a specific port and whether there are attacks in the network. At the same time, the monitoring console of the network intrusion detection system is installed to monitor the working condition and setting strategy of the detection engine. When the detection engine of network intrusion detection system detects the occurrence of network attack or the spread of network virus, it can implement various response actions such as alarm, blocking, firewall linkage blocking and recording to protect the security of server and network[5]. At the same time, as an audit tool, network intrusion detection system can record all network access in detail for review.

3. Conclusion

Adhering to the policy of active defense and comprehensive prevention and comprehensively improving the ability of information security protection is one of the overall requirements of the national information security guarantee work. “Active defense and comprehensive prevention” should also be taken as the overall strategic policy for information security of university campus network. However, the policy of “active defense and comprehensive prevention” does not mean unlimited strengthening of security measures. According to the importance of information system, we should focus on the guarantee of important information system, and adopt appropriate security measures

according to the actual security threats faced by the system, so as to improve the overall efficiency of campus network information security and ensure the implementation of the policy of active defense and comprehensive prevention.

References

[1] Research on Computer Network Security and Firewall Technology Based on Large Data Analysis[A]. Yongtao Xuan.Proceedings of 2019 International Conference on Information Science,Medical and Health Informatics(ISMHI 2019)[C]. 2019

[2] Research on Application of Firewall Technology in Computer Network Security Based on Data Mining[A]. Chenglong Du.Proceedings of 2019 International Conference on Information Science,Medical and Health Informatics(ISMHI 2019)[C]. 2019

[3] Design and Implementation of Intrusion Detection System Based on Data Mining Technology[A]. Li Xin.Proceedings of 2019 International Conference on Information Science,Medical and Health Informatics(ISMHI 2019)[C]. 2019

[4] Research on Computer Network Information,Network Security and Protection Strategies Based on Big Data Mining[A]. Qiang Mei.Proceedings of 2019 International Conference on Information Science,Medical and Health Informatics(ISMHI 2019)[C]. 2019

[5] On Application of Computer Network Security Technology in Network Security Maintenance[A]. Li Xiuping.Proceedings of 2019 International Conference on Information Science,Medical and Health Informatics(ISMHI 2019)[C]. 2019