Research on Security Construction of University Email System Based on Information Security Classified Protection

Qi Xu
Network Information Center, Shaanxi Normal University, Xi'an, Shaanxi 710062, China
xuqi@snnu.edu.cn

Abstract. Information security classified protection is the basic system of national information security protection work and the basic requirement for information system security protection. The construction of the email system of colleges and universities should meet the security requirements of the 2nd-Level information security classified protection. This paper sorts out and studies the existing email system from physical security, network security, host security, application security and data security by comparing the requirements of the 2nd-Level information security classified protection, and builds a perfect university email security system to ensure the security and reliability of the university's email system.

Keywords: Information Security Classified Protection, Email System, Security Construction.

1. Introduction

With the deepening of network technology, information security has become an increasingly important issue in the process of informationization. As the main tool for university information exchange, email carries important information data of colleges and universities, and its security is highly valued. Compared with other business systems, the email system has the characteristics of large span, multiple layers and high professionalism. At the same time, email security issues involve a broader and more stereoscopic technology, from protocols and specifications to access and integration modes, from storage methods to the Web. Service application, its security construction involves email security, account security, access security, transmission security, data security, storage security, system security.

Therefore, it is an effective way to build a security and reliable university email system by studying the requirement of 2nd-level information security classified protection, and continuously improve our current system from following aspects: physical security, network security, host security, application security and data security.

2. Security Threats Faced by University Email Systems

The security construction of the university email system should meet the information system security requirements of 2nd-Level or above under the guidance of the national classified protection document and the standard overall framework system, and fully consider the two major systems of technology and management in light of the actual situation of the university email system. In order to create a reliable and secure email system, we can integrate and plan together. The specific framework is shown in Figure 1.

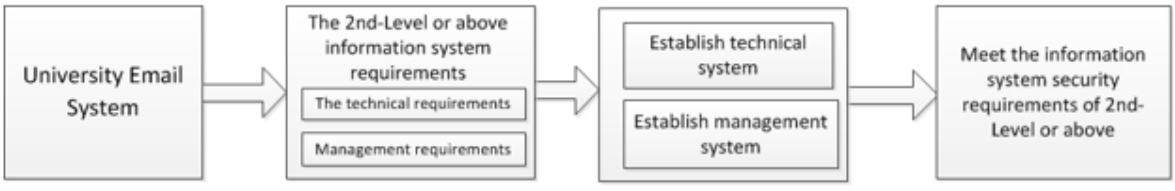

Fig 1.Construction Framework of Security Classified Protection of University Email System

With the popularity of the Internet, email has gradually occupied the status of mainstream Internet applications as a means of modern communication. Because of the convenience, quickness and economy of Email, teachers and students in colleges and universities are increasingly dependent on it. At present, most colleges and universities have their own email systems, but colleges and universities also face many security threats in the management and use of email systems. For example, the malicious attack of Email, in order to obtain a large number of Email addresses, the directory scanning attack on the Email system; Phishing emails and virus emails are emerging one after another, and spam messages carry Trojan viruses. Once they enter users' computers, they can steal various data of users, including online bank passwords, and delete various files of users, which seriously affect users' data security. Or, through phishing emails, the user can be induced to click the outer chain to obtain the user's data. In addition, the proportion of spam is increasing, occupying a large amount of network bandwidth, server resources and user storage space, system administrators need to spend a lot of time processing spam, increasing maintenance costs and so on. Therefore, how to deal with these problems and ensure the security of the university's email system has become an important issue in the construction of information technology in colleges and universities.

3. Security Construction of University Email System Based on Classified Protection

According to the basic requirements of GB/T22239-2008 information security technology information system security classified protection, from the aspects of physical security, network security, host security, data security and backup and recovery, the overall security of the university email system is carefully combed and strictly in accordance with the email. The operation and management specifications of the system can be used to ensure the security and stability of the university's email system. The following will start from these aspects to explain the security construction of the university's email system.

3.1 Physical Security of University Email System

In response to national requirements for the 2nd-Level information security classified protection, physical security mainly includes physical location selection, access control, anti-theft and anti-destruction, lightning protection, fire prevention, waterproof, moisture-proof, anti-static, temperature and humidity control, and power supply.

The physical security aspect of the email system is mainly the physical security of the computer network room, namely the wind prevention, waterproof and lightning protection measures of the computer room building. The specific measures are as follows:

The computer network room is equipped with a dedicated person and an electronic access control system to identify and control the visiting personnel. The computer network room is equipped with an anti-theft alarm system and a video monitoring system to monitor the personnel entering and leaving the room;

The computer network room is equipped with an automatic fire extinguishing system, a precision air conditioner for temperature and humidity control, a leak detection rope, etc.;

The cabinets and equipment in the computer network room are fixedly installed, and the labels in the uniform format are affixed. The cables and communication cables are laid in isolation, and the anti-static grounding measures are adopted. The anti-static floor is used to prevent static electricity;

The computer network room is configured as a UPS power supply. In addition, it is better to have a generator set to provide continuous power supply after the mains supply is interrupted.

3.2 Network Security of University Email System

For the national requirements for the 2nd-Level information security classified protection, network security mainly includes structural security, access control, security audit, border integrity check, intrusion prevention and network equipment protection.

At present, college campus networks use a number of Internet links to export, such as China Telecom, Education, China Unicom, etc. In order to ensure the security of the email system, the following security measures are taken at the network level for security protection:

Network security protection through firewalls and WEB firewalls, and only port policies such as IMAP, POP3, and STMP required for email services are enabled;

Set up reverse DNS resolution of the email server to prevent illegal and fake domain names from sending spam. In addition, set the SPF record in the school DNS server to declare the IP address of the email address sent by the university email server domain, except for the IP address other than the one. The addresses are not legal, thus ensuring the reliability of the email source and effectively preventing spam;

Configure strict device login password, login account, login failure times, login IP address and other security policies, require password length of 8 or more, three-character types, and periodically change passwords, reduce the risk of brute password cracking, and configure the device regularly. File backup;

Restricted network device management addresses, allowing only fortress machines to access network devices;

Manage network and security devices through SSH or HTTPS to ensure secure transmission during management.

3.3 Host Security of University Email System

As the infrastructure for information system storage and processing of email system, the host system is the main carrier of information system software application. According to the requirements of the state for the 2nd-Level information security classified protection, the main system includes identity authentication, access control, security audit, intrusion prevention, and malicious. Code protection and resource control can be protected by the following security measures:

In the authentication access, you can restrict the email host to log in and manage only through the fortress machine. The fortress machine uses the user name and password to log in. The password policy is longer than 8 characters, three-character types, and password replacement is performed periodically;

The expired and redundant accounts are forbidden or deleted on the host, and the user is granted the minimum authority according to the management responsibility to realize system management;

The host starts the log service, records the important security time and operation, and starts the audit function through the fortress machine to perform log auditing;

Regularly upgrade the server's operating system, shut down unnecessary components and services, and only enable the necessary functions;

Install security software to detect and prevent intrusion and malicious code behavior.

3.4 Application Security of University Email System

In response to national requirements for the 2nd-Level information security classified protection, application security mainly includes identity authentication, access control, security auditing, communication integrity, communication confidentiality, software fault tolerance and resource control.

In combination with the actual situation of the construction of the university's email system, the following security measures are taken at the application level for security protection:

Enable email system password check, set to medium strength password policy;

Limit the number of current user logins, and the number of failures reaches a certain number of locked users for a period of time;

Apply the blacklist and whitelist function to blacklist the suspicious senders reported by the user to blacklist or real-time blacklist, effectively improve the interception rate of the email, and add the trusted IP or domain name to the whitelist;

Install an SSL certificate for the email system, log in to the email system through the HTTPS protocol, ensure the integrity of the information transmission, and encrypt the transmission information;

In terms of software fault tolerance, the email system can be balanced by F5 to ensure that the service of a single server is interrupted without affecting the operation of the email system;

In terms of security auditing, the email system includes detailed log information and ensures that it cannot be deleted by the administrator. The audit record is retained for at least 180 days;

Email information is archived online, classified, long-term retained and allowed to be searched and accessed in real time by using an email archive server;

In terms of resource control, you should limit the frequency with which individual users send emails, including the number of messages sent per unit of time and the total number of actual recipients in the same message.

3.5 Data Security and Backup Recovery of University Email System

In response to the national requirements for the 2nd-Level information security classified protection, data security and backup recovery mainly include data confidentiality and backup and recovery.

The important data of the email system, such as the transmission and storage of the authentication information, is encrypted, and in particular, the registered user information in the email system is encrypted and stored. Regular backup of the database and email, you can use the system tool "Rsync" to do regular backups, it is recommended that the backup data in different disk arrays to ensure data security. In addition, do a recovery demonstration on a regular basis to ensure that data can be quickly recovered once it is lost.

4. Summary

In accordance with the requirements of the state for the 2nd-Level information security classified protection, the security construction of university email systems is carried out at the network, host, application and data levels, thus effectively ensuring the security and stability of the university email system.

In addition, universities should establish relevant systems or norms for email security management activities and personnel practices, review and revise these systems, and increase the implementation of email security systems to enhance the awareness of the safe use of emails by college teachers and students. Only through multi-party collaboration can we fully guarantee the safe use of university email systems.

References

[1]. GB/T22239-2008 Information security technology – Baseline for classified protection of Information system security.

[2]. GB/T25070-2010 Information security technology – Technical requirements of security design for information system classified protection.

[3]. HONG Xin-hua. The study on effective deployment of Campus net-based mail system. Network Security Technology and Application. (2010) No. 7.

[4]. WANG Yi-chen, LIN Yu-song, WANG Zong-min. E-mail service troubleshooting strategies on campus network. Journal of Guangxi University: Nat Sci Ed. Vol. 36 (2011) No. 10.

[5]. Zhu Shou-rong, Pei Jun-feng, Ye Xin, Jin Ying-ying. Precaution and Practice for Network Security Based on Level Protection of Mail System. Computer Applications and Software. Vol. 34 (2017) No. 11.

[6]. Ma Lin. Research on Mail Archiving Technology. China Education Informationization. (2009) No. 10.

[7]. CHEN Yu-xin. Classified Protection Building-up Practice for Governmental Web Application Security. Information Security and Communications Privacy. (2012) No.10.