ELSEVIER

Available online at www.sciencedirect.com

SciVerse ScienceDirect

IERI Procedia 3 (2012) 142 – 147

Procedia
IERI

www.elsevier.com/locate/procedia

2012 International Conference on Mechanical and Electronic Engineering

The Research on Strategy of Building Campus Network Security Based on University Management

Ma Tao,Wei Shaoqian,Liu Minglian,Wu Baozhu

Teachers' College of Beijing Union University

Abstract

Campus network play a crucial role in the study and management of the daily work of schools. With the rapid development and popularization of the campus network, the security issues become increasingly prominent. How to make safe and efficient operation of the campus network, give full play to its teaching, management and service functions, has become an issue cannot be ignored. On the basis of the analysis of the characteristics and common threats to the campus network security management, network security commonly used techniques such as firewalls, VLAN, and so on, made a series of security policy for the campus network characteristics.

Key words :campus network security threats strategy

1. Introduction

The campus network is a collection of teaching, research, administrative, educational administration and general management functions into one integrated network, it has inline Waiyin function, to meet, including Internet services, remote education services, electronic bulletin board, and video conferencing and off-campus data communications services and other requirements. With the rapid development and wider application of computer technology, network technology, the campus network in the school teaching and management play an increasingly important role for teachers and students work, study, living provides a great convenience, is about to change traditional teaching and management models. However, the security issues are increasingly highlight: computer viruses, hacker attacks, data tampering and loss of network security risks, posed a grave

doi:10.1016/j.ieri.2012.09.024

threat to the campus network. Once these security risks attack, will bring a lot of negative impact, can have serious consequences. Therefore, to understand and analyze the security risks, take the right strategy to resist the threat, is the fundamental construction of the campus network security is the protection of the campus network to function properly.

2. The campus network security threats

The reasons for the campus network and other network compared with its own characteristics, pose a threat to the safety of the campus network and the presence of the security risks are not the same. Due to the particularity of the campus network, campus network security threats are mainly produced in internal and external causes is followed.

2.1. Internal security threats faced by the Campus Network

The weak sense of confidentiality. Unauthorized access to internal users in the campus network is one of the main campus network security is threatened, the most likely to cause leakage or tampering with system resources and important information. For example, a school student in the campus network stumbled on the teacher computer papers, the results lead to many students around East rummaging, because the teacher's computer did not add any access restrictions, students simply in the Network Neighborhood be able to find the required data; In addition, some of the campus network for simple and save time, the naming of the computer often named after the name of the department, the computer's administrator account does not make any modifications to the default account, do not even set the login password, which is equal to The attacker opens the door, so that an attacker can easily find the target of interest from intruding into the confidential content, feel free to browse more dangerous, and some data of non-authorized any changes, there is no security can be statement.

Internal users to malicious attacks. This is another major cause of the campus network security is threatened. Schools focus on the local computer users, there is no lack of students master; at the same time, the curiosity of the student's weight, imitation and strong, even if the level is not high, can also be used to attack other people's computer, special software downloaded from the Internet. According to statistics, about 70 percent of the campus network attacks from internal users, as opposed to external attack for internal users more advantageous destruction. I taught at the school, the campus network of several servers are often attacked by students, some out of curiosity, some for malicious retaliation, especially the Credit Management System, is an important goal of student attacks.

2.2. External security threats faced by the Campus Network

Computer viruses. Computer viruses are the main reason for the campus network is facing external security threats. Due to the particularity of the campus network user base, the students often download software to use, often share resources with each other, provides a favorable way for the spread of computer viruses. With the rapid development of computer network, computer viruses spread more widely, the proliferation of faster and faster, more powerful destructive, the threat to the campus network is also growing. I school campus network, for example, the 2004 "shock wave" and "Sasser spread to install Windows2000 computer within the campus network; December 2004, a student opened the one containing the words" Love the back door " a virus, resulting in "Love the back door" into a network of DIY classroom, the virus constantly search network resources, resulting in the entire local area network resources are occupied, where there are shared directory on the viral replication in the past in a very short period of time 56 computers on the network in a semi-paralyzed state. The threat of computer viruses on the campus network is evident.

Hackers. In addition to the face of attacks from internal campus network but also to prevent attacks from external hackers. External hackers hacker programs, system vulnerabilities, remote control computer, and even direct damage to computer systems. Tireless hacker usually implanted in the user's computer with a Trojan virus, Trojan horse inside and outside the collusion poses a threat to computer security and thus endanger the network.

2.3. Campus Network defects and physical security threats

Addition by the security threats from inside and outside the system, the campus network, there are other security risks:

System vulnerabilities. This is one of the reasons for the defects of the campus network. Because of the huge operating system code, in varying degrees, there are some security vulnerabilities, some of the widely used operating system, such as Windows2000/xp security vulnerabilities more, plus the system administrator or use of complex systems and their own security mechanisms do not know enough, improper configuration, thus forming a security risk.

Physical security threats. Network surrounding environment and physical properties of network equipment and wiring is not available, such as the device is stolen, destroyed, destruction or intentional or not, link aging, resulting in information disclosure due to electron irradiation equipment unexpected failures, power outages and natural disasters physical factors of the destruction of harmful gases, etc., will also pose a threat to the normal operation of the campus network.

3. Campus Network Security building strategy

An undefended network or to prepare for a defective network at any time may be subject to threats, the existence of security risks attack, will bring unpredictable consequences, a serious cause of system crashes, network paralysis. Therefore, to take effective measures to ensure network security, it is very important. According to the characteristics of the campus network, to ensure the safety of the campus network, you must make an effort in the education of internal staff management and technology fortification.

3.1. to strengthen safety education to strengthen the management practices

To improve safety awareness. Internal prevent most important thing is to strengthen the network and information security education so that all users and network staff to establish a security awareness in the minds of. Especially to teach students to comply with network security management system and the national network information security regulations, to prohibit unauthorized access, you want to educational content and form of institutionalized and regular students in terms of ideology to establish network security, high-voltage.

Establishment of the secrecy. Network managers to monitor and audit the behavior of the user's actions, centralized management of confidential information and confidential documents, the implementation of the confidential storage and transmission of confidential content, not have access to personnel, non-contact information storage address. Data encryption and key management by the person responsible, the other person is not entitled to be informed of passwords, keys and decryption methods.

Serious management discipline. Malicious operation of the internal staff or intentional release of virus, in conjunction with school management, and an investigation has revealed that the abolition of the access qualifications, be given administrative sanctions, serious legal liability.

3.2. The proper use of the password the encryption means

Set a password. To frequent changes to the system administrator account and set arbitrary, there is a sufficient length of the password, the password anti-cracking ability, so that the attacker is difficult to find the account number and password to use the software program to crack the code more difficult. The password you set should be a complex password with letters, numbers, special characters, and cannot leave a record on the computer; can also build an "Administrator" trap accounts, does not confer any privileges, plus a super-complex password. Thus, even if the password is cracked, the attacker came with nothing.

Use the same password does not know that such has left a security risk. Because attacks are generally cracked a user's password, use this password to try the user every one that requires a password, so you want to use different passwords in different places

The use of encryption means. Web-based services, network security protocols, transmission encryption of Web services are generally implemented at the application layer, the storage and transmission of confidential information encrypted to prevent eavesdropping and hacking. WWW server to send confidential information, new technology, according to the IP address of the recipient or other identifier, select the key to encrypt the information operator; browser receives the encrypted data, according to the information in the IP packet source address or other identifier decryption of encrypted data, but also left interface, users can reload the encryption and decryption algorithm to construct your own encryption and decryption module. In addition, you can encrypt files and folders "feature, to prevent others from using the computer peek.

3.3. The use of anti-virus techniques adhere to the preventive detection

Route of transmission of computer viruses, it is necessary to take effective preventive measures and testing methods.

Ideological importance, strengthen management. Any copy information from the external floppy disk to the machine, should be on a floppy disk for virus scanning, if the virus must be removed, so you can keep your computer is not new transmission of the virus; In addition, because of the latent virus, it may also concealed the machine some old virus, when the time comes will attack, so, we should always check the disk, if a virus is found to be promptly removed. The most commonly used anti-virus software, made Rising, Jiangmin, Jinshan, foreign Norton, Mcafee, Trend, but the price is expensive than the domestic.

Grasp the anti-virus techniques, adhere to the use of unremitting. The ideological importance is the foundation, to take effective virus scanning technology to ensure. Effective defense against computer viruses, must adhere to the use of the following tips: Never open e-mail of unknown origin e-mail attachment, or are not expected to be received; install anti-virus products at least weekly updated virus definitions; installed on your computer for the first time the anti- virus software to ensure that the machine has not been given a virus infection; ensure that the computer insert floppy disks, CDs and other removable media and e-mail, Internet files do automatic virus checking; not from unreliable sources to download software security download software virus scan prior to installation as a guide; do not use a shared installation of software or copy the shared floppy disk, which causes the virus to pressure spread from one machine to another machine, the way; many virus worm uses the Windows Scripting Host may, without the user clicks, you can automatically open an infected attachment, you want to disable WSH.

To take the defense monitoring, killing the virus in a timely manner. It is necessary to install a set of anti-virus control server in a campus network and the other host to install anti-virus client, unified download the virus database from the server, and distributed to the client, so as to better anti-check kill the virus; within the campus network through the Sniffer software in a timely manner to discover the possible virus infection: the Sniffer software, a host and the rest of the campus network, dozens of host contact, and continue to send packets, which that this host infected with a virus; campus network access WAN can be found by setting the router possible virus infection: If you see a host continuously to the other host to send 48-byte packets, indicating that the host is likely to be infected with viruses.

Use of content filters and firewalls.Filter technology can shield the poor site, and have powerful interception of Internet pornography, violence and cult. The firewall technology includes dynamic packet filtering, application proxy services, user authentication, network address forwarding, IP anti-counterfeiting warning mode the sound of logs and billing analysis, intranet and extranet to isolate protect the campus network from intrusion by unauthorized third parties.

Use Vlan technology.ASwitched local area network technology (ATM or Ethernet exchange) of the campus network, you can use the Vlan technologies to strengthen the internal network management. Vlan technology is the core of the network segment, based on different applications business, as well as different levels of security, network segmentation and isolation, to achieve mutual access control, you can achieve the illegal purpose of the visit of the restrict users. Network segment can be divided into physical segmentation and logical segmentation in two ways. Physical segmentation usually refers to the network at the physical layer and link layer of the data segment is divided into several segments, each segment cannot communicate directly with each other. Logical segmentation segment sucked the entire system on the network layer. In the actual application process usually take the physical method of combining segmentation and logical segments.

Anti-virus software.Select the appropriate network anti-virus software can effectively prevent the spread of the virus in the campus network. It should have the following characteristics: ① able to support all system platforms, and software installation, upgrades, configuration of the central management. (2) To protect all possible virus entry in the campus network, that is to support all Internet protocol and e-mail system may be used to adapt to and kept pace with the rapidly changing pace of the Internet Age. (3) Has a strong protective function, the data the program can provide effective protection.

Access control. This is one of the most important measures of network security and protection, whose main task is to ensure that network resources against unauthorized use and unauthorized access. The user's network access control is usually a username identification and verification, identification and authentication of the user password, user account default limit checks. When the user enters the network, the network system to give this user access rights, users can only operate within its competence. In this way, to ensure that network resources from unauthorized access and illegal use.

3.4. focus on physical techniques to fix vulnerabilities

The focus on physical security. Focus on physical security of servers, switches, routers and other hardware in the entities and communication links in the network system protection from natural disasters, man-made destruction and attacks, to ensure that the network computer system has a good electromagnetic compatibility environment; to establish a complete management system to prevent illegal entry into the computer control room and all kinds of theft, sabotage occurred.

Using firewall technology. The best means of defense external threats is the use of the strong performance of the hardware firewall, which not only provides password protection to the network, and to restrict access to specific database application based on user login. Firewall to prevent intruders penetrated, allowing to identify and block rogue applications, to save bandwidth for business-critical traffic. Efficient network technology with high confidentiality requirements of the credit system and management system is critical.

To fix vulnerabilities. Any system is perfect, perfect, therefore, to strengthen the security of the host system, to install patches and security patches are necessary, it can make up the system security vulnerabilities in a timely manner. Should use the system vulnerability detection software to scan analysis of the network system on a regular basis, to identify possible security risks, and in a timely manner to repair. Commonly used in domestic scanning software X-Scan, it has the advantage is you can specify to scan a network segment, convenient and practical, can be seen that the scan results from the test report. This practical method of scanning the campus network system, including network devices, hosts, operating, inspection, reporting systems vulnerabilities and security risks, and proposed remedial measures and security policies, to enhance security.

4. Conclusions

Campus Network Security is a systems engineering, and not rely solely on one aspect of security policy, the need to carefully consider the security needs of the system, targeted internal education and management, cryptography, virus prevention detection, system bug fixes, firewall technology , physical security awareness and security technologies combine to produce an efficient network security systems. Of course, with the continuous development of computer network technology, the means and methods of maintenance of the campus network security will be more comprehensive; campus network will also be in the schools play an increasing role.

Reference:

[1] Wang Zhixian. Computer virus and its prevention in the modern network environment. "Computer network" 2005.3,4.

[2] Jiang Shaoping. Network security risk analysis and optimization. Computer and Network 2005.6.

[3] Dai Yingxia. Computer network security. " Tsinghua University Press, 2005.

[4] Zhang Yuqing. Security scanning technology. " Tsinghua University Press, 2004.

[5]Yang Yinhua. two types of Web server comparison of the data interface based on the MVC [J]. Computer Application and Software, 2006, (2): 69-71.

[6]Sun Ao, Huang Yan, Wu Ping. MVC mode. NET Framework and Implementation [J]. Technology Square, 2006 (1): 69 - 71.

[7] Lei Zhengrong,Wu Weichun. The campus network security and strategy [J. Guangzhou University (Social Science Edition), 2006.

[8] Shi Zhiguo, Xue Weimin, Yin Hao . computer network security tutorial [M]. Tsinghua University Press, 2007.

[9]Chen Liangkuan.Practical technology of computer networks tutorial, Beijing: Science Press, 2001.6

[10]Shi Shuo. Experimental computer network technology, Beijing: Electronic Industry Press, 2002.9