On Campus Network Security System of College and University

Ning Huang
Center of Modern Educational Technology, Gannan Normal University, Ganzhou, China
Email: hngzjx@qq.com

Zhongming Jiao
Collage of Communication and Media, Gannan Normal University, Ganzhou, China

Abstract—The rapid development and wide application of computer network effectively promoted the development of China’s economy and information technology, but network and information security problems also came. In our view, we should focus on management on one hand and grasp network security technique on the other hand. Both are equally important. Without the support of management, even the best technique does not work. Conversely, without technique, management becomes empty words. The management system mainly includes construction of leading bodies and technical team, establishing a set of rules, technology implementation strategy, and construction of internal and external environments. The technical system mainly includes physical security, reasonable network topology, the efficiency and reliability of network, the application security, against network attacks and data storage security. Campus network security management is a complicated and systematic project and it needs to be integrated into the agenda of college and university management and the cooperation of staff and students of the whole college and university.

Index Terms—Campus network, Network security, Protection system, Security management

I. INTRODUCTION

The rapid development and wide application of computer network effectively promoted the development of China’s economy and information technology, but at the same time, network and information security problems also came, therefore, e-commerce, finance, network security was compromised, relating to national security and commercial secrets of the computer system by hackers and viruses, causing leakages, some criminals take Black Hand reaching for computer information systems, either by directly modifying the illegal profits of computer programs, data, using the computer as the instrumentalities of criminal activities. All of these illegal invasion cause economic loss, threaten national security, cause panic and undermine social stability. Campus network of college and university is not paradise. With the growth of scale of digital campus construction, security problems arouse. How to establish reasonable and effective deployment of campus network security management system in college and university faced the grim task. This paper will explore these major issues. In our view, we should focus on management on one hand and grasp network security technique on the other hand. Both are equally important. Without the support of management, even the best technique does not work. Conversely, without technique, management becomes empty words.

The rest of the paper is organized as follows. Section II focuses on the management system in 6 subsections; Section III focuses on the technical system in 7 subsections; Section IV gives conclusions.

II. THE MANAGEMENT SYSTEM

A. Construction of Leading Bodies

Network security management is to manage in a word. Network users frequently demand more authority, more resources, and more convenience than actually needed. This desire results in the contradiction between user’s behavior and security management. If each user of the campus network could go its own way without any limitation, the campus network would be in a state of disorder and confusion, not to mention security. The basic guarantee of security measures is to set up a leading group of campus network security management directly under the leadership of the president of the university, with department heads as members, taking network security management as a daily routine of the university. This group can also serve as university information construction leading group to ensure the implementation of the rules. The governing body should not only include college and university leaders, but also technicians from various departments as group members. They deployed the department’s tasks and the implement specific tasks of collecting, collating, resolving or reporting problems.

B. Construction of a Technical Team

Both correct development of objectives of network security management and realization of goals depend on a qualified technical team of network security. Technical team members make and implement specific plans. Leaders use the authority to provide”the imperial sword”. In order to facilitate the work, the leadership group should have technical members. Each technical member should have a strong sense of responsibility, spirit of study for qualified technique. In order to continuously
improve the skill level of this team we should provide learning conditions by means of training at various levels of schools, seminars, raising the theoretical level of technicians as a whole. Through the implementation of the network security management system, we can improve the team’s working ability.

C. Establishing a Set of Rules

An effective set of network security management rules mainly includes information system security management, information system data management, computer room management, information system operations management, information system emergency management, information system performance management practices, computer resource management, information system archive management, network management, virus management approach and a series of supporting rules and regulations. The rules should be both scientific and operative. Once the rules are published, they must be firmly complied with in daily works. In order to avoid the so called: "first-firm, second-slack, third-invalid and forth again", the rules should be part of rules and regulations of the university. With the passage of time, rationality of rules decreases. Leading group should study the actual situation and establish new rules in time to fit the new case.

D. Technology Implementation Strategy

We can technically deploy unified planning, unified arrangement, and unified action and block rule. Unified planning is predictive of, or at least see the size and trend of development of campus network within 5 years, the overall design to the entire university’s network security scheme. This can avoid aimless investment and problems such as incompatibility or repeated construction. Unified arrangement is to dispatch and perform specific tasks under the leadership of the information security leading group of the university. Any project should not start without the permission of the group. Any security product should not be used on the campus network without the permission of the group. Unified action that is to complete the tasks assigned by the leading group in a specified period of time, implemented by the technical members of command at all levels. Block rule is to decompose the task down into departments like building blocks, forming cooperative engagement pattern as a whole.

E. The Construction of Internal Environment

Security management of campus network does not exist without a qualified internal environment that includes hard ware, software and user. Of all the three factors, user is most important. To make a good internal environment is to cooperate each other like a chess game through a variety of ways, according to the security rules, and not to see each technician play solo. In terms of rule implementation, refinement of various rules is required. Daily work processes, emergency handling procedures and so on should also be refined down to every section, which is no longer an abstract concept, but a practical instruction.

In terms of information and device security, we should classify management, clearly delineate permission range of various information and device, so that appropriate security is obtained under the principle of "minimal required permission".

F. The Construction of External Environment

Campus network is not an isolated LAN in China, usually having connections with China Net, Carnet, and the bank network (in the case of Campus Ecard). Campus network access such extranets via the service of ISP (Internet Service Provider). When the extranet blocked, technicians reported to relevant campus leaders who contacted the leaders of ISP later. Task to solve the problem was assigned to the technicians of ISP by their leaders. Technicians on both sides begin the communication to solve the problem. This is something like an up-side-down ISO network protocol layering model. This seemingly reasonable procedure spends a lot of precious time for the university to solve the problem. If the university improves relation between ISP, the "reciprocal" friendship can be developed. In the event of emergency, the leadership on both sides and the technique layer on both sides can make conversation at the same time such that the restore process can be greatly shortened.

Good ordered network is the basic assurance of security. With good relation between university and ISP, we can promote network security level of the university by learning advanced practice experiences from ISP. We can also promote the level of network security management by using service of a different ISP for redundant backup. On one hand, it can reduce the risk. On the other hand, introduce a competitive mechanism for ISPs to improve their service quality.

III. THE TECHNICAL SYSTEM

A. Physical Security

We should assure security of our central labs and departmental labs along with the devices in them. Antitheft, fireproof, waterproof, anti-magnetic, anti-static, anti-lightning measures should be effective. We should focus on safety construction of central labs to lead security construction of equipment rooms of departments. Campus network security cannot be guaranteed without physical security. Therefore, we should build central labs well according to the relevant national standards. For example, references [1-6] are appropriate standards in China.

B. Reasonable Network Topology

Reasonable network topology improves network security and efficiency. Dual redundant backup of switches, routers will help us improve service abilities of devices. Various kinds of applications should be packed in various subnets according to the security level of applications. Security products such as firewalls and anti-virus switches should be applied at the boundary nodes to
assure secure access to the important devices. More reasonable restrictions on broadcast domains can be achieved by the division of VLAN. This increases network efficiency and controls of sharing reasonably. Multi-level hardware firewalls of different manufacturers are expected to fend illegal attacks from external and internal network efficiently. Hardware firewall policy optimization improves the reliability to prevent hacking.

C. The Efficiency and Reliability of Network

First, routers, switches should be selected from qualified products by the same manufacturer with leading technology to assure quality and compatibility. Quality and compatibility of communication equipment impact on network performance directly. Leading manufacturers of products mean quality and security. Devices of the same manufacturer assure the quick replacement in the event on of emergency.

Second, let us discus the bandwidth planning and design. No matter how large a campus network bandwidth to the Internet is, compared with LAN, there will always be a bottleneck. If we do not make any restrictions, there should be some users who consume large amounts of bandwidth such that others can hardly access to the external. Bandwidth management is to restrict bandwidth for each user to provide stable, reliable service, improving the overall performance of users accessing the extranet.

Third, it is the planning of the IP address. Network management of IP address management issues is difficult. A good plan can bring about a lot of convenience to network management. Experience has shown that the computer user’s real name, the binding IP address, MAC address, with the unified authentication or authentication gateway, together with effective means of administrative penalties are effective to solve IP address embezzlement problem.

D. The Application Security

With uniform identity authentication, users do not have to register in each system and log in various application systems within the campus. This avoids trouble, confusion and duplication of data resource storage [7]. Uniform identity authentication is designed as a standalone module. Its task is to provide the security of the system. In general, its security level is higher than a single subsystem’s authentication modules. Once a uniform identity authentication is used in campus network, the only entrance of each application should connect with unified identity authentication seamlessly. Therefore it gets higher security.

In order to raise the security level, we should also consider higher security level of a cryptographic algorithm, such as 128-bit SSL. Protocol widely used on finance or e-commerce website’s [8]. SSL (Secure Socket Layer), protocol originally developed by Netscape Enterprise Development, has now become a global standard to identify users as well as encrypt communications between web site server and web browser. Because SSL technology has built into most major browsers and WEB server programs, we only need to install a digital certificate, or server certificates to activate the server functionality. Furthermore, SSL can effectively prevent attacks based on wiretapping and data package crawling.

E. Against Network Attacks

One of the main tasks of the network security management is to defense against a wide variety of attacks from the network. These attacks may be made, or may be caused by computer viruses. The targets of the attacks may be servers, switches, routers, and may also be personal computers. Many attacks may scan and make use of the target system’s vulnerabilities. The establishment of specialized, automatic upgrade patch server and implementation of automatic upgrading of system patches are effective ways to fend attacks.

Nowadays it is difficult to distinguish between the hacking program and computer viruses. On one hand, many virus programs feature with hacking ones. On the other hand, many hacking programs act as viruses. The establishment of a robust antivirus system is also an important task of preventing attacks. Anti-virus system should at least include anti-virus software of network version and anti-virus gateway products. The former kills viruses and upgrade in the entire network at the same time. The later blocks worms for the campus network. Zombie virus has caused great harm, let alone all kinds of worms. Currently, the number of “zombie computers” in the world increases daily by about 170,000. Chinese computer users do not pay enough attention to operating system vulnerabilities, resulting in unprotected computers vulnerable to attacks in the access to the Internet in just a few minutes [9]. Number of zombie computers of spyware is growing at more than 200%.

Large amounts of security problems occur in the user terminals, which leak a high incidence of information. Of these, about 20% of zombie computers from the United States, 15% from China, 6% from Germany, 5% from France, 3% from the United Kingdom. Half of spam comes from zombie computers which spread Trojans and viruses and malware. Hackers use zombie computers to do DoS attacks. Illicit enrichment via zombie computers decoy spread information. Illegal enrichments spread decoying information via zombie computers to steal user name s and passwords [10]. Thus, it cannot be ignored to improve the security personal computers. Ten steps of works are suggested to ensure personal computers , see reference [11].

Other security products, such as network management, intrusion detection, encryption transmission, vulnerability scanning and anti-scanning, anti-denial of service attacks, anti-snooping sources and IP address, anti-brute-force, anti-spam, email virus scanning, the networking equipment to monitor illegal outreach and waterproof walls and other network security products, can be selected according to the real need and the security level of campus network.

F. Data Storage Security

Data security is a very important aspect of campus network security. Damaged hardware can be replaced.
Crashed system can be reinstalled. However, once the data are lost, they are difficult to be restored. Therefore, we should focus on data backup. With a variety of media such as tape, CD backup, we can guarantee continuity of service. By using hot spare, mutual backup, load balancing, or duplex mode, we can improve the continuum of service capacity and reliability of the device. SAN (Storage Area Network) may be a good storage solution [12] to adapt to the development of gigabit network.

We should consider both system and application to make scheme of data backup and restore to develop a high degree of automatic, visualized method which is easy to operate. If conditions allow, we can also consider offsite disaster recovery.

G. Joint Action of Multiple Security Products

Monitoring server to complete the following tasks: It gives instructions to personal computers infected with large number of viruses. It closes specified ports of personal computers to prevent them from sending large amounts of virus packets to network communications equipment. It automatically forced to install designated anti-virus software to the personal computers without running that anti-virus software, or issue a warning, and guide users to access the specified server to install the appropriate security products. When it finds the personal computers act as hackers, it automatically sends warning messages and deletes their hacking tools. It automatically generated and added new rules to the firewall according to the analysis of intrusion detection systems against harmful packets. It protects critical servers against attacks of service denying and automatically shields harmful packets.

Only the use of advanced network security products, improve security management in order to adapt to the increasingly complex network environment. We can only adapt to increasingly complex network environment when we continue using advanced network security products and improving security management.

IV. CONCLUSIONS

Campus network security management is a complicated and systematic project. It requires administrative and technical attention at the same time. If we ignore any of them, we are unable to assure the campus network security. Security management of campus network is not only duty of few technicians. It needs to be integrated into the agenda of college and university management and the cooperation of staff and students of the whole college and university.

ACKNOWLEDGMENTS

The author is grateful to the editors, reviewers and any other helpful people for their valuable comments and suggestions to improve the presentation of this paper.

REFERENCES

[9] Infected Computers in China, PC Week 2006-3-6 P.17.

Ning Huang, born in 1958, received Master’s degree in applied mathematics and computer science from Jiangxi University, China in 1991, awarded senior engineer of the Industrial and Commercial Bank of China in 2001. He is now with Center of Modern Educational Technology, Gannan Normal University, Ganzhou, China, as an associate professor. His research interests include information security and digital campus.

Zhongming Jiao, born in 1962, is now with College of Communication and Media, Gannan Normal University, Ganzhou, China, as a professor. His research interests include digital campus and education management.