Research of Campus Network Information Security

Yao Zhang

(College of Information Engineering, Zhengzhou University Of Industrial Technology, Xinzheng 451150,China)
304963405@qq.com

Keywords: Campus Network; Information Security; Security; Cyber Security

Abstract. The paper relies on the design of network security in the network engineering of a university's campus network to comprehensively analyze the security status of the campus network and the needs of campus network security. Focusing on the analysis of security issues, we conducted an in-depth study of the campus network security architecture, analyzed and studied a variety of common network security technologies, and deployed corresponding solutions in each regional module to solve the network security problems existing in the campus network and ease the campus network Cyber attacks. The whole design idea, solution and technology realization of this topic have certain reference value for the construction and transformation of campus network in most universities.

Significance of Campus Network Security Construction

The campus network provides a learning and communication platform for teachers and students in various fields such as teaching, scientific research, teacher-student mutual learning and communication, and library management. It facilitates school management personnel in the aspects of school facilities, enrollment, student achievement, student status, etc. management. Improve school teaching, research, management and learning environment; familiar with the modern working environment and master advanced teaching, research, management and learning methods, is conducive to the training of modern, high-quality personnel.

With the continuous improvement of the construction and application of campus networks, the modern management level of universities has been greatly improved. It broadens the channels for students to acquire knowledge, improves the school's management level, and promotes the informationization and networking of education. Therefore, building a low-cost, high-performance, high-intelligence campus network is the goal of each university's future development and the direction of its efforts.

Campus Network and Network Security Related Concepts

Network Security Overview. Network security refers to securing the hardware, software, and data information in a network system. When subjected to attacks, tampering, or disclosure, ensure that the system is functioning properly so that network services will not be interrupted. Objectively understand that network security is to ensure the security of network data information. In a broad sense, network security refers to the availability, integrity, and security of data information on the network [1].

Ways to Protect Network Security. In order to protect the network security, the following are commonly used technical means:

(1) Firewall technology. A firewall is a technical measure to protect the security of a computer network. It establishes a corresponding network communication monitoring system at the network boundary to isolate internal and external networks so as to block intrusions from external networks. It is mainly divided into Packet Filtering, Application Proxy, and Stateful Packet Filtering.

(2) Intrusion detection technology. Intrusion detection technology is a technology designed and configured to ensure the security of computer systems. It can detect and report unauthorized or abnormal phenomena in the system in time. It is a technology used to detect the violation of security

policy in computer networks. The combination of software and hardware for intrusion detection is an intrusion detection system (IDS).

(3) Antivirus technology. The built-in anti-virus technology of the CPU is a kind of hardware anti-virus technology, which cooperates with the operating system to prevent most of the attacks against buffer overflow vulnerability. Intel's anti-virus technology is EDB. AMD's anti-virus technology is Evanced Virus Protection (EVP). However, whatever their name, their principles are similar.

(4) Data encryption technology. The so-called Data Encryption (Data Encryption) technology means that a message (or plain text) is converted into a cipher text through an encryption key and an encryption function, and the recipient will This ciphertext is decrypted into a plaintext through a decryption function and a decryption key (Decryption key). Encryption technology is the cornerstone of network security technology [2].

The Establishment of a Network Security System. The definition of the network security system: The network security management system is an application system that combines security technology and security management within the network system to realize multi-level security assurance of the system. The complete security system of the network system is shown in Figure 1.

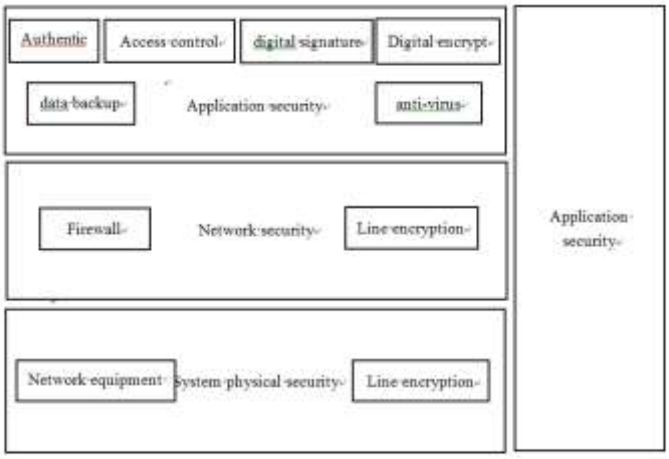

Figure 1 The complete security system of the network system

Analysis of Campus University Network Security Status

Analysis of Campus Network Demand in a University. In view of these risks in the campus network, security risk analysis must be done when designing security solutions, and corresponding security solutions and measures must be taken to address the risks [3, 4]. There are many major security factors faced by a university's campus network. The following three factors are more prominent.

(1) Design aspects of cyber security system. The early campus network security system can play a role in the security of small networks. However, for today's rapidly growing campus network, it has grown from dozens of hosts to several thousand host large-scale heterogeneous networks. The system can no longer meet the security requirements of today's campus networks. Under the network security system of this university, the most prominent problem is that the server and the core switch often crash and the network service cannot respond. The main reason for the analysis is that in the campus network security system, the firewall only comes from outside the network. Attacks are resistant. The internal network anti-virus system can only remove infected viruses from the host. Therefore, attacks from within the campus network cannot be defended. Frequent crashes in the network are caused by flooding attacks in the network.

(2) Network hardware security. During the construction of the school’s campus network, due to insufficient attention or architectural building design issues, various problems appeared on the

network lines, which made the data transmission on the physical layer of the campus network unreliable; and due to financial problems.

From the school's network physical topology, the outstanding performance problem is that when only the core switch is attacked during a period of time, such as the above mentioned red-hot attack, if it fails to work properly, it will cause the entire network to paralyze because there is no redundant design. Therefore, during the recovery of the network, it is impossible to provide services for campus users, thereby influencing the normal work of the campus.

(3) Network Attacks. The university's cyber attacks come mainly from two aspects: external and internal attacks.

Attacker type network attacks are initiated by attackers. Attackers who can analyze the school's campus network for cyber attacks can be roughly classified into three categories: Figure 2 roughly shows the actual number of attackers of the three types.

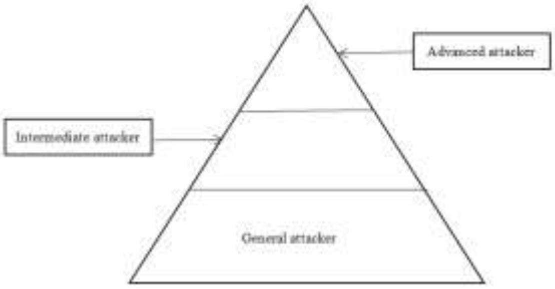

Figure 2 Attacker type and ratio

2) Attack classification The method of network attack is very flexible. It is difficult to accurately classify attacks. Some attacks meet multiple classifications, while others are difficult to classify. The attack analysis from the school network can be divided into physical attacks, active attacks, passive attacks, and man-in-the-middle attacks according to the physical location of the attacker and the attacked person. It can also be divided into read attacks based on the results after the attack. Manipulation attacks, spoofing attacks, flood attacks, redirect attacks, and hybrid attacks.

3) Attack Steps Attacking the campus network is the same as the normal network attack procedure. Divided into information collection, access to permissions, installation of the back door, expanded impact and elimination of traces.

4) Attack Results All attacks generate specific attack results.

Risk Analysis of Campus Network in a University. Based on the above analysis of demand and combining with the actual situation of the university, the following risks in the campus network are analyzed:

1.a large number of network viruses

2.Serious misappropriation of IP and MAC addresses

3. when a network security accident occurs, the user cannot be accurately located

4.the user access time, user network permissions control

5. various network attacks can not be effectively shielded

6.the device does not have redundant design

In summary, combined with the risk analysis method, the network terminal, network management area, network border area, and network core area in the university campus network have the highest level of availability risk, followed by information leakage, natural factors, and data integrity. There is a risk.

Campus Network Security Planning and Design

The entire campus network security is divided into four parts: attack protection, network boundary protection, security control and audit, and unknown threat protection. Each part includes multiple child security solutions.

(1) Attack Protection. DDoS attack protection scheme. Protecting DDoS attacks, which are the most popular and extremely harmful at the moment, through sophisticated seven-layer filtering technology; Intrusion detection and defense solutions. Intrusion behaviors such as Trojan horses, worms and backdoors are protected against various intrusions from within and outside the campus network data network.

(2) Border protection. Border access control security scheme. Through reasonable division of campus network data networks, effective access control and isolation are implemented at the network boundary; Network anti-virus security solutions. The network anti-virus gateway performs virus detection and protection on the traffic transmitted in the network to prevent the virus from spreading in the campus network data network.

(3) APT attack protection. Comprehensive traffic detection: Provides independent traffic restoration capabilities and can identify mainstream network protocols HTTP (Hypertext Transfer Protocol), SMTP (Simple Mail Transfer Protocol), POP3 (Post Office Protocol), FTP (File Transfer Protocol) to ensure identification All files transmitted over the network.

(4) Security Management and Audit. Unified security management program. Collect logs, alarms, and other events on the entire network, centrally correlate them, identify the root cause of the problem, quickly generate accurate security alerts for the operation and maintenance personnel, and output various compliance reports; Unified safety equipment management program. Centralized management of various security devices on campus network data networks; Security audit program.

At present, the campus network security is generally considered from the aspects of network supervision, border defense, access security, and remote access. Access security mainly guides campus security access, including terminal security access control, such as user isolation and port isolation. Remote access involves branch offices and business travelers' secure access to the campus. Border defense passes through the firewall and IPS / IDS effectively protects and isolates campus exits and organizational units on campus [5, 6].

Conclusion

The paper takes the campus network of a university as the background, analyzes the network security problems that appear in the campus network of this university, and according to the network security problems, takes the network security design principles as the guidance, carries on the demand analysis and the risk analysis, and deploys according to the analysis result. Corresponding security policy, combined with the actual situation of the university, gives the corresponding solution. The network technology and solutions involved in the paper have a wide range of application prospects in campus network security. The design ideas, solutions and technology realization in the paper have certain reference value for the current campus network construction and transformation of other universities.

References

[1] Meyer,Claire. Growing Security for a Growing Campus[J].Security,2014.

[2] Dix,John.University of Florida gets 100Gbps link to Internet 2,upgrades campusResearch net to 200Gbps[J].Network World(Online),2013.

[3] Wei,Hongjuan.Research on the Security Risk sand Strategies of Campus Wireless Networks[J].Journal of Convergence Information Technology,2013.

[4] [US] Mark, Stamp. Principles and Practice of Information Security [M]. Beijing: Tsinghua University Press, 2013.

[5] Zhang Feng. Design and Implementation of Campus Network Security System [D]. South China University of Technology, 2009.

[6] Yu Chao. Computer Network Security Hidden Trouble and Emergency Response Technology Analysis [J]. Information and Communications, 2015,1 (4): 185-191.