An Analysis of Information Security and Protection Strategies in Colleges and Universities in the Environment of Smart Campuses

Zhiyuan Huang*
Keyi College of Zhejiang Sci-tech University, Shaoxing, Zhejiang, China

*Corresponding author e-mail: huangzy81@haoxueshu.com.cn

Abstract. Smart campus construction is constantly promoted in colleges and universities. While teachers and students in colleges and universities are having convenience provided by smart campuses, their information security is also facing unprecedented challenges. This paper analyzes all kinds of threats to information security of colleges and universities in the environment of smart campuses, and explores the protection strategies of information security in view of the construction of smart campuses in many aspects.

Keywords: Smart Campus, Security Threat, Protection Strategies

1. Introduction
With the development of information technology, and the promotion of national education modernization in China's long-term education plan, Chinese colleges and universities attach great importance to the construction of smart campuses nowadays. Smart campuses are advanced forms of college informatization. They comprehensively apply cloud computing, Internet of Things, mobile Internet, big data, intelligent perception, business intelligence, knowledge management, social networking and other newly-developing technologies. Meanwhile, they can fully perceive the physical environment of the campus, identify intelligently students' and teachers' study and work situation and individual characteristics. What's more, they can organically connect the physical space and digital space on campus to establish an intelligent and open education and teaching environment and a convenient and comfortable living environment for teachers and students. However, due to the characteristics of information technology itself, the inadequacy of protection measures, and the lack of network security awareness of teachers and students, the information security problems have become more and more serious.

2. Threats to Information Security in the Environment of Smart Campuses

2.1. Security Threats from Terminal Devices
There are a huge number of computers, mobile phones, pads and other Internet-connected terminal devices in colleges and universities, and these devices belong to the same local area network. Due to loopholes in the operating system or application programs of the terminal devices, viruses like Trojan...
horse are very easy to infect these devices. Once a device in the local area network is infected with a virus, the virus can easily be spread among the hosts of the entire network. Viruses like Trojan horse are extremely harmful to computers and other terminal devices, and can easily cause computer programs to fail to run normally, causing a large area of computer paralysis. At the same time, viruses like Trojan horse can destroy or steal data and bring great economic losses to users.

In recent years, ransomware virus has been widely spread through the Internet, and ransomware virus has achieved the purpose of extorting ransom by encrypting the victim’s files. Scientific research documents of university teachers and students (such as academic papers or graduation papers) are often the objects of encryption. Blackmailers generally require the payment of Bitcoin as the ransom to decrypt the files. The victimized teachers and students are often unable to pay the ransom because they do not have Bitcoin, or even if the ransom is paid, the hacker may not decrypt the files, resulting in loss of the files, which will cause caused great losses to teachers and students.

2.2. Security Threats from Information Leakage
In a smart campus environment, the personal information of college teachers and students exists in electronic forms on terminal devices or in cloud systems. This information includes basic personal information such as name, gender, age, ID number, etc., as well as personal private information such as address, call records, chat records, etc., as well as personal account, password information, and network behaviors. Due to the security issues of personal terminals or cloud systems, it is easy to cause the leakage of the information. Once the information is leaked, it is very easy to spread on the Internet, causing great harm to teachers and students, or causing property losses to their schools.

2.3. Security Threats from Information Systems
There are inevitably lots of information systems on smart campuses. Take Keyi College of Zhejiang Sci-Tech University as an example. The college has or is building operation systems such as personnel, educational affairs, academic work, books, finances, logistics, and assets. The college also has or is building systems such as online service hall, data center and website group since "come at most once" work is promoting in colleges and universities these years. Some of these systems are attacked because of network vulnerabilities, and some are because the systems themselves are vulnerable, so they can be easily attacked. Although some systems have no vulnerabilities, the systems' security arrangements are not strict, which makes the accounts easily stolen. For example, the passwords of the accounts are in plain text, or in some cases, passwords are too simple, or passwords are some specific characters, which renders the accounts easily stolen. For instance, the account numbers of college students are generally their student numbers. The student numbers are serially numbered according to fixed rules. Therefore, the student accounts are basically public information. Many original passwords are the last six digits of students' ID cards or the fixed six zeros. The result of this is that insiders can easily steal other people’s accounts. At the same time, it is easier for hackers to use these accounts to attack. Once this situation exists in the VPN system, the attacker logs into the VPN system, the internal network is completely exposed to the external network. Due to the lack of internal network security strategies, the attacker can easily attack the internal network through VPN.

3. Analysis of Security Protection Strategy

3.1. Strengthen the Construction and Implementation of the Safety System
The Cybersecurity Law of the People's Republic of China was officially implemented on June 1, 2017. GB/T 22239-2019 Information security technology—Baseline for classified protection of cyber security is the new standard of Information security technology — Baseline for classified protection of cyber security 2.0. The standard was formally implemented on December 1, 2019 [1]. This determined the laws, regulations and norms that must be followed for network security. In the process of promoting the construction of network information in colleges and universities, colleges and universities must establish a complete set of security protection system to ensure network information
security management based on this regulation and national standard [2]. At the same time, after the establishment of the system, the most important thing is to implement the system and act in accordance with the system, which is crucial. Statistics show that more than 70% of information security problems are caused by poor management, and 95% of these security problems can be avoided through scientific information security management systems [1].

3.2. Strengthen Basic Network Security Protection
The university network generally adopts the LAN with three layers of core layer, convergence layer and access layer. The network uses VLAN to achieve floor or service isolation. According to the characteristics of university networks, it is necessary to strengthen network security protection. First, a firewall at the network boundary should be established and firewall policies should be added to ensure the security of the network boundary. Secondly, ACL rules within the LAN and on the aggregation switch should be set to ensure that different VLAN virtual networks are isolated and secure. Finally, the establishment of different private networks is dispensable, such as security private networks, consumer private networks, and property private networks, to ensure absolute isolation between important business or departmental networks and campus networks.

3.3. Strengthen Security Protection of the Data Center
The data center is the core of a smart campus. Various application systems are deployed here. Strengthening the security protection of the data center is the key to protecting the security of the information system. In terms of the physical environment, the data center needs to implement a strict entry and exit management and registration system for personnel entry and operation. The computer rooms should be equipped with an environmental power monitoring system to monitor the temperature, humidity, air conditioning, UPS, access control, fire protection and water leakage detection and use SMS to give an alarm. In terms of information system protection, it is important to deploy webpage tamper-proofing systems, intranet firewalls, web application firewalls, and database audit systems to achieve comprehensive protection of school websites, applications and data. In operation and maintenance management areas, it is necessary to deploy bastion servers, log audits and vulnerability scanning systems to achieve centralized operation and maintenance management, operation and maintenance audit, log management analysis, vulnerability scanning, etc [3]. On the server terminals, it will be better to update the system patches in time, and install the online antivirus software and firewall software to ensure the security of the server terminals.

3.4. Strengthen Personal Terminal Security
Strengthening the security of personal terminals is mainly to strengthen the security protection of personal equipment such as computers. First of all, the security of the operating systems of the computers and other equipment must be ensured, and the operating system patches need to be updated in time to ensure that the systems are free of loopholes. Viruses like Trojan horse mainly work through vulnerabilities. They exploit vulnerabilities to attack the systems, destroying or stealing user data. By installing system update patches, vulnerabilities in the systems can be repaired and terminal security can be ensured. Secondly, anti-virus, anti-trojan horse and firewall software should be installed, and the software should be ensured to update to the latest version. Facts show that after the system is installed with anti-virus and other software, the probability of the host being infected or attacked is reduced to 5%, which can prevent more than 90% of virus attacks.

3.5. Strengthen Security Training and Improve Personal Network Security Awareness
When colleges and universities promote smart campus applications, they also need to conduct network security training. Colleges and universities should regularly carry out lectures, documentaries and other special network security education activities for all teachers and students, in order to remind teachers and students to recognize the shortcomings of the network, recognize the importance of campus information network security, and help teachers and students establish a concept of network
security. Through WeChat, QQ and other commonly used media by teachers and students, they can regularly push network security knowledge to teachers and students, prompting network security risks and countermeasures, improving users’ awareness of network security, and avoiding various network security problems caused by teachers and students themselves [4].

For individuals, the most important thing is to raise awareness of network security. Teachers and students should set more complex passwords for all of their accounts and change them regularly. At the same time, don't store personal privacy and confidential information easily on terminal devices or in the cloud. Teachers and students should strengthen the protection of important data and ensure multiple local and remote backups.

4. Conclusion
While the smart campus brings convenience, there are also many security threats. It is necessary to establish a comprehensive security protection system for network information from the aspects of management and technology. At the management level, it is necessary to do a good job in the establishment, implementation, and supervision of rules and regulations, improve information security awareness, and strengthen information security publicity and education; at the technical level, it is necessary to do a good job in security protection and monitoring of various terminals, networks and information systems, improve the level of security protection, and ensure the security of smart campus terminals, networks and information systems in colleges and universities [5-7].

References
[1] Wenquan Wang. Research on the security protection strategy of university information system [J]. Cyberspace Security, 11(11), pp.48-51, 2020.
[2] Leilei Dai. On the information security and protection strategy of computer network in colleges [J], 33, pp.70-71, 2020.
[3] Lizhi Zhou, Shangming Zhu. Practice and thinking on the construction of university network information security system [J]. Journal of Shenzhen University (Science and Engineering), 37(S1), pp.73-77, 2020.
[4] Xiufang Zhou. Analysis of network security issues in the construction of smart campus in universities [J]. Information Recording Materials, 21(03), pp.150-151, 2020.
[5] Youhui Tian. Research on network Information Security Governance of smart Campus against the background of education Informatization 2.0 [J]. Information Technology and Informatization, 10, pp.184-187, 2020.
[6] Chen Gong. Research on the Coupling of Industrial Structure and Environment between China and the “Belt and Road” Countries- Take the 10 ASEAN countries as an example. International Journal of Frontiers in Sociology (2019), Vol. 1, Issue 1: 89-98.
[7] Zhenjie Sun. A Study on the Educational Use of Statistical Package for the Social Sciences. International Journal of Frontiers in Engineering Technology (2019), Vol. 1, Issue 1: 20-29.