ISSN 2616-7433 Vol. 5, Issue 7: 20-25, DOI: 10.25236/FSST.2023.050704

Cybersecurity Challenges and Prevention Strategies in the Construction of Smart Campuses in Higher Education Institutions

Yanhong Guo*, Jian Sun, Shibo Xu, Yongzhi Yang

Space Engineering University, Beijing, China
1148803417@qq.com
**Corresponding author*

Abstract: *With the continuous development of information technology, smart campuses have become an important direction for the informatization construction of higher education institutions. However, the cybersecurity issues in the construction of smart campuses cannot be ignored, and cybersecurity challenges have emerged accordingly. This paper analyzes the current situation and challenges of cybersecurity in smart campuses of higher education institutions, proposes prevention strategies such as improving cybersecurity policies and regulations, strengthening the construction and application of cybersecurity infrastructure and technology, enhancing cybersecurity awareness and capabilities, optimizing cybersecurity management and monitoring, and conducts case analysis and inspiration on the practice of cybersecurity prevention strategies in smart campuses of higher education institutions at home and abroad. The aim of this paper is to provide cybersecurity protection and reference for the construction of smart campuses in higher education institutions.*

Keywords: *Smart Campus; Cybersecurity; Challenges; Prevention Strategies; Practice*

1. Introduction

1.1. Concept and Background of Smart Campus

A smart campus is a platform that utilizes information technology to build intelligent, digital, convenient, efficient, and secure education management systems, to improve the efficiency of education management and the quality of services, and to promote the development of modern school management. The smart campus is one of the important directions for the informatization construction of higher education institutions, aiming to improve students' learning efficiency, promote the sharing and optimization of educational resources, construct an open, intelligent, efficient, and service-oriented school management model, and promote the reform and innovation of education and teaching[1].

1.2. The Importance of Smart Campus Construction in Higher Education Institutions

The construction of smart campuses in higher education institutions has significant strategic and practical significance. On the one hand, smart campus construction can improve the management efficiency of higher education institutions, reduce management costs, improve service quality, improve the school environment, and provide support for the long-term development of higher education institutions; on the other hand, smart campus construction is also an important manifestation of the combination of information technology and education and teaching, which can promote the reform and innovation of higher education institutions' education and teaching, promote the transformation and upgrading of higher education institutions, and enhance the core competitiveness of higher education institutions.

The issue of cybersecurity in the construction of smart campuses is becoming increasingly prominent, posing significant challenges to the informatization construction of higher education institutions. In a smart campus, a large amount of information is involved, covering a wide range of areas including teaching, scientific research, and administrative management. The confidentiality, integrity, and availability of data all face severe challenges. Once cybersecurity issues occur, they may lead to interruptions or severe impacts on the teaching, scientific research, and management of higher education institutions, bring adverse effects to the production and life of students and faculty, and

ISSN 2616-7433 Vol. 5, Issue 7: 20-25, DOI: 10.25236/FSST.2023.050704

damage the reputation and image of higher education institutions. Therefore, how to solve the cybersecurity problems in the construction of smart campuses in higher education institutions and ensure the information security of higher education institutions has become an important issue in the construction of smart campuses.

2. Current Situation and Challenges of Cybersecurity in Smart Campuses of Higher Education Institutions

2.1. Analysis of the Current Situation of Cybersecurity in Smart Campuses of Higher Education Institutions

(1) Weak cybersecurity awareness. Some students and faculty members lack sufficient understanding of the importance of cybersecurity and lack a full understanding and awareness of cybersecurity issues.

(2) Insufficient network infrastructure construction. The network infrastructure construction of smart campuses in higher education institutions is relatively lagging, with incomplete cybersecurity protection measures and a lack of comprehensive protection mechanisms and technical means.

(3) Non-standard network security management. There are some non-standard phenomena in the network security management of smart campuses in higher education institutions, such as the lack of specialized network security management agencies, effective network security monitoring and early warning mechanisms, and low cybersecurity awareness leading to a failure to adopt proactive security measures.

(4) Diversification of network attack methods. The network attack methods faced by smart campuses in higher education institutions are becoming more diversified, including various forms such as phishing emails, network viruses, and hacker attacks, increasing security risks and threats.

2.2. Cybersecurity Challenges in Smart Campuses of Higher Education Institutions

With the development of informatization construction in higher education institutions, smart campuses have become an important part of the informatization construction of higher education institutions. Smart campuses not only provide convenient campus services but also provide a more convenient learning and working environment for students and faculty. However, with the development of smart campuses, cybersecurity issues are becoming increasingly prominent, and cybersecurity challenges in smart campuses of higher education institutions have emerged.

2.2.1. Increased security risks of big data

Smart campuses have large amounts of data and various types of data, such as students' personal information, teaching performance, examination information, student status management, etc.[2]. The security of this data is directly related to the operation and management of the school. If it is attacked by hackers or information is leaked, it will cause great losses. Therefore, higher education institutions need to strengthen the protection and management of data, establish a sound data security management system, and strictly control the security of data collection, storage, transmission, and processing.

2.2.2. Security vulnerabilities in mobile devices and personal computers

Students and faculty members use mobile devices, personal computers, and other devices to access the smart campus network. The security of these devices varies, and there are security vulnerabilities and risks. For example, some devices have not installed the latest security patches, and some devices have weak passwords, which are easily exploited by hackers. Therefore, higher education institutions need to strengthen device management, provide secure access methods, such as virtual private networks (VPNs), and strengthen supervision and management of devices.

2.2.3. Uneven levels of technical support and security protection

The information technology support and security protection levels of smart campus systems in higher education institutions vary, with various vulnerabilities and weaknesses. Some schools' technical personnel lack professional knowledge and have difficulty dealing with complex network security issues; some schools have not updated and upgraded their systems in time, resulting in various vulnerabilities and weaknesses. Therefore, higher education institutions need to strengthen technical support and security protection capabilities, provide timely security patches and upgrade services,

ISSN 2616-7433 Vol. 5, Issue 7: 20-25, DOI: 10.25236/FSST.2023.050704

conduct regular security assessments and vulnerability scanning, and promptly discover and repair security vulnerabilities.

2.2.4. Increasing security threats

With the continuous increase of security threats such as hacker attacks and network viruses, the cybersecurity of smart campuses faces significant challenges. Hackers can obtain students' and faculty members' personal information through various means, leading to identity theft, phishing, fraud, and other activities, which pose serious threats to the property and privacy of students and faculty members. In addition, network viruses and malware can also spread through smart campus networks, causing huge losses to schools. In 2017, a ransomware virus exploited vulnerabilities in Microsoft systems and spread widely across campus networks in many universities nationwide. Infected computers' data would be destroyed quickly if users did not pay the ransom. Therefore, higher education institutions need to establish a comprehensive network security protection system, including strengthening intrusion detection and prevention measures, regularly backing up data, and conducting cybersecurity training to comprehensively improve the security and stability of smart campus networks.

3. Strategies for Cybersecurity Prevention in Smart Campuses of Higher Education Institutions

3.1. Improve cybersecurity policies and regulations

Higher education institutions should establish a cybersecurity responsibility system, clarify the responsibilities and tasks of cybersecurity management, and define the responsibilities of management personnel and relevant staff at all levels in cybersecurity management. They should implement responsibilities for cybersecurity work at the individual level.

Develop cybersecurity management processes and norms, standardize cybersecurity management and operations, clarify various aspects and processes of cybersecurity management, establish standardized cybersecurity management models and processes, and ensure that cybersecurity management follows established rules.

Establish emergency plans for cybersecurity incidents, develop disposal processes and standards for cybersecurity incidents, formulate response strategies and contingency plans for cybersecurity incidents, and ensure that cybersecurity incidents are promptly and effectively addressed and resolved.

Strengthen cybersecurity supervision and inspection, establish a sound cybersecurity supervision and inspection mechanism, strengthen supervision and inspection of cybersecurity management, promptly discover and correct cybersecurity problems, and ensure the security of smart campus networks in higher education institutions.

Strengthen the cybersecurity audit work for smart campus networks. Develop corresponding audit mechanisms for network security, database security, network logs, and operation security. Strengthen the smart campus network audit management and improve the cybersecurity of smart campus networks in higher education institutions.

In summary, developing comprehensive cybersecurity policies and regulations is the foundation and prerequisite for smart campus network security. Only by establishing a sound cybersecurity management system and mechanism can a strong guarantee be provided for the network security of smart campuses in higher education institutions.

3.2. Strengthen the construction of cybersecurity infrastructure and technology applications

With the rapid development of the internet and information technology, higher education institutions face increasing cybersecurity threats. Strengthening the construction of cybersecurity infrastructure and technology applications is a necessary means to ensure the safe construction and operation of higher education institutions' informatization.

Higher education institutions should increase investment, establish a complete cybersecurity defense equipment system, including firewalls, intrusion detection systems, anti-virus systems, VPNs, secure isolation gateways, etc., to ensure the safe operation of campus networks. In addition, they should also pay attention to the upgrading of equipment to keep up with the development of new technologies and threats.

Higher education institutions should establish cybersecurity incident monitoring and early warning

ISSN 2616-7433 Vol. 5, Issue 7: 20-25, DOI: 10.25236/FSST.2023.050704

systems to promptly detect and respond to cybersecurity incidents. These systems can monitor and analyze network traffic, security logs, abnormal behaviors, etc., in real-time, issue quick alarms in case of abnormal situations, and take corresponding measures to avoid or minimize losses.

Higher education institutions should strengthen research and application of cybersecurity technology, carry out targeted research, and provide a scientific basis and technical support for the cybersecurity defense of higher education institutions. For example, research on the analysis and response to new threats, strengthen cryptography, security protocols, network security testing, and other aspects, develop new security technologies and products, and improve the ability of network security defense in higher education institutions.

3.3. Enhancing Cybersecurity Awareness and Abilities

Cybersecurity has become a significant social issue, especially in large organizations like universities, where the importance of network security is undeniable. To improve students' and faculty members' cybersecurity awareness and abilities, universities can take the following measures:

Organize cybersecurity promotion and education activities: Universities can regularly hold events such as cybersecurity knowledge competitions, themed lectures, promotional posters, and cybersecurity drills to enhance students' and staff members' cybersecurity awareness [3].

Include cybersecurity-related knowledge in courses: Universities can add cybersecurity content to their curricula and publish educational articles and videos on their websites, official accounts, and other channels, allowing students and staff to learn and improve their cybersecurity knowledge independently [4].

Strengthen cybersecurity protection measures: Universities can enhance network security monitoring, install firewalls, and encrypt data transmission to ensure students' and staff members' network security.

In summary, universities need to prioritize cybersecurity education efforts and raise the awareness and abilities of students and staff to ensure the security of university networks and information systems.

3.4. Optimizing Cybersecurity Management and Monitoring

To ensure the security of university networks, it is essential to establish a comprehensive cybersecurity management system, strengthen network security inspections and monitoring, promptly detect and address cybersecurity issues, and improve the effectiveness of cybersecurity prevention.

Establish a comprehensive cybersecurity management system: Universities need to create a complete cybersecurity management system, including policies, rules and regulations, and an organizational structure for security management. Additionally, they must clarify cybersecurity responsibilities and authorities and establish roles and responsibilities for cybersecurity management personnel to ensure orderly network security management.

Regularly conduct network security inspections and monitoring: Universities should carry out routine network security inspections and monitoring to detect and address cybersecurity issues promptly. They can use methods like regular vulnerability scanning, intrusion detection, and traffic monitoring to identify network security threats and anomalies. Furthermore, they should establish daily security audit mechanisms to trace and analyze network security events and prevent similar incidents from occurring in the future.

Establish a robust cybersecurity incident response mechanism: Universities should develop detailed emergency response plans and clearly define the process and responsibilities for handling cybersecurity incidents. When a cybersecurity event occurs, they must act swiftly to contain the situation and prevent further damage [5]. Additionally, they should regularly organize cybersecurity drills to improve their emergency response capabilities.

ISSN 2616-7433 Vol. 5, Issue 7: 20-25, DOI: 10.25236/FSST.2023.050704

4. Practical Application and Case Analysis of Cybersecurity Prevention Strategies for Smart Campus Networks in Universities

4.1. Cybersecurity Prevention Practices in Smart Campus Networks at Domestic and International Universities

Several universities around the world have already begun to actively implement cybersecurity prevention strategies in their smart campus construction. For example, Harvard University focuses on strengthening network security protection and monitoring in its smart campus construction and adopts advanced cybersecurity technologies for prevention. The University of California, Los Angeles, has established the UCLA401 security policy, which outlines cybersecurity protection strategies, such as installing antivirus software on all computers and setting strong passwords to enhance campus network security.

In China, Peking University has adopted a variety of cybersecurity prevention measures, such as constructing a network security defense system based on a combination of human, technical, and physical defenses, implementing a cybersecurity responsibility system, strengthening cybersecurity training, and establishing emergency response plans for network security. These measures have effectively ensured the security of the university's network.

4.2. Case Analysis and Inspiration

Taking Zhejiang University of Technology as an example, the university has achieved security for its smart campus network through various means such as establishing a network security management center, using advanced network firewalls, adopting network behavior management systems, and conducting cybersecurity education and publicity. In 2018, the construction of a cybersecurity emergency response center laid a solid foundation for smart campus network security. Through this open vulnerability information platform, anyone can submit potential or confirmed security vulnerabilities. To make the most of this platform, the university's information office has developed corresponding emergency response procedures, offered online cybersecurity courses, and promoted cybersecurity awareness, thus raising the level of understanding and importance of cybersecurity among teachers and students. At the same time, Zhejiang University of Technology has established a network security management committee and formulated the "Zhejiang University of Technology Network Security Management Regulations," which clearly define the various responsibilities and tasks of network security management.

In addition, the network security protection of the campus network at Xidian University in Xi'an is also typical. Xidian University classifies and manages important and sensitive data in the campus network, strengthens the management of internal high-privilege users, and implements fine-grained audit management for databases. Through these measures, the university has strengthened internal control over campus network database assets and improved the security of the campus network database.

These successful cases demonstrate that the cybersecurity prevention of smart campuses in universities requires the comprehensive application of various means, including technical, managerial, and legal measures. At the same time, cybersecurity prevention requires the participation of all members, including students, teachers, and administrators, who need to actively participate in cybersecurity prevention and improve their cybersecurity awareness and skills.

5. Conclusion

The issue of cybersecurity in the construction of smart campuses in universities cannot be ignored. Universities need to strengthen their cybersecurity awareness, establish a sound cybersecurity management system, adopt various cybersecurity prevention strategies, and continuously improve their cybersecurity prevention capabilities and levels. At the same time, universities need to strengthen the cultivation of cybersecurity talent and technology research and development to gradually achieve the sustainable development of cybersecurity in smart campuses.

ISSN 2616-7433 Vol. 5, Issue 7: 20-25, DOI: 10.25236/FSST.2023.050704

References

[1] Li Yadong. Exploration and analysis of the construction and application of smart campuses in universities in the "Internet+" era [J]. TV Technology, 2020, 44(1):2-5.
[2] Chen Jian, Zhang Zhihua, Wu Yisheng, et al. Application of big data technology in the construction of smart campuses in universities [J]. Microcomputer Applications, 2021, 37(7):4-9.
[3] Liang Suxiang, Yang Lihong. On the cultivation of college students' network security awareness [J]. Educational Research, 2020, 3(11):9-10.
[4] Liu Qingying. Building a "firewall" for network ideological security in colleges and universities [J]. Jiangsu Higher Education, 2019(9):4-8.
[5] Zheng Shebin. Emergency response to network information security incidents in private colleges [J]. Information Network Security, 2020(2):4-7.