ISSN 2663-8169 Vol. 5, Issue 21: 88-92, DOI: 10.25236/IJNDE.2023.052116

Design and Implementation of Computer Information Security Management System in Colleges and Universities

Lin Shan

Sichuan Vocational College of Chemical Industry, Luzhou, Sichuan, 646300, China

Abstract: *Entering a new era, in order to ensure that universities can effectively respond to information security challenges in the digital age, protect sensitive data and information assets, and provide reliable support and guarantees for education, research, and administrative work, universities need to continuously strengthen information security awareness, take practical and feasible measures, actively establish a sound information security management system, in order to cope with future information security challenges and ensure that university information security is fully protected.*

Keywords: *Colleges and universities; Information security; Management system; Design approach*

1. Introduction

The construction of the university computer information security management system in our country is an indispensable part to ensure the sustainable development of the digital campus. With the increasing importance of information security, the effectiveness of university information security management system has become the focus of attention. Imperfect security and confidentiality work may lead to potential problems and loopholes, and then endanger the confidentiality of university information resources. Therefore, it is very important to explore and improve the university computer information security management system.

2. The importance of university computer information security management

The importance of computer information security management in colleges and universities cannot be underestimated. In today's digital era, computer systems and networks in colleges and universities have become the core infrastructure for academic research, education management, student services and administrative operations. Therefore, ensuring the security of these key information assets is essential for the stable operation and reputation maintenance of colleges and universities. Colleges and universities have a large amount of sensitive data, including personal information of students, faculty and staff, academic research results, financial data, etc. The leakage or use of these data by criminals will seriously damage the privacy of individuals and the reputation of the university, which may lead to legal proceedings and financial losses. University information security is subject to the continuous evolution of external threats, including network attacks, malware dissemination, social engineering, etc., which may lead to system disruption, data loss, and even pose a threat to the normal operation of the university[1]. The exposure of information security vulnerabilities in colleges and universities may also damage the reputation of the university, reduce the trust of students and faculty members, and have long-term adverse effects on enrollment, donation, and other aspects. In addition, the management system of information security in colleges and universities is not only related to the internal university, but also to national security. Universities undertake important tasks of scientific research and technological innovation, and many research results are of national defense and national strategic significance. If these research results are stolen or destroyed, it will pose a direct threat to national security.

3. The information security challenges faced by universities in the current stage

3.1 The threat of data leakage

Among the information security challenges faced by universities at the current stage, the threat of

ISSN 2663-8169 Vol. 5, Issue 21: 88-92, DOI: 10.25236/IJNDE.2023.052116

data leakage is undoubtedly one of the most prominent and urgent problems. Universities store a large amount of sensitive information, including personal identity data, academic research results, financial data, etc. The leakage of these data may lead to the leakage of individual privacy and the breeding of illegal activities, and then damage the reputation and credibility of the university. In addition, academic achievements and research data of universities are also valuable intellectual assets. Leakage of such data may lead to academic misconduct, damage to the interests of research teams, and even endanger national security. In terms of financial data, universities manage a large amount of important information related to tuition, donations and funds. Once leaked, it will lead to serious economic losses and affect the normal operation of the university. In a word, the threat of data leakage is not only a problem of information security for universities, but also related to individual privacy, academic reputation, economic interests and national security. Therefore, taking comprehensive information security measures to strengthen data protection has become an important challenge for university management to solve.

3.2 The increase in cyber attacks

One of the current information security challenges facing universities is the surge of network attacks. Network attacks are no longer an occasional event, but a continuous and refined threat, posing a serious threat to university computer systems and sensitive information. These network attacks are diverse, including distributed denial of service (DDoS) attacks, malware, ransomware, social engineering, and so on. The motives of the attackers are also different, some are hackers seeking to make a profit, some may be competitors or political activists, and some may be state-sponsored attacks[2]. The diversity of attack methods and the variability of attackers make the information security of colleges and universities face great challenges. These cyber attacks may lead to the disruption of the school system, the theft of data, the destruction of academic research, and even the serious impact on the personal privacy of teachers, students and employees. In addition, once a university is attacked by a network, it will cause damage to the reputation of the university, which may lead to legal proceedings and economic losses.

3.3 The spread of malware

The threat of malware is increasing day by day, and it has evolved into a broad and covert attack method, which poses a great risk to university computer systems and sensitive information. Malware includes viruses, worms, Trojan horses, and ransomware, which can enter university networks through email, insecure downloads, malicious links, or USB devices. Once malware is inside a system, its harms can be many: They can steal sensitive data, disrupt system functions, encrypt files and demand ransom, or even be used to control infected computers to become part of a "botnet" for larger cyberattacks, threatening not only the normal operation of universities, but also the loss of academic research data and the disclosure of personal privacy of teachers and students. The spread of malware presents an ever-evolving trend, with attackers adopting increasingly sophisticated and covert methods that are difficult to detect and remove in time by traditional defense tools.

4. Analysis of information security management technology in universities

4.1 Network firewall technology

Table 1: Characteristics of packet filtering and application agents

Types	Data flow control mode	Processing power	Level of security
Packet filtering method	Each packet is detected and the transmission is controlled according to the filtering rules	About hundreds of thousands to millions of packets per second	Basic security, suitable for large-scale traffic scenarios
Application proxy approach	Intercept and inspect application layer data through proxy servers	Packets processed per second can range from hundreds of thousands to thousands	Advanced security, but slower processing

As an effective network security technology, the network firewall can control and filter the data flow in and out of the network according to the pre-set security policy. It not only has powerful protection function, but also has high security performance. Network firewall technology mainly uses packet filtering and application proxy to control data flow, and their characteristics are shown in the following

ISSN 2663-8169 Vol. 5, Issue 21: 88-92, DOI: 10.25236/IJNDE.2023.052116

table. According to different security requirements, different types of network firewalls can be selected. For example, stateful detection firewalls can effectively prevent IP address spoofing and DoS attacks, while stateless detection firewalls can better prevent complex protocol attacks[3]. In addition, the deep detection firewall can perform double detection at the network level and the application level to improve the detection ability of unknown attacks. In practice, it is also necessary to combine other security technologies, such as intrusion detection system (IDS), intrusion prevention system (IPS), virtual private network (VPN), etc., to build a multi-level and multi-means security protection system to achieve comprehensive protection of information security in colleges and universities, as shown in Table 1.

4.2 Intrusion detection technology

Intrusion detection technology is an important part of information security management technology in colleges and universities, which is mainly used to detect and identify unauthorized network access and system intrusion. This technology monitors network traffic and system status in real time by setting sensors at key locations, and conducts in-depth analysis of the collected data to find abnormal behavior or potential attacks. Intrusion detection techniques are mainly divided into two categories: misuse-based detection and anomaly-based detection. Misusage-based detection detects intrusions through known attack patterns and known security events. This method has high accuracy, but it needs to constantly update the detection mode to cope with new attack methods. Anomaly-based detection detects deviations from the normal behavior of a system or network by establishing the normal behavior pattern. This method can detect unknown attack methods, but the false alarm rate is high. In practice, intrusion detection technology needs to be combined with other security technologies such as firewall technology and intrusion prevention system to form a multi-level security protection system. At the same time, it is also necessary to respond to and dispose the detected intrusion behaviors in time to minimize the security loss.

4.3 Encrypted communication technologies

Encrypted communication technology is one of the key technologies in the university computer information security management system. It can ensure the confidentiality and integrity of data in the transmission process. This technology uses cryptography methods to encrypt the transmitted data, so that unauthorized users cannot get the real data. In practice, encrypted communication technology mainly includes symmetric encryption and public key encryption. Among them, symmetric encryption uses the same key for encryption and decryption, which has high encryption strength and efficiency, but it needs to transmit the key between the two communication parties, and there are certain security risks. Public key encryption uses different keys for encryption and decryption, which can better protect the security of the key, but the encryption and decryption speed is slow. In practice, different encryption algorithms and protocols can be selected according to specific application scenarios and security requirements. For example, SSL/TLS protocol is a commonly used encrypted communication protocol, which can provide high strength data encryption and integrity protection, and is widely used for communication between Web browsers and servers. In addition, RSA algorithm is an asymmetric encryption algorithm, which can achieve efficient encryption and decryption operations, and is suitable for encrypted transmission of large amounts of data.

5. Design and implementation of information security management system in colleges and universities

5.1 Clear design objectives and principles

The design of university information security management system mainly lies in the establishment of clear design goals and principles, this process is the cornerstone of the whole system construction. First, the protection of sensitive information, including personal data, academic research results and financial information, must be ensured to ensure its integrity, availability and confidentiality. Second, it is essential to maintain continuity and availability to prevent the impact of cyber attacks and hardware failures on the information systems of colleges and universities, and to establish data backup and recovery mechanisms. In addition, the establishment of a security culture of full participation is also one of the goals, through the development of clear security policies and procedures, regular training and simulation exercises, to improve the information security awareness of staff and students. In addition, the management system should be flexible and adaptable, capable of upgrading and adjusting as information

ISSN 2663-8169 Vol. 5, Issue 21: 88-92, DOI: 10.25236/IJNDE.2023.052116

security threats and technological trends evolve. Finally, continuous improvement is key, and universities need to establish mechanisms for regular review and evaluation to ensure the effectiveness of the management system, and to continuously improve and update policies, procedures and technical measures based on the evaluation results. By adhering to these principles, colleges and universities can better design and implement information security management systems to cope with changing information security challenges, protect sensitive information, maintain reputation, and ensure continuous operations[4].

5.2 Build the organizational structure of security management

In the construction of university information security management system, the establishment of a sound security management organization structure is very important, this organization structure should reflect the clear responsibilities and division of labor, in order to effectively promote the information security management work. Colleges and universities should set up an information security committee, composed of senior leaders and information security experts, responsible for formulating information security strategies and policies, as well as overseeing the implementation of the entire security management system. The committee needs to regularly review the latest trends and threats in information security to make corresponding decisions and adjustments. The Information Security Office (ISO) is the key organizational unit that is responsible for the actual management of information security. The ISO should have enough technical experts, including cybersecurity analysts, data protection experts, and security engineers. Based on technical data, colleges and universities need to ensure that the ISO has sufficient technical resources to monitor and analyze network traffic, detect and respond to potential threats, and ensure that vulnerabilities in the system are fixed. In addition, a close collaboration mechanism needs to be established between the information Security Committee and the ISO to ensure that information security policies are in line with actual operations. Monitoring and reporting of technical data will play a key role in this process, with the Information Security Committee relying on data provided by ISO to assess the security situation and formulate policies accordingly. Universities will also need to have information security contacts within each faculty and department, who will serve as branches of information security management to assist ISO in promoting information security awareness at all levels. These contacts can assist in educating staff and students, dealing with information security incidents, and communicating information security policies and guidelines[5].

5.3 Intrusion detection system design

The design and implementation of intrusion detection system (IDS) is the key step of information security in colleges and universities. First of all, it is necessary to clarify the goal and scope of IDS, determine the monitoring network and system according to professional data analysis, and consider the scale of data traffic handled by the university network every day. Secondly, select the type of IDS suitable for the university network environment, and decide whether signature-based IDS or behavior-based IDS is more appropriate based on detailed data analysis, including network traffic characteristics and attack history. Next, the best sensor location is determined based on professional data analysis in order to comprehensively monitor the network. Subsequently, rules and policies are tailored to identify potential intrusions, which should be tailored based on known attack patterns, network protocols, and characteristics of the university network. Finally, IDS is implemented and tested, including the deployment of IDS sensors, the configuration of rules and policies, and the establishment of alarm and response mechanisms, while monitoring the performance of IDS and continuously adjusting and improving according to the results of data analysis. Through these steps, colleges and universities can establish an effective intrusion behavior detection system, and use professional data analysis to continuously improve the performance of the system to ensure the information security of colleges and universities.

5.4 The design of data backup/off-site disaster recovery

First, the importance and sensitivity of critical data are clearly defined through professional data analysis to develop an appropriate backup strategy, considering that the amount of data generated can reach hundreds of gigabytes per day, and backup frequency and storage capacity need to be determined. Secondly, choose the appropriate backup technology, professional data analysis can help to choose local backup or cloud backup, and determine the full backup or incremental backup, etc. At the same time, it is necessary to ensure that the backup system can copy the data in a timely and complete way, and verify the effectiveness of the backup through regular data recovery tests. Secondly, the off-site disaster

ISSN 2663-8169 Vol. 5, Issue 21: 88-92, DOI: 10.25236/IJNDE.2023.052116

recovery plan is designed, and the remote storage location of the backup data is determined under the guidance of professional data analysis to ensure the security and availability of the data in the event of a disaster, such as backing up to a geographically distant data center. Finally, monitoring and automation are implemented to guide the development of monitoring strategies through professional data analysis to ensure the normal operation of backup and disaster recovery systems. At the same time, the automation process can optimize the efficiency of backup and disaster recovery based on data analysis, such as adjusting the backup policy according to the importance and change frequency of backup data. In summary, the design of data backup and off-site disaster recovery needs to fully rely on professional data analysis to ensure the integrity and availability of the university's information security management system, especially to effectively protect critical data in the face of potential risks and disasters.

6. Conclusion

Information security has become the top priority of university management and will continue to face new challenges and threats in the future. Therefore, the construction of university information security management system is not only an urgent need, but also a continuous evolution of the task. We must deeply realize the urgency and complexity of information security management, take proactive measures to continuously improve security awareness, update technical means, and strengthen organizational cooperation. Universities need to deal with information security problems in a multi-level and multi-dimensional way, including the comprehensive use of network firewall technology, intrusion detection system, data backup and off-site disaster recovery.

References

[1] Wu Jinhong. Countermeasures of University information security management under the background of big data [J]. Digital Communications World, 2022(08):101-103.
[2] Du Kai. Analysis of information security problems and countermeasures based on the background of smart Campus [J]. Computer Knowledge and Technology, 2012, 18(21):26-27.
[3] Zhao Hongwei, Wang Xiwen, Du Xiaogang. Innovation of unified strategy information security management methods in universities in the datalization era [J]. Public Standardization, 2022(18):133-135. (In Chinese)
[4] Li Qi. Analysis of information security problems and countermeasures in colleges and universities under the environment of modern information technology [J]. Network Security Technology and Application, 2020(12):106-107.
[5] Liang Yan, Li Yating. Information Security and protection strategy of University Computer Network [J]. Electronic Technology and Software Engineering, 2021(12):255-256.