Research on Information Security Management Strategies in Universities from the Perspective of Level Protection 2.0

Yuhui Wu*

Anshun University, Anshun, Guizhou province, 561000, China

*Corresponding author: wuyuhuide2009@qq.com

Abstract. The Network Security Level Protection System 2.0 standard puts forward higher requirements for information security construction. Through research on the information security construction of some universities in Gz Province, it was found that there are difficulties in implementing the new standards. Based on the analysis of the new standard of Level Protection 2.0, this paper summarizes the ideas of network security management in local colleges and universities from the perspective of classification and hierarchical management, and proposes targeted network security management strategies, providing a certain reference for promoting the construction of network security in local colleges and universities.

Keywords: Level protection system; Network security; Campus network

1 Introduction

The implementation of the Action Plan for Education Informatization 2.0 signifies that China's education informatization construction has entered a new era of 2.0[1]. However, China's cybersecurity issues are prominent[2], and cybersecurity has become the main obstacle to educational information. The construction of national network security systems provides legal protection and action guidelines for the construction of network security in universities. Implementing the 2.0 standard of network security and other guarantees to build a network security guarantee system for universities has become an important aspect of measuring and evaluating the level of network security construction in universities. However, to meet the new requirements of network security and other security 2.0, universities need to invest a large amount of professional technical strength and funds. Therefore, in universities with limited available resources, especially local universities, it is particularly important to adopt network security management strategies. By researching the current situation of network security construction in local colleges and universities in GZ Province, and based on the relevant theories of information security management, this study aims to study suitable network security management strategies, providing a reference for promoting information security construction in local colleges and universities.

Y. Kuang et al. (eds.), *Proceedings of the 2024 5th International Conference on Education, Knowledge and Information Management (ICEKIM 2024)*, Atlantis Highlights in Computer Sciences 22,
https://doi.org/10.2991/978-94-6463-502-7_112

2 New Standard for Information Security

2.1 The Formation and Characteristics of New National Standards

The Network Security Level Protection System 2.0 includes the Basic Requirements for Network Security Level Protection (GB/T22239-2019), the Technical Requirements for Security Design of Network Security Level Protection (GB/T25070-2019), and the Evaluation Requirements for Network Security Level Protection (GB/T28448-2019)[3]. The new standard refers to a security assessment standard in China's national information security level protection system. This standard is widely used to evaluate the security of information systems and meet the requirements of relevant laws and regulations to ensure the confidentiality, integrity, availability, and controllability of information systems. This standard, specific evaluation indicators include: network and terminal security, server and storage security, data security, application system security, key management security, security operation and maintenance management, security event and emergency management, personnel security management, etc.

2.2 New Standard Architecture

From the perspective of the steps for building key information infrastructure, the new standard divides the construction process into five stages: project approval, design, deployment, operation and maintenance, and abandonment, as Figure 1. The most critical stages include grading and filing, grading evaluation, and security construction rectification[3-4].

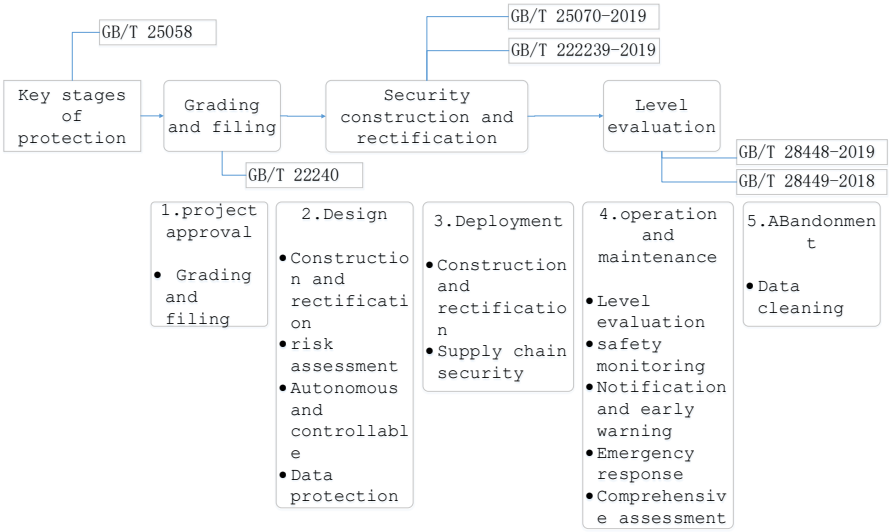

Fig. 1. The steps for building key information infrastructure according to the new standard

Classification is the primary step in level protection, which refers to determining the boundaries of information systems and determining the level of information systems or networks based on their importance and the degree of harm caused by damage. Filing is the core of level protection, which means that information systems or networks designated as second level or above must go through filing procedures with public security organs. Level evaluation is a method of evaluating the security protection status, which refers to the activities of evaluation institutions to detect and evaluate the security protection status of non-state secret information systems under relevant management norms and technical standards. The rectification of security construction is the key to the implementation of level protection work, which refers to the implementation of information system security responsibilities under national standards, the construction of information system security management systems and technology, and further improvement of protection measures for classified objects.

3 The Analysis of the Current Situation of Information Security in Local Colleges

3.1 Explanation of Investigation Situation

GZ Province has 72 higher education institutions. Select 2 general local undergraduate colleges, 4 local vocational colleges, 1 independent college, and 1 private university, totaling 8 local colleges as the survey subjects. Conduct research from five aspects: funding investment, campus network infrastructure construction, information security management personnel, application information system construction, and the operation of information security management systems.

3.2 Current Situation of Information Security Construction in Local Colleges and Universities

1. In terms of information security management. Most local colleges and universities lack sufficient awareness of the importance of information security. Surveys have shown that there is a general lack of efficient information security organizational leadership structures, sound information security management systems, unclear information security management responsibilities, limited methods for carrying out information security work, a lack of effective information security protection systems, failure to respond to information security incidents promptly, leakage of privacy information of teachers and students, frequent website vulnerabilities, password leaks, and other problems, and often inadequate information rectification work.

2. In terms of network security construction. The survey shows that the construction of educational informatization application information systems in most local colleges and universities is limited in quantity, the construction content is not rich, the construction levels are not clear, the degree of data sharing between existing application information systems is low, and they have not effectively supported scientific decision-making in school education and teaching. The overall level of information

application is not high. Due to the limited level of local economic development, the investment in higher education information funds in various regions is not high. The level of educational information in local colleges and universities is still relatively low. Most universities are limited to building application information systems such as school websites, teaching management systems, and document transmission to ensure the normal operation of the school. Businesses related to information security, such as campus communication networks, network storage space, and teacher information management, rely on third parties. The construction of network security infrastructure is still weak.

4 Information Security Management Strategies

The classification and grading management technology is commonly used in the top-level design of systems and has the advantage of clear thinking when applied to the construction of network security in universities[5]. At present, universities widely adopt the method of classified construction to develop application information systems and implement graded protection for the security of application information systems through regional and hierarchical technology. Therefore, classification technology is suitable for managing the network security of corresponding application information systems; The hierarchical management of network security is consistent with the national network security level protection 2.0 concept and meets the requirements of the new standards. This section studies the network security management strategies of local universities from the perspective of classification and grading.

4.1 Information Security Classification Management Strategy

Classified Management by Security Elements

The general requirement of the new standard is to divide network security elements into management elements and technical elements[6]. Technical management strategy is the key to managing technical elements. Adopting a full lifecycle security management strategy can effectively reduce the incidence of information security incidents. That is, all newly built application information systems (including website groups. Currently, most universities in GZ build their respective websites through website groups) must undergo security testing before they are officially launched. Only after meeting the predetermined requirements can they be approved for launch. Regular security vulnerability testing should be conducted after launch, and any discovered security vulnerabilities should be repaired promptly; According to the needs of network security, different levels of application information systems are divided into different areas, and security management platforms, IT operation, and maintenance monitoring, firewalls (web application firewalls), IPS, fortress hosts, VPNs, antivirus software, etc. are used to achieve security protection for school network zoning; Using a combination of automatic technology backup and regular manual backup to perform disaster recovery backup on important data.

The technology platform is the core of technology element management and a technical means to meet the requirements of new standards for "manageable" access. There are three common public technology platforms: website group platform, website shared space, and virtual host. Classify the school homepage website, the websites of each secondary college, and the application information system according to the type of application information system and the degree of impact on the public. Configure protection parameters according to their respective protection areas, and implement a "classification, classification, and separation" platform operation and management model; For websites that do not use the school's public platform, they will be uniformly published through reverse proxy to achieve unified management of the university's external websites.

Universities need to achieve controllable and auditable behavior of campus network users, which is a requirement of the Level Protection 2.0 standard[7]. In addition to deploying audit security products and improving the parameter configuration of network security equipment, they also need to strengthen the management of information security management elements. Functional departments and job responsibilities can be clearly defined from aspects such as network monitoring and public opinion analysis. Professional skills training for security management personnel can be strengthened, and campus information construction evaluations can be organized. The level of information security construction should be an important aspect of year-end performance evaluation.

Manage Attack Events According to Their Stages of Occurrence

According to the adaptive network security model, network security protection could be divided into three stages based on the temporal characteristics of network security events: pre-event, during the event, and post-event[8].

Information security pre-warning should fully collect and analyze network threat intelligence from various channels. Through comprehensive analysis of this intelligence, possible network security threats can be identified. Analyze the vulnerability of the school's network, evaluate security risks, and develop corresponding network emergency plans. Use the national information security vulnerability database, CVE, vulnerability detection platforms of education authorities, and relevant provincial and municipal security monitoring information sharing platforms to obtain intelligence on information security situations, and to adjust network configuration parameters in a targeted manner before network security incidents occur.

During the incident phase, capture network security incidents, respond promptly, and minimize the harm of the incidents. The difficulty lies in making timely and effective responses to security incidents. Therefore, local universities need to organize technical forces to study possible network security incidents, develop contingency plans, strengthen coordination and cooperation, and form a working force. Considering the construction cost, local universities can explore establishing a linkage response mechanism with the public security network supervision department, government public opinion analysis department, education regulatory department's network security management department, and related enterprises. Multiple units can jointly use the same linkage work mechanism to share the construction cost of the linkage mechanism.

In the post-event stage, identify the root cause of the event and completely eradicate it. Not only should we avoid the school network from being attacked again, but we also need to restore all compromised systems or network devices to their normal tasks, learn from them, and improve the defense level of the network.

4.2 Information Security Classification Protection Strategy

Implement Hierarchical Management Based on Information Security Responsibility Entities

Implementing information security responsibilities is the key to effectively improving the level of network security work in local universities. At the school level, a network security leadership structure should be established and improved; Establish and improve a network security management system, and implement grid-based responsibility management for secondary units in schools; Strengthen network security education and comprehensively enhance the awareness of network security among all teachers and students in the school.

1. Establish an information security leadership organization and implement information security leadership responsibilities. Establishing an information security leadership organization at the school level can strengthen organizational leadership, improve execution, and help coordinate the promotion of educational informatization and information security construction.

2. Establish and improve the campus information security management system, and implement information security management responsibilities. According to the requirements of the new standard, local universities should establish 41 rules and regulations, including the Network Security Management System, System Security Management System, Operating Procedures for Key Equipment, Outsourced Software Development Security Management Regulations, and Management System Review and Revision System. Based on relevant national laws and regulations, schools should systematically establish and improve information security management regulations that are suitable for their development, and meet the requirements of the security management system for the Level Protection 2.0 filing process. According to the spirit of national and provincial ideological work on the internet, local colleges and universities must also establish relevant systems for ideological work on the internet. At the level of management and coordination of specific affairs, we should adhere to the characteristics of a "two-pronged approach" to technical security and content security, and establish an Information and Network Security Coordination Office to be responsible for contacting and promoting specific work. The members of the coordination office are responsible for contacting the usage and operation departments of various application information systems, conducting security monitoring, and supervising rectification. The operation and maintenance management department of the campus information transmission network and various application information systems is the network security management department, and network and information security management security responsible persons should be set up according to the scale of the application.

3. Strengthen comprehensive governance of information security and implement information security management work. It is necessary to adhere to problem orienta-

tion, highlight key areas, and firmly implement them. Local colleges and universities should establish unified identification and standardize information dissemination; Clean up domain names; Monitoring and early warning, detect risks; Grading and filing, evaluation and rectification; Standardize data management, delineate key facilities, and develop and implement emergency response systems. Specific measures include cleaning up the application information service systems placed outside the school, comprehensively cleaning up and rectifying the use of network domain names and campus Internet IP, completing the grading and filing of various application information systems inside the school, standardizing the collection, storage, and use of data related to school management and teachers and students' behavior, carrying out information release inspection on campus websites, and strengthening the personal terminal protection capabilities of teachers and students. To fulfill the responsibility of network security and facilitate the comprehensive management of network security by the secondary departments of the school, the school should timely formulate and update relevant requirements for comprehensive management of network security.

4. Strengthen information security education and enhance the awareness of network security among teachers and students. Organize hierarchical and diverse forms of cybersecurity learning activities. The main leaders of the school can take the lead in learning relevant laws and regulations on cybersecurity, the Cybersecurity Coordination Office can organize and carry out cybersecurity seminar activities, and the school's propaganda functional departments and secondary colleges can carry out various forms of propaganda and education activities to comprehensively improve the awareness and literacy of cybersecurity among all teachers and students in the school.

Implement Graded Protection According to Information Security Requirements

The network security level protection system includes four steps: grading, filing, evaluation, and rectification. Universities need to complete the classification and filing of level protection for application information systems and regularly carry out level evaluation and rectification work according to requirements. Only through evaluation and rectification can network security be better guaranteed.

5 Conclusion

Universities have huge information security needs in campus infrastructure protection, personal information protection for teachers and students, and education digital resource construction. The Level Protection 2.0 policy will bring a stricter regulatory environment for campus informatization. In addition to Cybersecurity 2.0, laws and regulations such as Cybersecurity Law have put forward high requirements and standards for the construction of campus information security in China. Driven by policies such as Cybersecurity 2.0, it will help China's campus information security industry continue to develop rapidly.

Based on the current situation of information security construction in local universities of GZ Province, this paper studies the construction of information protection measures for universities from the perspective of classification and hierarchical man-

agement. specific measures for constructing a network protection system in universities are proposed from the perspective of classification and hierarchical management. Propose to implement classified management of network security elements, control network security incidents in stages, implement graded protection for critical network information systems, and implement graded management for network security management responsibility entities. The proposed measure has the advantages of clear thinking and easy implementation, which can provide a favorable reference for universities to carry out network security management work.

Acknowledgments

This work was supported by the growth project of young scientific and technological talents in Guizhou China for colleges and universities [grant number Qian Jiao He KY2020 137].

References

1. Notice of the Ministry of Education on Issuing the Action Plan for Education Informatization 2.0 [EB/OL]. 2018.04.18. http://www.moe.gov.cn/srcsite/A16/s3342/201804/t20180425_334188.html,
2. Feng Dengguo, Lian Yifeng. A Review of Cyberspace Security Technology Hotspots in 2023 [J]. Science and Technology Review, 2024,42 (01): 232-244
3. China National Standardization Administration. GB/T22239-2019. "Basic Requirements for Network Security Level Protection in Information Security Technology" [S]. National Standardization Administration. 2019.
4. China National Standardization Administration. GB/T25070-2019. "Information Security Technology Network Security Level Protection Security Design Technical Requirements" [S]. Beijing: China Standards Publishing House, 2019.
5. Tang Di, Gu Jian, Yu You, et al. Research on Personal Information Security Grading Method Based on Level Protection [J]. Information Network Security, 2020, (S2): 13-16
6. Liu Xiao, Li Jing, Xu Ke. A model for predicting the duration of security alarm events in smart grids based on survival analysis [J]. Computer Applications and Software, 2024,41 (01): 328-335+342.
7. Zhang Li. Building a Strong National Network Security Barrier [J]. Red Flag Manuscript, 2024, (02): 22-24
8. Fan K .Research on Dynamic Self-Adaptive Network Security Model Based on Mobile Agent[C]//International Conference on Machine Tool Technology and Mechatronics Engineering.2014.