Construction of a digital Campus Network security prevention system

Xianping Meng

Zhejiang Highway Technicians College, Hangzhou City, Zhejiang Province, 310000

Abstract: With the rapid development and widespread application of modern technologies such as big data and artificial intelligence, all industries are showing a trend of digital and intelligent development, which has brought obvious impetus to the development of the industry. For the education industry, which takes talent cultivation as its main responsibility, the application of technologies such as big data and artificial intelligence has practical significance for the development of various tasks including school establishment and operation, teaching and education, and logistics management. Against the backdrop of the continuous deepening of educational informatization reform, emerging technologies such as big data, cloud computing and the Internet of Things have been widely applied in school construction, providing convenient services for students, faculty and staff, as well as administrators, and bringing new opportunities. At the same time, it also brings certain challenges to the development of various tasks in the school. Building a digital campus network security prevention system is a necessary task for schools to promote the digitalization of campus construction and the intelligentization of education and teaching. In view of this, based on the concept overview and value analysis, this paper starts from five aspects: daily maintenance of equipment operation, strengthening the virus detection and removal function, analyzing the network usage behavior of teachers and students, intercepting any network attacks, and exploring network security risks. It focuses on exploring the strategies for constructing the network security prevention system of the digital campus, hoping to improve the standardization of teachers and students' network usage behavior and the security of campus network operation.

Keywords: Digital Campus Cyber security Prevention system Build

DOI:10.12417/3029-2328.25.06.004

Against the backdrop of the rapid development of network technology in society, computers are increasingly widely used in social production and life, and are influencing people's lives and work in an irreplaceable trend. In school construction, the full coverage of local area networks has become a necessary condition for teaching, research and teaching, entertainment, communication and office work. While the campus network brings great convenience to the work, study and life of teachers and students, it also brings certain challenges to them. The most significant challenge is the data security risk existing due to the influence of subjective and objective factors. If the network security risks cannot be identified in time, analyzed accurately, fed back in real time and effectively avoided, It will have adverse effects on the development of various tasks such as students' learning, teachers' teaching and scientific research.

1.The Concept of Digital Campus Network Security Prevention System

A digital campus is a campus network that achieves full coverage of wired and wireless networks, providing overall services for the work, study, life, communication, entertainment, etc. of all teachers and students in the school. Smart classrooms, smart teaching, mobile campus platforms, etc. are all important components of the digital campus, which greatly facilitate all students and staff of the school. The network security prevention system is a technical system aimed at ensuring the security of data and the network through means such as network supervision, identification, assessment and processing[1].

Author's Profile: Meng Xianping(1983.04 -), female, Han ethnicity, from Tengzhou City, Shandong Province, works as an information technology center staff member. She holds a master's degree and is an Information System Project Management Professional. Her research interests include educational informatization, network security, and data governance, among others.

Funding: This research is supported by the 2024 Institutional Project of Zhejiang Highway Technicians College, titled "Research on the Construction and Performance Optimization Strategy of Integrated Wired and Wireless Campus Network in Digital Campus Construction" (Project No.: 202415).

2.The Value of Building a Digital Campus Network Security Prevention System

2.1 Standardize the Internet usage behavior of teachers and students

Against the backdrop of the continuous deepening of educational informatization reform, new devices such as multimedia teaching AIDS, projectors and electronic whiteboards have been introduced into campuses and play significant roles in various aspects including teaching and research. The teaching of teachers, the learning of students and the communication between teachers and students are all realized with the support of the local area network covering the entire school, and the efficiency and level of various educational and teaching work have been greatly improved. While accelerating the coverage and digitalization of the digital campus network, the school is building a digital campus network security prevention system. This can not only better serve the communication, work, life and entertainment of teachers and students, but also effectively restrain various network usage behaviors of both. From the perspective of subjective factors, it ensures the security and stable operation of the digital campus network and avoids network security risks caused by subjective factors[2].

2.2 Protect the security of campus data

With the application of advanced technologies such as big data, cloud computing and artificial intelligence in the construction of digital campus networks, teachers' teaching, research, scientific research, lesson preparation and students' learning behaviors have gradually expanded from the offline physical space to the online network space, greatly broadening the space for the work and growth of teachers and students. While serving teachers and students in their work, the digital campus network realizes the comprehensive collection, data analysis, real-time feedback and intelligent processing of all kinds of data generated throughout the process. It ensures that any network usage behavior is recorded and assists each subject in promptly and accurately identifying their own problems, thereby ensuring that they can analyze and solve problems at the first moment they are discovered. Enhance the security and stability of the digital campus network operation[3].

Big data, artificial intelligence and other technologies that support the construction of digital campus networks and the establishment of prevention systems can achieve comprehensive collection, intelligent analysis and processing of various types of data generated during the operation of digital campus networks through functions such as speech recognition, data analysis, natural language processing, content generation and intelligent processing, assisting teachers, staff and students in extracting key information from numerous data.

3.Strategies for the Construction of Digital Campus Network Security Prevention System

3.1 Purchase and debug equipment, and maintain the operation of the equipment on a daily basis

The construction of a digital campus network requires the purchase of digital equipment that can meet the daily work needs, such as computers, multimedia teaching AIDS, projectors, VR glasses, electronic whiteboards, etc., so as to support the realization of informatization, digitalization and intelligence in teaching, research, scientific research, management, information transmission, student learning and other behaviors. As the construction of the digital campus network security prevention system becomes increasingly complete, schools should also purchase equipment that can protect local area networks, digital devices and software, such as first-generation firewalls, intrusion prevention systems, Web application firewalls, disaster recovery and backup all-in-one machines, server security management systems, operation and maintenance audit systems, vulnerability scanning systems, log audit systems, etc. By purchasing, debugging and maintaining various digital devices on a daily basis, starting from meeting the hardware conditions, a well-structured digital campus security prevention system is constructed to ensure the safe and stable operation of all kinds of software on campus. Meanwhile, schools should provide SSH encrypted login and management functions to avoid potential risks during information transmission. Through the encryption and authentication functions provided by SNMPV3, it is ensured that the data is sent from the legal data source. Moreover, the MD5 and SHA authentication protocols are adopted to guarantee that the data will not be tampered with during the transmission process between devices, ensuring the integrity and security of the data.

In addition, to ensure the secure operation of the digital campus network, the school should pay more attention to various types of equipment. Starting from the procurement of equipment, under the conditions of the school's local area network, the parameters of the purchased various types of equipment should be debugged to ensure their orderly operation in the specific local area network. In the process of maintaining close communication with the equipment purchasing units, the school's logistics management department understands the functions and performance of the equipment. Under the professional operation and maintenance services and usage guidance of the units, a regular operation and maintenance system is established to achieve daily maintenance of the operation of various types of equipment.

3.2 Download and update software to enhance virus detection and removal functions

Computer viruses such as "Panda Burning Incense", "Online Game Thief", and "Melissa" have caused extensive damage to computers and systems, leading to the leakage of files and information existing on computers and causing significant impacts. Therefore, when schools are accelerating the construction of digital networks, they should download and update virus detection and removal software, such as 360 software and Computer Manager. Through timely software updates and virus detection and removal, the adverse effects of viruses on campus computers, multimedia teaching AIDS and other digital devices can be eliminated[4].

The school downloads and updates software such as computer Manager, and regularly checks and removes viruses from computers and network systems. It starts from preventing virus invasion, detecting invading viruses, locating invading viruses, and removing viruses discovered by the system, etc., to avoid the irreparable damage caused by various viruses to the system as much as possible. It establishes and improves a unified, centralized and school-wide network coverage virus prevention system. Realize timely and comprehensive virus detection and removal as well as system protection for the digital campus network, take targeted measures for system viruses at all stages, and strengthen the virus detection and removal function of the digital campus network. Especially for the important network segments and servers in the digital campus network, real-time and thorough virus detection, removal and interception should be carried out to achieve precise identification, detection, removal and prevention of various viruses. With the increase in the types of network viruses and their increasingly powerful functions, the virus database of virus detection and removal software is updated accordingly to achieve precise identification and intelligent processing of various viruses and prevent new viruses from taking advantage of loopholes. For instance, based on the coverage of the local area network, the school selects suitable antivirus software from the numerous antivirus software available in the application market. When necessary, multiple antivirus software can also be chosen. During the combined application of multiple antivirus software, comprehensive virus scanning, identification and killing can be achieved for the operation of devices and network usage behaviors in the digital campus network. Detect and eliminate digital campus network viruses to the greatest extent. For instance, the anti-virus software is cross-linked with the digital campus network access system to achieve real-time supervision of the Internet usage behavior of all teachers and students in the school, as well as virus prevention and timely detection and elimination.

3.3 Supervise and audit logs, and analyze the Internet usage behaviors of teachers and students

Teachers and students, as the main service targets of the digital campus network, are also the key factors that trigger network security risks. Strengthening the supervision and analysis of the Internet usage behavior of teachers and students is a key measure for the construction of the digital campus network prevention system. It can start from the key factors that lead to the emergence of potential network security risks and effectively avoid network security risks. Therefore, the school has established and improved a log auditing system to automatically collect, analyze, intelligently evaluate and process various types of data on the online behavior of users, including teachers and students. It extracts key information from the various types of data generated by the online behavior of teachers and students, and based on the results of data analysis, identifies the bad behaviors of teachers and students that pose

security risks.

Firstly, establish an online log in the digital campus network to collect data on the online behavior of users using the campus local area network. Accurately record the online time and IP address of each user, and accurately locate the user's access device, port, and MAC address. Based on identity authentication and the collected online data, automatically generate a statistical chart of user online behavior. In a more intuitive way, accurately organize the online data of all teachers and students in the school, providing comprehensive and accurate information for the log to accurately identify, mark and locate online users. Secondly, the log auditing system also has the function of accessing users' detailed online data. It can comprehensively record specific information such as the sites visited by users, port numbers, access duration, and traffic, and identify various types of online data of users from it, distinguish behaviors that do not comply with network security protocols, and take corresponding handling measures as soon as the data is discovered. Prompt and warn users. Meanwhile, with the support of the NAT conversion log function, the log auditing system can achieve comprehensive collection of router records, recording detailed information such as the user's network IP address, the IP address converted from network access behavior, and specific port numbers, ensuring that the network security management department can accurately locate the source of bad access information. Issue network alerts and behavioral constraints to the corresponding users at the fastest speed. Finally, the log auditing system established based on the digital campus network can achieve comprehensive storage of network logs within three months, and can intelligently identify and specifically process repetitive and redundant data, eliminate some low-value repetitive data confirmed after analysis, establish a high-value and compact database, and realize the structured storage of complex user online data. Some low-value information is only stored for three months. For some high-value information, accurately categorize it into the database to achieve long-term storage of such data, providing structured data support for analyzing users' online behaviors and ensuring that the system can comprehensively, clearly and accurately identify users' online behaviors.

3.4 Strengthen the construction of firewalls to intercept any network attacks

After the establishment of the digital campus network and the connection of various devices such as computers and multimedia teaching AIDS, various types of data generated in real time will be automatically recorded, specifically including the network usage behaviors of teachers and students, browsing records, IP addresses, etc. At the same time, there is also the risk of data leakage. If the personal information, Internet usage behavior and other data of teachers and students in the system are leaked, it is very likely to bring adverse effects to them. Therefore, while schools are building digital campus networks, they should start from the perspective of avoiding external malicious intrusions. By strengthening the construction of firewalls, establishing a "solid wall" campus local area network, and replacing real ips with virtual ips, they can provide multiple layers of security protection for the digital campus network.

For example, schools build virtual IP firewalls, which operate at different deployment points of the digital campus network through bridging mode or virtual machine monitoring program mode to intercept network traffic and determine whether to allow, discard, reject or forward data packets. Meanwhile, the integration of network functions such as VPN, QoS, and URL filtering in the virtual IP firewall, as part of network function virtualization, can simplify network management. Without direct contact with physical network components, it can virtually adjust and modulate, identify network security risks more efficiently and comprehensively, and intercept any type of network attack. Effectively prevent malicious external intrusions. Through the construction of a firewall based on virtual IP, the real IP address of the digital campus network is hidden. Even if external malicious intruders attempt to invade the campus network, they cannot accurately locate the real IP address of the campus network in a short time. When external intruders attempt to locate the real IP address, the campus firewall, virus detection and removal software, and protection system are automatically activated, entering the anti-tracking and network alarm mode. The IP address of the located intruder is informed to the network police, and the internal protection system is upgraded to

achieve accurate early warning, automatic identification, and efficient interception of various network attack behaviors.

3.5 Big data analysis of risks and identification of potential cybersecurity hazards

Due to the influence of subjective and objective factors, during the operation of the digital campus network, it is very likely to face various security risks, which will have adverse effects on the entire network system and the network usage behavior of teachers and students. The network also has a certain degree of instability. If the relevant information cannot be identified in a timely and accurate manner, it will directly affect the operation status of the network system and even easily lead to data security issues such as personal information leakage. Extracting key information from the large volume of data generated during the operation of the network and analyzing it is an important measure to solve the above problems. Therefore, when schools are building a digital campus network security prevention system, they should actively introduce big data analysis technology to provide new ideas for campus network security risk assessment. By collecting, analyzing and mining massive network data, they can more comprehensively and accurately identify and evaluate network security risks, discover potential hidden dangers, and thereby formulate and implement effective strategies.

For instance, while building the digital campus network, with big data analysis technology as the core and supported by functions such as machine learning algorithms, expert systems, and speech recognition, a campus network security risk assessment model is designed and established to achieve full-process supervision, data analysis, real-time feedback, and intelligent processing of the campus network security operation status. For instance, the risk assessment model starts from both internal and external aspects to achieve comprehensive supervision of subjective and objective factors. It collects and analyzes data in real time, extracts key information from it, accurately identifies potential security risks, and traces them back to the source. It focuses on the root causes of network security risks and takes targeted measures to eliminate them and avoid security risks.

4.Conclusion

With the continuous deepening of educational informatization reform, various new technologies and equipment such as multimedia teaching AIDS and computers have been widely applied in campus construction and operation. While meeting the needs of digital office work for teachers and staff and online communication between teachers and students, there are also certain security risks when achieving real-time data recording. Therefore, when schools are accelerating the construction of digital campus networks and the process of digital transformation, they should adopt effective data security protection measures. That is, they should intensify the construction of the digital campus network security prevention system, starting from five main aspects: equipment maintenance, software updates, log auditing, firewall construction, and hidden danger exploration, to improve the protection structure of the digital campus network. Accurately identify and intelligently analyze the cybersecurity risks caused by subjective and objective factors, and intensify the efforts to avoid risks, comprehensively and dynamically strengthening the network protection of digital campuses.

References：

[1] Song Yang.Analysis of the Current Situation and Preventive Measures of Campus Network Security in the Advanced Digital Campus[J]Information and Computer(Theoretical Edition),2023,35(10):228-230.

[2] Shen Shuping.Prevention Mechanism of Online Fraud on University Campuses from the Perspective of Cybersecurity[J]Legal Affairs Review,2023,(08):124-126.

[3] Qian Wu.Application of Campus Computer Network Security Technology Based on Network Security Maintenance and Prevention[J]China New Communications,2023,25(02):113-115.

[4] Su Zhizhong.Construction and Practical Analysis of Network Security Prevention Mechanism for Digital Campus[J]Computer Knowledge and Technology,2021,17(16):40-42.