Lecture Notes in Economics, Management and Social Sciences, ISSN 2617-1031

2021 3rd International Conference on Economics, Marketing, and Management

Vol. 36, 2021, pp. 105-108

Analysis on Current Situation and Defense Measures of Network Security Management in Colleges and Universities

Fangyi Zhang

Jiangsu Institute of Commerce, Nanjing, Jiangsu, 211168, China

ABSTRACT. As the main place of modern education, colleges and universities are not only users of the network but also promoters of the network, so Internet are more frequently used in colleges and universities. Network has the characteristics of freedom and openness, making the teaching and management activities in colleges and universities more information-based and open. However, network information management has become the focus of network security management in colleges and universities because the popularization of network has brought new means of information crimes. The theft of network information and the theft and reselling of personal network information have seriously damaged social security. Under the background of big data, it is very urgent and important to strengthen the protection of network information. This paper analyzes the current situation of network security management in colleges and universities, introduces advanced key technologies such as early warning, protection and monitoring, and further puts forward the protection strategies of network information security under the background of big data era.

KEYWORDS: Network information security, Colleges and universities, Protection strategy

1. Introduction

China’s social and economic development continues to accelerate, and network has become a platform for people to exchange. In the era of big data, network security is more important and has a direct impact on the personal and property safety of the public [1]. At present, the network crime rate is obviously increasing. Criminals use the loopholes in campus network to steal students’ information and then help others cheat in exams. Therefore, it is urgent to build a perfect, dynamic and in-depth network security management system to improve the system’s security defense capability. The widespread use of big data in various industries not only helps to improve the work efficiency, but also brings challenges to network information security [2]. The network is open and virtual, and its security has become the primary consideration of the users. Once the campus network is invaded, it will easily cause information disclosure [3]. A large amount of data and information spread rapidly in the network, so the demand for information security is getting more and more urgent. Constantly improving the level of network security and establishing a more efficient information protection system are the requirements of network information security in the era of big data [4]. If there is any mistake in the network security management, it will cause accidents such as interruption of teaching activities and data leakage. Therefore, we must pay full attention to the network security in colleges and universities.

For universities, the Internet is used more frequently. However, opportunities and challenges coexist. Although the Internet can bring convenience to the teaching activities and management of colleges and universities, it also brings challenges to the network security management [5]. In addition to improving the protection of computer technology, it is also necessary to strengthen the construction of network protection capabilities, and enhance the security of network information from aspects of personnel, technology and resources. In this context, many organizational decisions, methods and models for analyzing problems become reality with the help of big data, and the results under the big data algorithm are served as reference [6]. Up to now, the network has become an important platform for teaching, management and scientific research in colleges and universities. However, due to the defects of the network, network security faces many threats, which seriously affect the sound development of teaching activities [7]. Problems such as network paralysis, leakage of important data and interruption of teaching activities in network management of colleges and universities happen one after another, so network security management cannot be ignored. This article analyzes the problems in the network security of colleges and universities, and puts forward corresponding measures to deal with these problems, so as to play a positive role in reference for network security management in colleges and universities.

2. Factors Affecting Computer Network Security in Colleges and Universities

DOI: 10.23977/ICEMM2021025

2.1 Hardware Problems

At present, the computer network technology is continuously improving. At the same time, the network attack methods are becoming more and more sophisticated. In the complex network interaction, there will inevitably be weak points, which will be used as loopholes for attacks. Computer networks are characterized by openness under a wide range of application requirements, which makes computer network systems vulnerable to external attacks and leads to a decrease in security. Hardware devices and network components are the physical basis for computers to operate. Once problems occur, they will easily threaten their security and stability. In the era of big data, it is of certain practical significance to strengthen the level of network information security, especially the importance of current information and data to production and life is gradually prominent, and the importance of strengthening computer network information security is especially important [8]. In the initial design of the network system, the main consideration is whether it can run smoothly, even if there is a local failure, it will not block the normal communication, thus ignoring the consideration of security issues. Some computer network users who are not professional have poor awareness of network security and weak operation technology. Under the background of rapid development of science and technology, the society is increasingly demanding the use of data information. In order to ensure the accuracy of data information, the processing and screening level of data information is also continuously improving. The operating system is not absolutely safe, the key network technology is not guaranteed, whether the firewall can play the expected role, these problems are not completely solved, the security of the computer network cannot be guaranteed, if there are many uncertain risks, the results can be imagined [9]. The contents of data and information are diverse, mainly for communication, including pictures and videos, etc. At the same time, there are differences with traditional single data results. Users of computer network information lack the awareness of security protection, and negligence may cause the problem of disclosing users' security passwords or other security information during operation. This inappropriate operation mode is just created by the destruction of illegal elements. Enterprises and individuals need to strengthen the awareness of preventing computer hackers. First of all, they need to perfect the computer network management system to prevent hackers from invading and improve the level of automatic identification capability of computer systems.

2.2 Software Problems

Various functions of the computer need to be executed under the user's operation, and the user's operation of the computer is often subjective. It is inevitable that some damages will occur to computer facilities and equipment, thus causing some phenomena that affect the safety of computer information, resulting in interruption or loss of transmission of computer information. With the development of computer technology and the convenience it provides, computer technology is playing a more and more important role in all walks of life. As hackers and viruses have only gradually arisen in recent years and have affected the normal operation of computers, some management systems of computer networks themselves are not aware of such potential dangers and have not made advance prevention against potential intrusions. Encrypted data can be understood as controlling access rights, and can also be understood as using encryption keys and algorithms provided by computer systems to change data information into unique ciphertext so as to improve the invisibility of encrypted information. The Internet itself has its own risks. The campus network of colleges and universities is inseparable from the Internet. It is more convenient and fast to obtain information, and at the same time, it also provides opportunities for people outside the school to obtain internal resources. Junk information is usually transmitted compulsorily in the form of mails and news notices. Many enterprises steal trade secrets and important documents of other enterprises by means of this mandatory feature, and this kind of information stealing behavior is mainly carried out by spyware. For computers that need access rights and passwords, hackers can write programs, debug them continuously, and finally invade. The computer network itself has relatively fixed equipment, and the network equipment cannot fully resist external infringement, resulting in the computer being unable to protect itself in time when encountering disasters and pollution.

3. Suggestions on Network Security Precautions in Colleges and Universities

In the design process of university network security management system, active and hierarchical security defense principles and technologies are adopted, and various active defense technologies such as network security early warning, security monitoring and security protection are introduced. The school also needs to carry out research work, reasonably select relevant equipment, pay attention to independent research and development of the school, and communicate with other colleges and universities, learn from successful experiences, and debug the system after the installation is completed. The imperfect system is the root cause of the network information security problem. First, users lack of maintenance and repair of computer network systems, which results in the destruction of network information. After the anti-virus software is successfully installed, it needs to be guaranteed to run all the way during the use of the computer, thus effectively preventing viruses from invading the computer through network channels. The security defense system integrates various network security defense technologies to realize the detection and killing of network viruses and trojans, prevent the spread of network trojans and viruses, prevent the attack and infection of university networks, and disrupt the normal use of university networks.

In order to effectively ensure the security of computer network information, special information security protection mechanisms should be formulated to reflect the authority and persuasion of laws and ensure the security of computer network information. After calculation, the average loss caused by each computer crime is 1.6 million US dollars. If the losses caused by traditional crimes are compared with those caused by computers, they cannot be compared at all. The average crime loss is shown in Table 1.

Table 1 the Average Loss of Crime

Crime Type	Average loss (ten thousand US dollars)
Computer crime	40-170
Blackmail banks	3
Robbery	0.5
Steal	0.01-0.4

Hardware equipment pays attention to overall coordination. Considering durability and cost, too high cost will increase the financial burden of the school, while too low cost will affect the quality of hardware equipment. The university network center needs to update the software in time and remind the students to download the upgrade package of antivirus software in time through the way of university network client, which is an effective measure to prevent virus hiding and improve network security. Some hackers may be in the psychology of competition and destroying ambition. They may also attack the other party's computer network system, steal information, destroy the network structure, and cause the paralysis of the computer network information system. For passive attacks, it is a means for network information to be cracked and intercepted. Under normal circumstances, it will not hinder the smooth use of the network [10]. Security awareness is the premise to ensure network security. Without security awareness, no advanced protection software can ensure safety. Managers of relevant enterprises need to strengthen the awareness of managers about the security related to computer network security management and maintenance, and also consider the possible problems in the safe operation of humanoid computer networks. For university network users, it is necessary to download system software through regular entrance and download system patches according to reliable security software prompts. Users should strengthen their ability to distinguish hacker's stealing behavior, and reduce the probability of successful virus and hacker invasion by optimizing firewall level and distinguishing internal and external data.

4. Conclusion

Today, the Internet has penetrated into every corner of society. As the forefront of the generation and application of new technologies and knowledge, colleges and universities have a large number of network users, so there are correspondingly many hidden dangers of network security. Only by enhancing the technical level and strengthening the relevant safety awareness can the potential network information leakage be effectively avoided. University network security defense is a dynamic and systematic project, which needs to improve the system defense capability in time and further enrich the functions of security management system according to the status of network security threats in actual application. Only by establishing and strengthening the network security technology and the complete network security system, can we have a place in the future data analysis era. To a large extent, network security problems are caused by non-technical factors. Security management loopholes and managers' negligence are the biggest security risks. To improve the application of firewall and other related security systems, strengthen the awareness of information storage and transmission, and improve the computer network security management system are important measures to enhance the security of big data computer network information, but also the only way.

References

[1] Wang Xingguo. Research on Problems and Strategies of Network Security Management in University Campuses. Journal of Liaoning Administration College, no. 5, pp. 50-53, 2015.

[2] Yang Hu. Problems and countermeasures of network security in colleges and universities. SME Management and Science and Technology Journal, no. 1, pp. 309-310, 2015.

[3] Tang Xu, Chen Bei. Analysis of the effective use of computer information technology in network security in colleges and universities. Computer Knowledge and Technology, vol. 12, no. 26, pp. 58-59, 2016.

[4] Xu Hao. Research on problems and countermeasures of network security management in colleges and universities. Digital Technology and Application, no. 9, pp. 200-201, 2016.

[5] Chen Xinliang. Hidden Troubles and Countermeasures of University Campus Network Security. Contemporary Education Practice and Teaching Research, no. 5, pp. 262-263, 2016.

[6] Yang Xu, Gao Yuzhuo. Research on network security problems and strategies of college campuses. Computer Knowledge and Technology, no. 6, pp. 37-38, 2016.

[7] Liang Jian. Analysis and countermeasures of network security problems in colleges and universities. Information recording materials, vol. 17, no. 4, pp. 92-93, 2016.

[8] Gong Xiao, Zhou Yinping, He Dongqin. Application of wireless network security precautions in university networks. Information Technology and Informatization, no. 5, pp. 142-144, 2019.

[9] Lu Jiaqi. Discussion on Geographic Information Data Network Security under the Background of Big Data. Surveying and Mapping Engineering, no. 7, pp. 73-75, 2015.

[10] Yang Yan, Zhang Ying. Research on network information security in the context of big data. Automation and Instrumentation, no. 10, pp. 149-150, 2016.