DOI: 10.23977/infkm.2023.040103
ISSN 2523-5893 Vol. 4 Num. 1

Campus Information Network Security Vulnerability Analysis and Security Reinforcement

Fan Liu[*], Zhengrong Luo

Department of Electronics and Information Engineering, Guang'an Vocational & Technical College, Guang'an, China
[*]Corresponding author

Keywords: Campus, information network, security breach, security reinforcement

Abstract: Information technology has become the core of school construction and management. Information technology construction provides high-quality teaching, management and services for schools. The campus information network becomes more and more complex. But as network complexity increases, so do network security vulnerabilities. With the development of network technology, the security loopholes of campus information network are becoming more and more prominent. It has also become the focus of attention of network security researchers and professionals. This paper firstly introduces the status and types of campus information network security vulnerabilities. The security loopholes of campus information network are analyzed. At the same time, it discusses the causes of security loopholes and their threats to the campus information network, Based on this, the corresponding security reinforcement measures are put forward in order to improve the security of the campus information network.

1. Introduction

In today's information society, information network is an important tool for people to communicate and transmit information. It is also one of the important pillars of economic and social development. The "Statistical Report on China's Internet Development Status" released by the China Internet Network Information Center in 2021 shows that my country has 989 million Internet users by the end of 2020, achieving an Internet penetration rate of 70.4%. This means that the Internet has penetrated into people's lives in all aspects of work, study and entertainment. It also means that the security of the Internet affects national security and social stability [1]. In recent years, with the rapid development of mobile intelligent systems and mobile Internet, more and more software runs on mobile terminals. In addition to the well-known Trojans, viruses, worms, DDoS, hijacking, zombies, and backdoors, malware such as spyware, adware, scareware, ransomware, and trackware (trackware) have also appeared on mobile Internet platforms[2,3].

We are in an era of rapid development of information technology, and information technology has become the core of school construction and management. Information technology construction provides high-quality teaching, management and services for schools. The campus is a unique social environment, which has its own characteristics with the external environment. Therefore, the campus information network established in the campus is relatively more unique and more and more complex.

But as network complexity increases, so do network security vulnerabilities. If these security loopholes are not discovered and repaired in time, it may have a serious impact on the security of the campus information network. Therefore, how to analyze and strengthen campus information network security vulnerabilities has important practical significance.

2. Campus Information Network Security Vulnerabilities

Campus information network security loopholes mainly include system loopholes, network loopholes, and human loopholes.

System vulnerabilities mainly refer to security holes in the operating system and application software. Once the vulnerability is exploited by an attacker, it may lead to malicious attacks on the operating system and application software. Thus the security of the campus information network is destroyed. For example, the operating system used by the school's network system may not be the latest version, and there may be some security holes that are easy to be attacked.

Network loopholes refer to the security loopholes in the campus information network structure. It may lead to attacks on network communication protocols, thereby destroying the security of campus information networks.

Man-made loopholes refer to the security loopholes existing in campus information network users or managers. This type of vulnerability could lead to password disclosure via verbal transmission, email, or other means. Therefore, the security of the campus information network is destroyed.

The above three types of security loopholes may become a security threat to the campus information network. But the most common one is the system loophole, which is most likely to be exploited by attackers, thus causing serious damage to the campus information network.

3. Causes and Threats of Security Vulnerabilities

The campus information network is connected to the Internet, and hidden dangers to network security are inevitable. The main reason is that the campus information network technology is not mature enough. Because the campus information network technology is still in its infancy, the relevant technology has not yet reached a mature level. There are security loopholes in the software and hardware devices used in many campus information networks. It is an easy target for attackers. Such as routers, switches, etc. Due to insufficient technical level, it is easy to have defects, which seriously affects the security of the network. However, there may be some security loopholes in network applications, such as viruses, Trojan horses, etc. It easily undermines network security and causes information leakage.

Secondly, there are many users of the campus information network. System administrators lack professional and technical capabilities, and network management norms are often not strict enough. Some sysadmins don't even manage at all. These provide an easy loophole for attackers to hack.

There are also improper usage habits of users.

Many users lack information security knowledge and have improper usage habits. For example, security warnings are often turned off when using software, causing users to install malicious software. Malware is a general term for software that is not expected to run by users, has malicious purposes, or completes malicious functions [4, 5]. There are many types of malware, such as Trojans[6], viruses, worms, DDoS, hijacking, zombies, backdoors/trapdoors[7], malicious compilation, spyware, adware, ransomware, tracking software, etc[8,9]. Sometimes users visit websites that are not securely authenticated. These will further increase the security risk of the campus information network.

With the continuous improvement of the level of campus informatization, information technology has become an important means of campus intelligent operation. While bringing convenience to teachers and students in terms of teaching and management, it also promotes the campus information system to continuously increase external services on the basis of the previous intranet operation. Due to its high privacy and high value, a large amount of student data is even related to social public interests and national security. It has always been the focus of infiltration attacks by black industry organizations.

Campus network security breaches can lead to the theft of transmitted information. Due to security loopholes in the campus information network, attackers may attack the campus information network and steal information transmitted in the network. As a result, information leakage is caused, and the learning, teaching and management in the campus are seriously affected.

In addition, system security will be affected. Attackers can exploit security holes to carry out malicious attacks. A successful attack may destroy the security of the campus information network. It seriously damages the school's network data and network equipment.

The emergence of campus information network security vulnerabilities will pose a serious threat to network data and system security. It will lead to network data leakage, system paralysis, network tampering and other consequences. It will seriously affect the normal teaching and management of the school, and even cause damage to the school's reputation.

4. Security Hardening Measures

Campus information network security reinforcement first needs to improve the campus information network structure. The campus information network structure should be based on the principle of layered management, and control points should be set reasonably to improve network security. The system can use identity authentication technology, dynamic token encryption storage and other forms. The administrator sets the user level and the file directory that can be browsed according to the user level. Schools can also use encryption technology to systematically encrypt very important information.

Schools should update their operating systems and install security patches in a timely manner. In this way, viruses, trojans, and malware can be prevented from invading. The administrator should regularly check the network equipment, find problems and fix them in time to ensure the normal operation of the network equipment. In order to ensure user security, the dynamic token of the network device must be set to a user name and password exceeding eight characters. At the same time, the password must have special characters, combining numbers and letters.

Secondly, the security reinforcement of campus information network needs to strengthen system maintenance. A complete system maintenance system should be established, and system updates should be improved regularly to ensure system security. Schools should establish a sound safety management system and refine safety management responsibilities. This will further clarify safety management responsibilities and formulate safety management norms.

In addition, users need to strengthen security education. Schools should provide safety education to campus information network users. This can increase their awareness of information security and increase their awareness of information security. Managers should strengthen safety awareness and improve the level of safety management. They need to continuously improve their network security knowledge to prevent security breaches from happening. At the same time, the management agency should also establish a safety audit system and conduct regular safety reviews. In this way, security loopholes can be discovered and dealt with in time, and security protection can be strengthened.

The campus information system should install a firewall to prevent hackers from entering the network. This prevents malicious attacks. Managers need to strengthen network monitoring for network and system operation. A sound network monitoring system should be established to monitor the network in real time and discover and deal with security vulnerabilities in a timely manner. In order to ensure the security of campus information network, schools should strengthen network management. In particular, it is necessary to strengthen the security protection of network equipment to reduce the occurrence of security breaches.

5. Conclusion

This paper mainly analyzes and summarizes the security aspects of the entire campus information network. The inadequacy of this paper is that it does not discuss deeply about the technology that is specifically applied in network security. This will continue in future research. Security loopholes are an important threat to campus information network security. If these security loopholes are not discovered and repaired in time, it may have a serious impact on the security of the campus information network. In order to ensure the security of campus information network, schools should strengthen network management to reduce the risk of security breaches.

References

[1] Ye W, Cho K. Hybrid p2p traffic classification with heuristic rules and machine learning. Soft Computing, 2014, 18(9): 1815–1827.

[2] Castillo CA. Android malware past, present, and future. White Paper, McAfee Mobile Security Working Group, 2011: 1–16.

[3] Zhou Y, Jiang X. Dissecting Android malware: Characterization and evolution. In: Proc. of the 2012 IEEE Symp. on Security and Privacy. IEEE, 2012. 95-109.

[4] Skoudis E, Zeltser L. Malware: Fighting Malicious Code. Upper Saddle River: Prentice Hall Professional, 2004.

[5] Sikorski M, Honig A. Practical Malware Analysis: The Hands-on Guide to Dissecting Malicious Software. San Francisco: No Starch Press, 2012.

[6] Wei Junxu, Tuyatsetseg Badarch. Research on the Application of AI in the Cyberspace Security: A Case Study of Smart Campus Network Security. American Journal of Computer Science and Technology, 2022, 5(2).

[7] Huang Chang Wei, Xiong Jin Quan. Study of Campus Network Security Based on Dynamic Self-Adaptive Network Security Model. Advanced Materials Research, 2013, 846-847(846-847).

[8] Wei Hong Fu, Jian Hua Liu. Study on Campus Network Security and Protection Technology. Applied Mechanics and Materials, 2012, 2025(220-223).

[9] Chen K, Wang XQ, Chen Y, Wang P, Lee Y, Wang XF, Ma B, Wang AH, Zhang YJ, Zou W. Following devils footprints: Crossplatform analysis of potentially harmful libraries on Android and iOS. In: Proc. of the 37th IEEE Symp. on Security and Privacy, Ser. (S & P 2016). 2016.