Analysis of Campus Computer Network Management and Security Technology Based on the Status Quo of Modern Network

Zhenguo Liu

1Shandong University of Political Science and Law, Jinan, Shandong, China, 250014

*Corresponding author e-mail: liuzhenguo@sdupsl.edu.cn

Abstract. At present, with the comprehensive improvement of modern computer science and network literacy, people are increasingly demanding the quality of their lives and related rationality. Slowly, we will gradually find that the computer has now become an important unit in our lives\textsuperscript{[1]}. It seems that without the support of computers, our lives cannot continue. It is precisely because of the development and application of computer networks that the current network security and management measures of some campuses in our country cannot keep up with the upgrading of computer technology. This situation will also lead to loopholes in computer network management and security. In a nutshell, computer network technology unites the space and time of our lives. It is an innovative process in the network age. However, we still need to pay attention to the security management of some campus networks and the enhancement of information technology.

Keywords: Modern Campus, Network Management, Security Status

1. Introduction
In the early years, with the popularity of the Internet and the accumulation of time, people gradually realized the importance of computer network technology to our production and life. After that, people store and trade all relevant information chains in life and work through computers. This approach has brought a lot of self-confidence and convenience to human life. On this basis, it has also promoted the development of campus education in our country. However, for now, the research on computer network management and security technology inside our campus is sluggish. Experts believe that this may be due to a lot of loopholes in the internal computer network of the campus and an uncertain state caused by human factors. Perhaps in a short time, people will not be able to see its destructiveness. However, if things go on like this, the information chain inside the campus will be badly destroyed\textsuperscript{[2]}.

Cyber attacks and cyber security have always been the knowledge points that cyber experts are actively propagating. However, in recent years, there have been endless cyber attacks on campuses and unknown cyber threats from hackers. This has sounded the alarm for the safe construction of the internal network of our campus. Network administrators on campus should also reflect on the reasons
for these cyber threats. Indeed, the Internet has an open and social policy. Although the school's network is gradually opening up, this puts forward higher requirements for our network security skills.

2. Interpret the dangerous elements affecting the school's internal network based on the current status of the modern network

2.1. Negative factors in the operation of campus network
As the internal network of the campus network, many schools may use the local area network to limit the scope of the internal network. But this is unrealistic. If the local area network always maintains the network share connection, this will also lead to the emergence and increase of serious security risks. Furthermore, the browsing of internal management personnel's web pages and the information transmission of some external devices with computer viruses are all negative factors (see Figure 1).

![Image of network security management](image)

**Figure 1.** Conceptual diagram of network security management.

2.2. The invasion of campus external network and information
Each school has its own internal computer room. The network composition of this computer room is the internal connection of the local area network. In the process of network invasion, many of the network administrators believed that this was not an invasion of the campus external network. However, this is indeed the case. When people use external computers to transmit some maliciously intrusive information to any computer inside the school, due to the limitation of the local area network, this will cause the entire computer system of the school to be implicated.

2.3. Network invasion caused by experimental equipment
In many cases, we do not think that the experimental equipment will bring negative network impact. Such a cyber attack occurred on the author's university campus. Finally, the expert team found out that the reason was the intrusion of a malicious virus from a computer in a device of the Electronic Information Laboratory. Therefore, when teachers or students conduct extracurricular experiments, they must pay attention to the phenomenon of cyber attacks on electronic experimental equipment.

3. Interpretation of hidden dangers affecting school internal network security based on computer terms

3.1. Network security issues due to the operation of malicious programs
We know that the school's local area network is a network mode that can limit the range of users' network status. However, the scalability of computer programs cannot be restricted. Moreover, the operation of each series of programs is accompanied by the emergence of probabilistic loopholes. If
network vulnerabilities occur, some hidden network risks will be exposed during the operation of the program. Moreover, some hackers may also look at these vulnerabilities and make a fuss.

3.2. Errors in program operation caused by the appearance of computer invasion Trojans
In computer terminology, we refer to program operation errors as improper execution of the language of the program. This will lead to the appearance of loopholes with great probability. What's more frightening is that a large part of the program running errors are due to the computer inside the campus being attacked by invading Trojan horses. Once, the transmission of the Trojan is accepted by a certain computer. Then all the programs in this computer will run disorderly and have no rules.

3.3. Security risks of script viruses that steal personal information
When we interview some people with hacker experience and experience, we will find that they can create all kinds of computer viruses. Among them, the scripting virus is the simplest, and at the same time, its threat ability is also the greatest. Moreover, these script viruses often attach to the login entrances of some websites. Once someone logs into this website, the script virus will steal personal information from the personal computer.

4. Implementation of the basic strategy of campus computer network management and security technology based on the status quo of modern networks

4.1. The simplest standard of campus computer operation common sense
Schools can compulsorily require students not to use the computers on campus to access external networks. For example, some foreign language websites, game websites and some small program software websites. In addition, the school can regulate students as far as possible not to transfer the off-campus hard disk directly to the campus network through the USB interface. Moreover, reducing the use of social software on internal networks is also a way to limit cyber threats (see Table 1).

Table 1. Investigation of basic computer strategy and security technology in campus based on modern network.

| Basic strategy          | Safety technology                  |
|------------------------|-----------------------------------|
| Operating common sense | Use of firewall                   |
| Use of antivirus software | Encryption of core data            |
| Use of restore software | Network supervision technology     |
| Unified supervision of LAN | Supervision of internal procedures |

4.2. Use of simple antivirus software
I remember that when the author was in junior high school, the instructor of the computer course told us to let us install an anti-virus software on the computer at home to protect and clean the computer. If the school cannot prevent students from using computers to access external networks. Then schools can install anti-virus software to avoid the invasion of external viruses. Unfortunately, there are still a large part of viruses that are not found by ordinary anti-virus software, which is also a drawback.

4.3. Use of computer recovery software
The software that drives the restoration is mainly to restore the original system and software of the computer. This can be thought of as a system restore setting. If the student downloads the information software of the external network through the internal LAN, and the malicious information has not been completely invaded by the software, the computer can restore the software, and the computer can delete the software completely without leaving any traces.

4.4. Use of unified monitoring software for local area network
According to the above description, we know that current schools use local area networks to restrict the output and input of network programs. However, a local area network can restrict the entire
network, but it cannot restrict the entry of externally input programs from each computer. Then, we can carry out the unified detection software of the local area network to communicate the information of each computer device. This prevents the input of computer viruses.

5. Based on modern network in the campus computer network management and security technology application

5.1. The measures taken by the computer firewall
When the computer was first studied, people proposed the use of firewalls by referring to the actual examples of wall isolation in order to maintain its internal network information. At present, in order to avoid the invasion of external viruses, compared to anti-virus software, the more practical is the firewall technology. Unfortunately, many people now turn off the firewall for playing games. This approach is incorrect.

5.2. About the encryption method of the school's core data
This is a computer protection measure to pave the way first. If the school cannot protect its own network from external hackers or viruses. Then, the school can encrypt the core data. At present, some anti-virus software also provides the use of these encryption software. Moreover, it is very difficult to crack the files through improper methods after being encrypted. Therefore, the author believes that this is also a security measure that can effectively enhance the campus protection network.

5.3. Application of network supervision technology
Some people have proposed that if the computer self-testing technology is used to protect the information inside the campus, this is also a unique protection measure. With people's research, the emergence of this technique is called the real-time self-regulation technology of the network. If the computer appears to be attacked, the network will appear to lock itself. In this state, the information on the campus internal network cannot be transmitted. It is equivalent to bundling computer viruses inside the computer. Then use the computer's anti-virus software to check and kill.

5.4. Supervision of internal computer programs
In many cases, the virus of our internal software can be hidden. This is because the expression of the virus is unilaterally restricted by anti-virus software or firewalls. However, it is also a hidden bomb. Under the current situation of modern networks, internal supervision procedures are also a major measure for computer self-protection. However, this also depends on the status quo of computer program expression.

6. Content analysis of network security scanning based on modern networks

6.1. Security scan of remote network
A lot of information from computers in different regions is transmitted through network sharing, so in this process, we must scan the network security must be cross-regional or cross-time restrictions. Fortunately, current computers can perform remote security scanning to determine the security of the information of the docked computer and the security of the transmission path.

6.2. Scanning of network firewall
Many people do not understand the reason for scanning the firewall of the campus computer. In fact, in our lives, part of the cases of computers being attacked by external viruses is because the firewall was first attacked by viruses. After the firewall loses its function, the internal network will suffer. Therefore, timely firewall scanning is also a precautionary security measure.

6.3. Scanning of visited websites and downloaded software
No one knows whether there is an Internet virus in the website they have visited or the website they have downloaded\[5\]. Then, based on this requirement, the computer can scan the security of external websites and software that enters the internal network from external websites. This can guarantee the security management of the internal network\[6\].

7. Conclusion

In fact, the technique of preventing computer network security based on the current status of modern campus networks is a relatively difficult and complicated electronic project. The knowledge it involves is diverse. However, for the security of the campus’ internal network, we must overcome numerous difficulties and persevere in security management.

Perhaps the realization of this process is very difficult. What keeps us going should be our love and noble worship for network technology\[6\]. Enthusiasm can help us find the way forward. Struggling hands can help us develop advanced technologies for network security.

Acknowledgement

This article is the phased achievement of the scientific research project of Shandong University of Political Science and Law "Design and Implementation of Campus Network Security Protection System" (Project Number: 2017Z10B).

References

[1] Qi-Liang H U, Jin-Bo L, Ran T. A relative research on the status quo of the sports culture construction in the campus of the central areas' common college and universities [J]. Liaoning Sport ence and Technology, 2008.

[2] Xiangyang C. On the Security Status Quo and Countermeasures of Campus Network in Higher Colleges [J]. Computer Study, 2010.

[3] Li-Na F U, Qing-Qing X U. Analysis on the Status Quo of Primary and Secondary School Students' Campus Wear [J]. Journal of Henan Textile College, 2006.

[4] Changchun L I. Realization and Performance Analysis of IPSecVPN System in Campus Network [J]. Journal of Panzhihua University, 2017.

[5] Jin-Ding B. Higher Network Management Practice of the use of NetFlow Technology [J]. Computer Knowledge and Technology, 2009.

[6] K. Shankar, Mohamed Elhoseny, Trust Based Cluster Head Election of Secure Message Transmission in MANET Using Multi Secure Protocol with TDES, Journal of Universal Computer Science, vol. 25, no. 10 (2019), 1221-1239

[7] Yamei M U. The Analysis and Solution on the University Campus Network Security [J]. Intelligent Computer and Applications, 2012.