Security Management and Prevention on the Campus Network against Hacking

Xue-rui WANG, Yong-qiang HE
Henan Institute of Engineering
Zhengzhou, Zip Code: 450007
China

ABSTRACTS: *At present, the Internet had got great development in our country. Internet security problem has received widespread attention. After a long period of development, network security technology has become a comprehensive discipline. In our future work and life, the internet is not only a tool, but also a patent only for the minority. It will become a kind of cultural symbol and the way of life into all areas of our lives. Through the analysis of campus network security management of hacking and prevent, this study had put forward some of the techniques and methods against the hackers in the campus network security management. The campus network security management not only could prevent hackers invasion, but also remind the users to pay attention to network security management methods.*

Keywords: Internet Security Management, Hacking Invasion, Prevention

Received: 18 April 2019, Revised 5 July 2019, Accepted 19 July 2019

DOI: 10.6025/jisr/2019/10/3/87-91

1. Introduction

In today's society, computer network has got rapid development, the worldwide Internet traffic is far more than the traffic between person and person. And the Internet has shifted from a data center into a more intelligent developed network, and it will be the regulation of information between person and person. While copying and pasting are forecasting people between the information demand, through the network of replication, users could filter the information what they need. And put the information you need in the form of a the best. At the same time, the problem of network security are getting more and more attention from people. Once the computer network security problems come up, the computer system will collapse, and will cause great economic loss even unit or individual, or more likely to hinder the normal work. Therefore, strengthening the management of computer network security and the prevention work will become the important content of informatization.

Since 1990s, many colleges and universities of our country began to implement the informatization construction, the current campus network in colleges and universities in one billion trunk, and one hundred million to a computer. Campus have wireless

AP one to two hundred, and basically covers all the campus offices. Campus network are mostly on the basis of integrated wiring platform, digital management, teaching and scientific research, life in the internal overall digital campus construction. And put into use in the construction of the digital has a unified, unified portal, unified data standard, unified database platform certificate authority, also built with orientation, registration, course selection, OA, educational administration, personnel, scientific research, integration of the assets, youth corps committee, archives of an information management system. Campus built the campus one-card system, this system includes the campus consumption and utilization, management and identity authentication. A series of measures for teachers and students in the school campus digital construction provides a convenient living and working conditions.

Although, the computer network has provided many conveniences for college teachers and students, but the problem of campus network security is becoming more and more obvious. Many campus website and the server are intrusive and attacks, the campus electronic administrative data may be tampered with, the student Internet account and password are often stolen on campus, but also occasionally spread bad information on campus. If there is no management and restriction for the conditions, it will seriously affect the normal campus life of teachers and students, and will also bring many bad consequences for the schools. The computer network technology is very complicated, and enable the computer network security raise to a new field, and update timely.

2. Hacking in Campus Network Methods and other Factors

Currently, there is a lot of version and methods of hacking method of computer network, and its danger has far more than the dangers of the virus. Because the Internet is not limited by geography and space, so each kind of hacker attack spread all around the world in a very short period of time, and the means of attack is mainly using the Internet and leading to computer system vulnerabilities, even attack the computer network system paralyzed. Some hackers straightly hack the base protocol and direct invasion of the Internet operating system level, so the campus network security faces great problems. Through the analysis of the research for a long time, this study has summarized the way of hacking in campus network and other factors affecting the safety of the campus network, with the below details: following details:

2.1 Computer Network Software Vulnerabilities

As we all know, no matter what a computer system or network software, it can't be perfect, there will be some shortcomings and loopholes. Due to such problems, it will make the campus network in a very dangerous situation. At the same time, the campus network users are easy been attacked by hacker, and easy attached by the virus, the campus network is unstable and unsafe one of the important factors.

2.2 The Existed Problem in Network Security Configuration

Network security equipment can cause some security problems, when it is not configured correctly, for example, some security software may make the software can't work properly. And for a specific web applications. When it started, it can appear certain security gap, and a lot of bundled software will be started. Some remote network port has been in a state of open, give hackers a network convenience. If the user doesn't forbid or mis-configure these software, the potential safety hazard will always exist.

2.3 Computer Virus

Computer virus mainly affect the safety of data inside the computer. It is in a computer program by the virus writers, write a piece of damage to a computer program has the data. Computer virus can cause a certain for both software and hardware of the computer, a computer virus can copy another group with the same destructive procedures or instructions. A computer virus has many characteristics, such as: infectious and parasitic, concealment, trigger, destructive, and so on. So, we should improve our vigilance against the computer virus invasion.

2.4 Network Hacking

Computer hackers is one of the most important risk factor for campus network security. For this factor, mainly, there are a lot of people on the network using computer system vulnerabilities in the illegal invasion of other people's computer system. It is very huge for the influence of the factors and the harm, even larger than the harm of the computer virus.

3. The Campus Network Security Precautions

We mentioned above a number of factors affecting the safety of the campus network, and hacking, for these problems and

factors, the school should set up a complete information network security system, the network security protection system should be a dynamic concept. In order to ensure the safety of network information attack, the network security guard system is based on such a principle and method: fusion of a variety of safety factor, such as anti-virus software, firewalls and security vulnerabilities detection tools, etc., and then create a variety of security of network protection barrier. This requires that the security system is not only to start from the security technology, but also start from the network security management. On the way of hacking, according to the network status and characteristics, the users can adopt the following techniques and methods:

3.1 Application of the Computer Firewall Technology

As we all know, firewall technology is one of the measures to protect the safety of campus network information, it is mainly refers to be protected built a safety barrier between the network and external network, the purpose is to prevent the illegal invasion of unpredictable, and potentially damaging. It is primarily through monitoring, limitation, modify data flow across the firewall, maximum internal blocking network structure, and operation information, internal network security and protection.

Computer mainly provide various network or firewall an information network security domain of the gateway, it can be according to certain security policies to control the information flow in and out of the web portal for certain, and firewall itself has a certain ability to resist the invasion. It is also the basic facilities to provide the campus network information security. Logically, a firewall is a separator, and a limiter, at the same time, it can effectively monitor and control activities between internal network and external network, to a certain extent to ensure the security of the network. And it is the key to researching and developing firewall subsystem to achieve high performance and scalability firewall. However, firewall, after all, is not everything, if there's a lot of Trojan attacks on it or a large number of hackers invaded it appears powerless. So, we should combine other technology to protect the security of campus network.

3.2 The Hacker Intrusion Detection Technology

What is a hacker intrusion detection technology? Usually in the sense of the hacker intrusion, detection technology mainly refers to the computer and computer network system operating status information flowing to intercept, and on the information analysis, and judgment. When users found been attacked or blocked, and record, alarm for abnormal behavior and response, so it is the method to minimum the losses of hacker intrusion behavior. The hacker intrusion detection system, meanwhile, also analysis the behavior of the user and the system can monitor and audit the system configuration and loopholes, identification of abnormal behavior and aggressive behavior, response to attack or abnormal behavior, etc.

Hacker intrusion detection systems are divided into four parts: the first part, the event generator, event generator is mainly provide the source of information flow record events. The second part, analyzer, events analyzer is found signs of intrusion analysis engine. The third part, the response unit, unit response is mainly response is based on the analysis results of the analysis engine. The fourth part, database, events database is mainly refers to store all kinds of intermediate and final data, it can be either a database can also be a common file.

Hacker intrusion detection system is currently the main measures to prevent hacking campus network, in this system, there are some problems and loopholes, we need to further improve it. Firewall technology and hacking are complementary relationship, a combination of both to prevent technology and being the very big enhancement, but also make the campus network defense capability get greatly increased. Firewall technology and hacker defense technology combined with each other, can foster strengths and circumvent weaknesses, give full play of their advantages, built a solid wall to the campus network.

3.3 Build A Web Site Cluster System

In addition, on the campus network, we can security manage the software platform, this way can reduce the difficulty and workload of network management, the campus every site has a separate domain name and the page style, and independent management background, able to information sharing between different sites. Now website construction is more convenient and smart, just need to find a platform that does not require any code, configuration directly, in this case, even if is professionals can also be set up and manage the website. General construction site use the template for separation and website information, convenient for revision in the future. Campus site safety issues related to the image of the whole school and teaching order, and also is an important part of the campus network security management. And the campus web site can be used in a static web technologies, thus can reduce the hackers and the Trojan invasion.

3.4 Establishment of Relevant System

In the process of campus network security management, adopting technical measures to prevent proved to be more important,

but the technical prevention alone is not enough. For example, many college students' Internet account got stolen, the reason is the student did not modify the password when using the Internet to use account and password are common password. It is easy to be stolen, campus network information center in consultation is with the student affairs office, some punishment in violation of the campus network security measures and measures. Through the propaganda of network information security, and thus for the policy.

4. The Myth of Campus Network Security Management

In the campus network, it is very important for the network management personnel need to set up the correct safety awareness. However, from the point of the present situation, the understanding of the campus network security management still exist many misunderstandings, mainly reflected in the following four aspects.

4.1 Did not Pay Attention to Hacking, and don't think Campus Network will become the Target of the Hacker Attack on

Now many campus network managers think that the something that hackers interested is not in the campus network, unlike financial trading website and big company website which with temptation of material things. In fact, this kind of understanding is not correct, first of all, the hacker must not only comes from external network, campus network users all the students are likely to be a hacker from the network promoter. Second, because of the campus network users is numerous. Therefore, hackers could attack campus network users, and the user as a root, then launch attacks on other users. Thus, campus network is also the risk of being attacked by hackers, must be taken seriously.

4.2 Network users did not need to install a Firewall

Campus network in most of the campus network users might think, hardware firewall already installed in the network center, then the network computer can not install a firewall, this understanding is not correct. A firewall defend against external merely, and in fact, 80% of the attacks are from the internal network. Therefore, internal users also have to install a firewall.

4.3 As long as Installed Anti-virus Software and Firewall, is absolutely Safe

Many users think that once installed anti-virus software and firewalls, the users can gain absolute security. There is no absolute safe, in fact, in the network anti-virus software and firewall can only to have some virus defence and attack. While, viruses and attacks are constantly updating. Therefore, if the defense software is not updated in time, it will be useless, even if, the last version have been guaranteed, it is still difficult to guarantee the new virus, Trojan invasion.

4.4 Installing the Patch can Guarantee System has no Holes

Most users, besides some network managers agree that, as long as the computer's system operation, patch could be sure that no loophole exists, and won't be hackers invaded. In fact, this idea is wrong. Because a loophole in the operating system itself may be growing, patch released by Microsoft are only Microsoft's own vulnerability, and hackers itself can be found through various methods before the invade attacks.

5. Conclusion

In general, the practice of the author, after such a long time, can fully realize and prevent campus network hacking, as hacking is not only a problem of network security, but also it will derive a lot of other problems, it may also be induced campus unstable factors. Therefore, schools can through relevant technology and measures for the administration, in ensure the safety of school teachers and students use network resources, at the same time, to test the unstable factors of network security and guard against, and actively developing some new network security protection technology. It will also research and analysis the campus network security and network security system development and plays a big role in promoting. At the same time, we also should constantly summarizes the successful experience and practices at work, to make our campus network more secure, more stable society.

References

[1] XUE, Fang-fang. (2009). Introduces the campus network security management, *Science and Technology Information* (*Scientific Research*), 2009, 13.

[2] HE, Yi-hui., WEI, Jie-qun. (2011). Basic strategy of campus network security management research, *Journal of Guangxi*

Radio and Television University, 2011, 1.

[3] TAN, Zhen. (2010). Hacking in the campus network security management and prevention , *Computer Security*, 2010, 10.

[4] TIAN, Hong-li., PAN, Wen-lin. (2009). Brief Introduction of Hacker, *Journal of Information Science and Technology*, 2009 (12) 100.

[5] CHEN, Wen-Fang. (2009). Based on the analysis of hacking means security system, *Computer Knowledge and Technology*, 2009, 5 (8) 1850-1854.

[6] JIN, Wei. (2010). An analysis of the present situation of network security in our country and its countermeasures, *Journal of Information and Computer*, 2010, (5) 82-83.

[7] XU, Yi-yun. (2011). Hacking techniques of analysis and detection, *Journal of Network Security Technology and Application*, 2011, (2) 14-16.