Research on Web Security Management in University Computer Laboratory

Qiu Zhongmei[1, a],Yin Shoujun[2, b]

[1]Electronic Information Training Base of Beijing Union University, Beijing, China

[2]Electronic Information Training Base of Beijing Union University, Beijing, China

[a]xxtzhongmei@buu.edu.cn,[b]ldtshoujun@buu.edu.cn

Keywords: University teaching practice, Computer laboratory, web security measures.

Abstract: With the rapid development of information technology and the Internet, online learning in university computer laboratory has become more and more popular, which spurs close connection between diverse teaching activities and computer. However, the web system in university computer laboratory tends to be vulnerable due to high risk caused by viruses as well as hardware and software breakouts. The research is devoted to the analysis of web security, management and preventing measures of problems in university computer laboratory, suggesting that measures including reinforced management and improved technology can ensure the efficient operation of computer laboratory in universities.

Introduction

With the birth of the Internet and information age, the dependence on computer can be seen in all businesses. As the major factories of leaders and specialists nationwide, universities have become increasingly important, especially their computer laboratories. The main tasks they undertake are as follows: management of computer operations in the laboratories and inferior security, supervision of technicians and students' working on computers, management of web security, management of hardware and software and many other multi-media applications. Among all these mentioned, web security is of greatest significance to administrators. Therefore, it has appeared on the top list for the sake of efficient management of web security in computer laboratory. It requires both the reliable hardware, support of web technology and the cooperation of administrators and students.

How web is used in university computer laboratory

Larger numbers of students admitted into universities result in the transfer to computer laboratories and the increase in numbers of computer laboratories. Various experiments take places in these places and thus many problems arise: basic courses and professional courses may have different hardware and software requirements for the same laboratory; courses of the same kind may have different requirements for software versions; sciences and arts courses require different software; the number of courses offered in computer laboratories is on the rise; the laboratories need to be open to all teachers and students, etc. All these factors may lead to the heavy burden and complexity of management, making it possible to have frequent hardware and software breakouts and high risk of being infected or hacked.

Potential danger in web security in university computer laboratory

Infection of Virus

In the computer laboratories, teachers show PPT, send materials to students or students submit assignments by using their U disks or mobile hard disks through which viruses find easy access into the computer and web of the laboratories. Virus, as it is called, spreads very quickly and often hides in a link, a picture or two-bar codes. It is hard to detect and troublesome for administrators. Usually, viruses attack system files and occupy web bandwidth and resources. By duplicating and reproducing, viruses always causes the breakdown of the network and some viruses may attack the server until it can’t work normally or loses large numbers of data.

System vulnerabilities

Different courses have different requirements of installation of several operation systems and application systems in the computer laboratories. It may lead to occupation of storage space. But the bugs in the computer system makes it easy for the network to be attacked. It includes: 1) the bugs in operation system --- Windows Server2008 is widely used in many universities and the users are mainly teachers and students. There are many management modules in the operation system, each with its own management system. The bug existing in the system means fault and viruses as well as illegal invaders can enter the laboratory network without difficulty. 2) the defects in the database --- it can cause lack of authentication, wrong input of data, modification and deletion of database information without authorization and backup data exposure, etc. 3) problems of setting firewall --- firewall is regarded as the first protective screen for office system when connected with exterior network while it doesn’t guarantee absolute security of the system because it can prevent the attack from the exterior network. If the attack comes from the interior network, however, the firewall becomes useless.

Weak security operation awareness of users

Many teachers and students who come to computer laboratories do not have strong security awareness and technological literacy. They randomly download or upload multitudes of documents and materials in the laboratories and some even upload their virus-infected documents onto the server, increasing the insecurity of the interior network. In addition, many often keep the computers running for very long time without powering-off, which causes the wastage and shortened life of computers.

Technical deficiencies of network security administrators

Network security administrators in most universities are not so technically qualified (some universities don’t have administrators) that there is no good management of the operation of interior network on campus. It is often ignored at first and nobody pays enough attention to the problems until it is too late.

Spread of immoral information

Some users would download or upload immoral information on the interior network. Although students have the ability to distinguish, this information still has negative influence on their physical and psychological development. Additionally, it also brings potential dangers to the security of campus culture and the network on campus.

Students’ inappropriate operation

Freshmen or beginners are more likely to have such kind of problems like:

Formatting：unintentional formatting hard disk as soft disk causing the loss of data in the hard disk and the failure of starting computer.

Modification of configuration：Students with certain level of computer skills tend to modify computer configuration but have no knowledge of how to restore. It always leads to the failure of starting computer or the wrong performance after startup.

Network breakout：There is network breakout due to problems of card or cable connection, students’ modification of configuration and identification.

Misusing deletion：Deleting computer system files causing the failure of starting computer.

Playing games：Students play games or use software harboring viruses. They hide the software so it can’t be detected or the viruses hidden in the software can’t be killed. It wastes a lot of resources in the hard disk.

Protective measures for the security of university computer laboratory

Analysis of the potential risks in university computer laboratory should be made to figure out protective measures so that network security of university computer laboratory can be ensured.

Establishment of network security system of university computer laboratory

Sound management system has an immediate effect on the information security of laboratory network. It can be taken as a “firewall” to protect regular teaching practice. First of all, regulations should be established for everyone to follow so that information security can be protected. Secondly, professional administrators should be assigned with clear duty instructions. Users (especially freshmen) receive technical training and the operation of campus network is supervised at a regular basis. It is necessary that users awareness if security and technical skills be improved and security operation instructions be established so that there will be less information leakage.

Reinforced training of professional staff

Professional network management staff receive training so that their technical skills can be improved, which is the precondition of network security. Meanwhile, advanced network monitoring software can help scan and supervise visit data so that the potential security risks can be detected and dealt with immediately.

Setting different database access rights according to different administrative privileges

Enhance the division of rights and management among users, different users having different data levels and authority. Manage and control effectively the visit levels of university database, which can help monitor the legal using information by users of different levels. In this way, there will be no illegal modification of information or the failure in system operation. Make sure data can be sent, stored and applied safely via encryption, which is classified into data transmission encryption, data storage encryption, data module encryption, data integrity authentication and key management.

Construct system security protection net

Due to the complexity of teaching system in the computer laboratory, an effective firewall system should be constructed to detect and repair system vulnerability, clean and maintenance computer system regularly, specify e-mail attachment format and provide barriers to filter suspicious files. Close network sharing to prevent the likely illegal invasion. Monitor the port in the system and close some unnecessary ports to enhance regulation and management of administrator accounts. change the password or increase the complexity of the password to reduce the likeliness of decoding administrator access. Optimize the security of server, adopt the server with higher protection levels, clear and monitor network visits and filter malicious plug-in. Keep IP address safe to avoid illegal attack from the address, stealing of data or other threat on the network security.

Divide and manage areas where campus network is used

Divide the areas into safe area and unsafe area according to the importance of information security in campus network. In the safe area, visits are allowed only in specific areas of network and visitors’ identity will be registered, personal information checked. Effective management and control makes the safety degree in the safe area the highest (such as experiment data). On the other hand, the unsafe area refers to information exchange platform where the transmission of information is scattered and irregular. Therefore, it is highly recommended that the access path, the format of uploading and downloading materials as well as the scanning of materials be specified. What is worth mentioning is even in the unsafe area visitors’ identify should be monitored, personal information checked, which is helpful in supervising students’ use of the network.

Improve computer literacy and application level of both teachers and students

Provide application security training for teachers and students and clarify their purposes of using university computers. Organize activities such as lectures and encourage students with strong interest to participate in the maintenance of university network security. Their active participation will make great contributions to the desired security of campus network.

Conclusion

Computer laboratory network security management is a systematic project, which needs the cooperation of techniques, regulations and users for a comprehensive protective mechanism. Only by establishing a good laboratory network environment can teaching practice be ensured and teaching efficiency in the laboratory be improved. Therefore, students will have a better network environment in which they can develop positive goals and values in life.

References

[1] Sun Jianzhi. Computer Network Application Technology Course. Beijing, Tsinghua University Press. 2006

[2] Yang Yunjiang. Computer and Network Safety Application Technology. Beijing, Tsinghua University Press. 2007

[3] Yang Fei. Analysis on the Management and Maintenance of Computer Laboratory in Colleges and Universities. Journal of Chifeng University (Natural Science) , 2009 (10)

[4] Ding Luai, Management and Personnel Training of Nonlinear Editing Laboratory in Colleges and Universities. Journal of Hunan Mass Media Vocational Technical College. 2006 (2)

[5] Cai Jinhua. Discussion on the Management Mode of Laboratory in Colleges and Universities. Science and Technology Wind. 2011 (7)

[6] Hu Haijun. Research on Network Security Technology. Journal of Wuhan University. 2010.01)

[7] Lu Tongtian. On the Security of Campus Network Construction and Corresponding Strategies. Computer Application. 2008. 10