Prevention Strategy of Computer Security Problems in Network Times

Wei Zhou
Shanghai University of Engineering Science, Shanghai, 201620, China

Keywords: Computer network, network security, attack, prevention strategy.

Abstract: In network times, information can be randomly exchanged and connected, thus bringing network security problems as well as convenience for people's life and work. Therefore, it is necessary to find a method to avoid influence of computer network security to application with the use of computer network technology. Network security prevention techniques, including firewall and password setting, play an important role in safe operation of computer network.

1 INTRODUCTION

In network times, fast information communication promotes the use of information resources and progress of society. Computer network has been an important tool for modern life and work. Network security problems, including disclosure and damage of important information, have threatened network security, thus bringing huge losses to the users. Some methods, such as protocol isolation technique and firewall, can be used to protect computer network (Nie Mengjie, 2014). In addition, scientific cognition of computer network security and effective use of prevention technology can minimize network security threats.

2 COMPUTER SECURITY ANALYSIS IN NETWORK TIMES

2.1 Computer security in network times

Network is a free information space. Not all the problems can be solved by prevention of computer network. E.g., identification can determine user identity rather than truth and information transmission security between users. Virus defense of computer network can prevent damages from computer virus. However, it cannot perform identification and determine user identity in network. With the development of network, computer network security, including individual privacy and state secret, has been one of key problems of computer fields. Firstly, computer network security affects national safety and social stability. E.g., the terrorists apply network to make false information and political intrigue. Secondly, computer network security can cause great threats to economic development. E.g., hacker attack is used to transmit virus, thus damaging regular service of enterprises and individual users and causing economy and property losses (Liu Yanqing, 2012). Thirdly, with the popularization of network, the criminal activities become more and more rampant in hidden space, thus affecting social stability as well as personnel and property security. In conclusion, computer security is threatened. Acquisition, control and use of information are affected by network communication, thus causing great influence to individuals, enterprises, countries and society. Consequently, with the development of computer technology and network, computer network security is getting more and more attention.

2.2 Computer attack analysis in network times

The largest problem of computer network security is computer attack in network times. The hacker can steal information resources, spread false information and destroy computer program by using computer attack, thus causing serious results and bad social influence (Zhang Yanping, 2014). Computer attack

229

Zhou W.
Prevention Strategy of Computer Security Problems in Network Times.
DOI: 10.5220/0006447802290231
In *ISME 2016 - Information Science and Management Engineering IV (ISME 2016)*, pages 229-231
ISBN: 978-989-758-208-0

contains active and passive behavior. The former can destroy important computer information by various methods; the latter can intercept and decode secret computer information. In general, computer attack is presented by change, damage and steal of information. The common attack methods are as follows.

(1) Forged IP and MAC addresses can result in network interruption, communication block or indirect invasion.

(2) The attack, started by vulnerability of development spot, can cause unusual software operation and system crash.

(3) Trojan horse program and virus are usually used to start attack by the hacker. Trojan horse program has characteristics including concealment, latency, ignitionability and destruction. Once attacked, the host will be controlled and destroyed, thus causing disclosure of important information. Virus can be spread through hard, soft and light disks as well as network operations including document copy and transmission, thus causing damage of system documents and decrease of working efficiency.

(4) With characteristic of concealment, olfactory detector can intercept information destination from network interface and obtain user name and password by analysis of information, thus causing network security threats. Scan attack is to attack the host using computer network vulnerability and obtain host information.

As the important means by which criminals attack network, these attack methods are prevention targets of network security. Computer network has characteristics such as open, wide distribution and resource sharing. The hacker can perform hostile attack behaviors including data interception, correction and damage, thus causing hidden danger of computer network application. At present, the best method to deal with all kinds of attack is prevention because of virtual network and difficult user identification.

2.3 Factors causing network security problems

Factors that cause computer network security problems in network times are as follows. Firstly, damage of computer hardware such as hard disk will cause system crash. Secondly, there is great security hidden danger in network system. E.g., open network provides convenience for hacker to attack. Besides, hackers can disguise IP address to perform network attack based on TCP/IP protocol. Thirdly, the defect and vulnerability of computer software, as the target of hacker attack, can cause operational obstacles and security problems. Fourthly, most operators are short of security prevention consciousness of computer network application, although with popular computer network. E.g., simple user passwords, such as single repeat numbers and birth dates, are easily decoded, thus causing hidden network security danger. In addition, operation miss can result in system crack and document loss. Fifthly, some network attacks are caused by curiosity and desire, while other attacks are performed with purpose. E.g., serious security problems can be caused by stealing information and password of objective computer, as well as activities including commercial crimes, religious dissemination, spread of harmful information and program damage. Sixthly, Network is an open environment with a large amount of information at different levels. Great benefit of network crimes and deficiency of computer network escalate network security problems. With the popularization of network security, various measurements are conducted to ensure security and stable operation of computer network.

3 PREVENTION STRATEGY OF NETWORK SECURITY

3.1 Prevention technology of network security

Prevention technology of network security is to prevent and clear hidden danger in network operation. At present, protocol isolation, firewall and encryption techniques are widely used.

(1) Internal network is insulated from the rest to form a protocol by protocol isolation technique. The two hosts are connected with network, serial, parallel and USB interfaces and bound by specialized protocol. If network is invaded, dangerous information and file packets will be isolated by protocol for the purpose of prevention. Under specialized protocol, operators can hardly enter internal network for invasion through external network, thus making a positive significance in internal network protection.

(2) A barrier between internal and external network can control information communication of different networks by filtration and detection of firewall technique. Then, internal network can be prevented from bad access of external users.

230

Prevention Strategy of Computer Security Problems in Network Times

(3) Although convenient and simple, encryption technique can be easily attacked with finite security. Mixed encryption technique applies hardware and software encryption methods to build connection between internal and external network on basis of mutual recognition. By this technique, information transmission can be protected.

(4) After scanning computer for inspection, we can find the attack situation by vulnerability and carry out system repair using patch. The largest advantage of vulnerability scanning technology is to find and monitor the vulnerability of system security within a short time.

3.2 Strategy analysis of computer network security prevention

Computer network users have paid great attention to the heavy losses caused by computer security problems. Prevention of network security is improved. Firstly, effective techniques such as protocol isolation and firewall are used to reduce security risk of computer network. E.g., in firewall application, the firewall logs are regularly kept and examined to find attack behaviors and bad internet records, thus eliminating serious security threat to computer application. Secondly, antivirus software, system reinstallation and disk formatting are used for worm elimination in infection zone. Meanwhile, updates and remote killing virus technology of antivirus software should be emphasized to ensure security and operation of computer network. Thirdly, unknown mobile HD and U disk should not be used to avoid virus transmission by connection. After worm elimination, the external hardware can be read to ensure computer application security. Fourthly, comprehensive computer security education and cultivation are conducted to intensify security consciousness and legal and moral idea, thus effectively reducing security risk of computer network. E.g., complicated login account and password should be used to ensure security. Different accounts in the same host can maximize security prevention and minimize the losses caused by network attack. The user password should be regularly updated. Numbers, letters and special symbols are used to improve security of password. Fifthly, security levels are set to intensify account management according to differences of user levels, thus avoiding security issues including account leakage. Sixthly, unified management of computer hardware, including temperature and humidity of machine rooms as well as dust and static electricity prevention, is emphasized for computer operation security. Seventhly, users should make regular back-up copies of computer system and documents for recovery. Effective remedy will be performed to minimize network losses and promote computer network application when there are problems such as hardware breakdown, operation fault and attack.

4 CONCLUSIONS

Computer network and security prevention techniques are methods which cannot replace human thinking and operation. In network times, computer security prevention should intensify security, legal and moral consciousness of operators and regulate network application to ensure operation security and stability.

ACKNOWLEDGEMENT

The work was supported by Research and Application of High-end Large-scale PLC Automation System, Subproject of The National High Technology Research and Development Program of China (No: 2013AA040302).

REFERENCES

Liu Yanqing, Development and Security Prevention Strategy of Computer Network Technology, *Digital Technology and Application*, 2012(05): 179-179.

Nie Mengjie, Computer Network Communication Security and Its Prevention Strategy, *Chinese Electronic Commerce*, 2014(13): 34-35.

Zhang Yanping, Computer Network Communication Security and Its Prevention Strategy, *Digital Technology and Application*, 2014(05): 198-198.

231