

Research of the Main Risk in Computer Network Security and Its Management Measures

Qing Yang^{1, a}

¹ Zhengzhou University, School of Information Engineering, Zhengzhou, Henan, 450001

^a email

Keywords: Computer; Network Security; Risks; Management Measures

Abstract. With the popularization and application of Internet technology, it has brought great opportunities, challenges and has a significant change to various industries, which entered the Internet age. Computer network is double-edged sword, bringing convenience to people at the same time there are some security risks, seriously affecting the information security of the Internet Age. Therefore, this article is to explore the main computer network security risks and to lower the risks of computer security management measures, thus providing an important guarantee for computer network security.

Introduction

For now, computer network technology has been applied in all walks of life and work as well as entertainment people are of great significance and role of the computer network is a double-edged sword, it gave rise to great the convenient, due to its characteristics of openness and freedom, but also led to the security risks of computer networks, this security risk to some extent, will give users a tremendous loss. In such an environment background, how to manage and troubleshoot computer networks evils become an important problem in computer networks.

A Major Hazard in Computer Network Security

The main risk at this stage, computer network security is the following. First, the impact of natural factors causing a computer network security risks. Natural factors mainly refers to unpredictable and irreversible accidents, such as earthquakes and tsunamis and other natural disasters destroy the land or undersea cable, causing the computer to a network server power outages, formed a computer network security risks. Once the natural factors cause great losses, it is difficult to predict and prevent, the occurrence of natural factors, but the probability is very low, seldom the case. Secondly, the impact of human factors caused the computer network security risks. In the current computer network security, the human factor is more common security problems, and the frequency with respect to the high natural many factors, mainly refers to human intrusion on the computer network and the destruction, such as cutting the cable and cable, hacker attacks and other computer network security risks, hacker attacks can be divided into non-destructive and destructive attack attack categories. Non-destructive attack to disrupt the general operation of the system, not the system data theft, denial of service attacks commonly used information, or bombs, and devastating attacks based invade someone else's computer system, theft of confidential information system, the destruction of the target system for the purpose of data .Finally, the network protocol and operating system vulnerabilities caused by computer network security risks. It includes the network operating system vulnerability, security flaws TCP/IP protocol, the database management system security vulnerabilities, network resource sharing, data communications, computer viruses and the like.

Computer Network Security Management Measures

Firewall technology refers to an internal network and the public access network separate from the computer network security means, in essence, is a kind of firewall technology isolation technology to intranets and extranets effectively separated so that the user can accord to their needs to computer

network. Firewall access control network communications. Allows authorized network users access the internal network, and unauthorized network users shut out, so as to effectively prevent hacker attacks and invasion of the internal network, internal network information to avoid change and the destruction of copies and other network attacks. In the configuration of the firewall, to adhere to the principles on the basis of simple basic configuration of the firewall on both inside and outside and in-depth principle and the principle of simple firewall designed to reduce the probability of error, will help ensure the firewall security features, firewall management to improve the reliability and convenience nature and effectiveness. Depth principle refers to the firewall settings to take comprehensive and multi-layered system of defense in depth strategy, facilitate coordination and strengthen the various aspects of the configuration. On the one hand you want to design a multi-level Firewall Internet firewalls and departmental boundaries boundary firewalls and host firewall combined together to form a multi-layered network security defense. On the other hand should intrusion detection and network encryption and other security measures and virus killing reasonable combined to form a multi-layer security system of computer networks. Both inside and outside the main principle is in the process of using a computer network, so that no foreign anti-anti within, in terms of internal protection can use intrusion detection and prevention, and virus killing the host computer network security measures.

Computer network viruses to the computer network security is a big threat to human factors mainly refers to the code inserted in a computer program function or destruction of computer data, computer network using a huge impact, and can automatically copy the computer program instructions code. Computer viruses spread, concealment, infectious, latent, excitability, performance or destructive. Its period is the "development of - infectious period - latency - attack - found - A digestion period - the demise of" process. Therefore, for the virus is a computer network in addition to the use of firewall technology, but also to improve their fighting capabilities of computer networks, the use of security software and processing network killing virus, to update and detection killing the network system, the timely introduction of advanced network virus killing technology, such as virtual machine technology heuristic scanning software NOD32 and Dr.Web, as well as behavior-based analysis of micro-point active defense software technology initiative.

Computer security awareness of network users on a computer network security risks prevention has a very important role, first of all, a computer network users the ability to use computer networks to enhance the quality and use, to avoid possible security risks because of personal computer network resulting from the incorrect use, bring greater losses. Secondly, users of computer networks to strengthen the routine maintenance and preventive measures, can take advantage of the way to set a password, the rational management of login password. Hydrogen gas and firewall security checks, is to update the computer security software, the importance of security and management software for inspection and sign the personal information in public places, to improve their awareness of the use of computer network security for the safe use of computer networks to provide an important guarantee.

Conclusion:

Based on the main computer network security risk analysis and management measures, this paper explains computer network about its characteristics of openness and freedom, leading to computer network security risks, such security risk to some extent and will give computer Internet users huge losses. Therefore, this article is mainly based on the computer network of natural and human factors, and network protocols and computer network security risks caused by the operating system vulnerabilities, proposed to strengthen the computer network security firewall technology to improve the capacity of the computer network killing viruses, computer network users to improve security awareness and other preventive measures computer network security risks, thereby providing an important guarantee for the safe use of computer networks.

References

- [1] Wu Suxia. Computer network security analysis of major risks and management measures [J]. *Computer Programming Skills & Maintenance*, 2014, 12: 115-116 125.
- [2] Kong Honghai. main risk management measures and computer network security analysis [J]. *Network Security Technology and Application*, 2014, 11: 222-223.
- [3] Shi Linghua, Zhang Yufeng. Main risk management measures and computer network security analysis [J]. *Jiamusi Vocational College*, 2015, 08: 418 + 420.
- [4] Sun Hailing. Computer network security risks, and effectively safeguard measures analysis [J]. *Information and Computer (Theory Edition)*, 2014, 26 (9): 292-293.