Computer Network System Security Management and Maintenance Strategy

Chen Chen¹*, Zhang Hui²

¹Jiangsu college of tourism, China, 225000
²Guangling College of Yangzhou University, China, 225009

*Corresponding author e-mail: jslycc@qq.com

Abstract. Computer network system security management has always been an important part of computer management. In the process of enterprises using computers, network security has always been one of the important factors affecting the security and stable development of enterprises. Therefore, strengthening computer network system security management has always been one of the important tasks for enterprise development. This article mainly analyzes the influencing factors of computer network system security and proposes corresponding security management strategies in order to build a comprehensive computer network security defense system and promote the enterprise computer network environment to achieve more security and stability.

Keywords: Computer Network System, Security Management, Maintenance Strategy

1. Introduction
Information management has become the mainstream management form of modern enterprises. Ensuring the stability and security of computer network systems has become one of the important tasks for the stable development of enterprises [1]. There are many security risks in enterprise computer network systems, including internal system problems and hardware. Deficiencies also include external attacks and threats. These are the reasons for the formation of computer network security risks. To comprehensively improve the construction of computer network security and achieve complete and stable information services, enterprises should establish a comprehensive computer network security defense system [2-3].

The comprehensive development of computer network technology not only drives the development of science and technology in China, but also breaks the constraints of time and space, and maximizes the management level and efficiency of enterprises [4]. However, if you rely too much on computer...
networks and computer systems for management work, once the computer network or computer system crashes, it will cause incalculable losses to the enterprise [5-6]. Therefore, relevant staff must strengthen comprehensively the importance of computer network security management and operation and maintenance, and adopt a series of scientific and effective methods to continuously improve the security and reliability of computer networks to ensure to ensure that the computer network can bring into play to the greatest extent possible in the actual business management.

2. Factors Influencing Computer Network Security

2.1. Internal system problems
Internal system problems in enterprises are generally caused by improper or incorrect operation of computers. Network failures caused by such internal operation problems generally belong to internal failures, and most often occur in small and medium-sized enterprises. Insufficient ability of computer operation and information management and use, often leading to some operation errors, which will cause problems such as network instability or network interruption. At this time, the security impact caused by the poor operation of the internal system generally belongs to relatively simple and easy-to-handle network failures.

2.2. Hardware
As a major hardware component of an information system, a computer is an auxiliary tool. It is composed of multiple parts, and the components work closely together to form an overall computer working system. Therefore, if any one of the components has a problem, it will affect the normal work of the entire computer. Damage to computer components is mainly caused by errors in network specifications and network connections or physical damage to the lines. These are unpredictable but will threaten the stability and normal working of the computer system.

Of course, hardware problems, in addition to computer component problems, also exist in the overall management and maintenance of the information terminal equipment room of the enterprise. As the core part of the enterprise information system, the equipment room is responsible for the management and output of enterprise information. The existing problems and damages will also cause large-scale program problems within the enterprise. This is also one of the issues worthy of attention in computer hardware.

2.3. External threats
External threats generally refer to external malicious attacks. Common computer viruses and hacking are the main ways of external threats, as shown in Figure 1. Generally, enterprise systems are built on the basis of mutual trust. Therefore, when the system faces external hidden dangers, its defense ability is very weak, which creates an opportunity for computer hackers. This is a threat and risk from weak prevention awareness and a bad network environment. In addition, the design of computer operating procedures is also an application with many vulnerabilities. Moreover, the methods and channels of hacking and virus infection are becoming more and more diversified. The endless emergence and continuous strengthening of hacking techniques are not very defensible, and they have become chief enemy of the computer system security. These external threats and attacks are
caused by a bad network environment. It is particularly important to strengthen the security and prevention capabilities of applications.

3. Computer network security countermeasures

3.1. Technical level
On the technical level, corresponding countermeasures can be taken against the security threats of a wide range of computer network systems. First, setting up a firewall is a basic measure for general enterprises to carry out network defense, and it is also an important measure for maintaining network security. The firewall is generally used for control of access scale, blocking inaccessible IPs, and allowing IPs that are allowed to access, to effectively avoid intrusions and attacks from unsecure IP and software. Second, it is also a very effective way to set up an intrusion detection system in a critical part of the corporate network. It detects incoming abnormal lines and sends out alarm messages, which not only can detect network intrusions and attacks, but can also detect attacks between intranets of the enterprise. To a large extent, it makes up for the shortcomings and functional defects of the firewall, and better defends enterprises against network attacks.

In addition to the above-mentioned system protection, there is also a related physical isolation and information exchange system. This system can isolate the VLANs that affect the security of the local area network, preventing the transmission of information between it and the internal and external networks of the enterprise. The technical effect of such a system is better than firewalls and intrusion detection systems. In operating system security, many ports that are not needed can be closed. For virus protection, a combination of antivirus software and system detection software is often used. The overall system virus is checked and killed, and the vulnerability is scanned to ensure the security of the network operation at all times, to ensure that the system can run safely, and the system vulnerabilities...
can be updated and compensated in a timely manner. The mobile devices that have not received security certification within the company are monitored, and operations that violate the relevant system of corporate network use is strictly controlled. The illegal monitoring devices are isolated and more network isolation are carried out to ensure network security.

The computer network data transmission rate is shown in formula (1):

$$R=1/T\times \log_2^N(bps)$$  \hspace{1cm} (1)

$T$ is the width of a digital pulse signal (full-width code case) or repetition period (zero-code case). The unit is second.

The number of symbols transmitted through the channel per unit time, the calculation formula is shown in equation (2):

$$B=1/T$$  \hspace{1cm} (2)

The correspondence between the computer network modulation rate and the data transmission rate is shown in equation (3):

$$R=B\times \log_2^N(bps)$$  \hspace{1cm} (3)

Where $R$ is the modulation rate.

In addition to the prevention methods on the above systems and the protection of viruses and malicious attacks through the improvement of network anti-virus capabilities, It is also necessary to develop and improve a highly secure network operating system, to develop the more humane and highly secure network system operations, and to achieve a more complete cooperation between system software and hardware.

3.2. Management level

In addition to the improvement of the technical level, the security management of computer network systems must also strengthen the construction of the management level. The strength of the laws and regulations on computer security protection is also very important. Management can ensure the better realization of computer network security effects. The security management of computer networks must first establish a security management organization, strengthen computer network legislation and law enforcement management, carry out corresponding computer user safety education, improve computer users' moral and security awareness, prevent the occurrence of computer crimes, but also to better prevent computer hacker attacks, and strengthening of computer network security management capabilities is also very important. Education and popularization of computer security law, crime law, data protection law, etc. It is also very important. In addition to maintaining the security of computer networks and systems, and conducting more computer security education to better use by users. Relevant maintenance and management systems should also be established to strictly manage and control the use of computers, and there should be special security protection programs for data, computer rooms, etc., and strict division of labor management and hierarchical management systems. The use of computers in the enterprise is strictly controlled to ensure the comprehensive security of the computer network.
4. Establishment of computer network security defence system

The best way for an enterprise to strengthen its computer network security management ability is to establish a computer network security defense system. A perfect security management system is an effective means and measure to ensure computer network security. Starting from the overall concept, the overall supervision and control of the enterprise computer network system can be conducted to achieve the best results. To achieve comprehensive security maintenance of the computer network system, it is necessary to establish a comprehensive network security system.

The establishment of a computer network security defense system is the future trend of the development of enterprise informatization and an important measure for the creation of a computer network security environment. To achieve informationization and modern management, an enterprise must establish a comprehensive computer network security protection system to ensure computers the network environment is comprehensively monitored and managed to prevent the emergence of security risks.

There are many noteworthy aspects of the establishment of a computer network security defense system. The corresponding computer system should be designed in accordance with the actual situation of the enterprise to build an information security and network defense system that suits the needs of the enterprise. What needs to be paid attention to when establishing a security defense system is specifically discussed and introduced as follows: First, the enterprise network should be partitioned accordingly. For example, the production private network of the enterprise should be isolated from other private networks of the enterprise. This is to prevent one of the private networks from being infected or attacked by a virus. Other private networks will not be affected and implicated to minimize the possible damage caused by external attacks and threats. Secondly, in the establishment of network defense systems, attention should also be paid to the classification of corporate information security levels. Important information should be specially set. The division of different importance levels of information is to set different information usage rights, to provide more security protection for important information, and to use corresponding security areas to manage security of information of different security levels. At the same time, in the construction of computer network security systems, the corresponding firewall technology protection measures such as physical isolation and intrusion detection must be used consistently to ensure the normal operation of the enterprise system. Moreover, corresponding rules and regulations should also be formulated for the internal network traffic of the enterprise, and the use of traffic should be restricted to ensure the smooth and stable internal network of the enterprise. Finally, the internal system use of the enterprise should be appropriately authorized and controlled. Only formal authorization management can ensure the internal information of the enterprise. Use more security, the internal system of the enterprise can run more normally and stably.

In a word, in order to realize the establishment of enterprise computer network security system and strengthen the management ability of enterprise network security, in addition to the comprehensive management of computer network protection software and hardware facilities, and the realization of technical management and administrative capital reconciliation, it is also necessary to establish a layered network protection system prevention system. The enterprise's network security system should be structured to form a complete structure, achieving the perfect coordination from the core to all levels., as shown in Figure 2, strict internal and external restrictions and the perfect implementation of
system protection measures, Strengthen the construction of the enterprise's hierarchical network protection mechanism, isolate the corporate network from the internal network and the external network, isolate the private network, set the security level, etc., and combine advanced network protection technology and perfect computer network management measures. Carry out hierarchical and standardized management of enterprise computer networks to achieve a comprehensive improvement in the safety factor of computer network security systems.

![Network security protection architecture](image)

**Figure 2.** Computer network security protection system.

5. Conclusions
With the continuous development of informatization, computer network system security has become one of the important management tasks for enterprise development. In the face of many system security threats from internal and external sources, to strengthen the ability of enterprise computer network security management, it is necessary to take corresponding countermeasures at the technical level and the management level, and establish a comprehensive computer network security defense system. to achieve comprehensive computer network security for the enterprise and comprehensively improve the level and level of enterprise informationization.

Following Work
Intellectualization opens another door for the security of computer network system. Enterprises can grasp the specified network information according to the plan by deploying the network equipment supporting programmable and cooperating with computer programming language (such as Python etc.). Through the analysis and comparison of key information such as transmission rate and packet loss rate, they can judge the current network condition intelligently. During the working time, they can The visual interface feeds back to the system administrator, which can send the fault information to
the intelligent device of the administrator during non working time to realize all-weather network monitoring. Next, the author plans to design a set of universal network equipment operation and maintenance code, study and judge the common faults in daily work, and dynamically send execution instructions to network equipment through the pre-set black-and-white list in the program, so as to ensure the normal operation of enterprise network system. In the follow-up operation and maintenance, the strategy of computer learning is involved to improve the diagnosis and debugging of network faults, so as to further stabilize the operation of the whole network of the enterprise.

References
[1] Yiran Wang. Food Information Management and Security Strategy of Computer Network[J]. Advance Journal of Food Science & Technology, 2016, 11(12):792-794.
[2] Yoshizumi Serizawa, Tatsuji Tanaka, Hiroyuki Yusa. Verification of Distributed Real-Time Computer Network Architecture Associated With Off-The-Shelf and Dedicated Technologies[J]. IEEE Transactions on Power Delivery, 2017, 24(3):1206-1217.
[3] Deccio, Casey. Maintenance, mishaps and mending in deployments of the domain name system security extensions (DNSSEC)[J]. International Journal of Critical Infrastructure Protection, 2018, 5(2):98-103.
[4] Chang H , Kang J , Na Y . The Security Management Model for Small Organization in Intelligence All-Things Environment[J]. Lecture Notes in Electrical Engineering, 2017, 107(1):69-75.
[5] Lu, Hengbo, Xu, Haiming. Contradictions Encountered in Running Large Chinese Sports Venues and Contradiction Management[J]. International Journal of the History of Sport, 2017, 32(8):1109-1114.
[6] Zegzhda, P. D, Kalinin, M. O. Automatic security management of computer systems[J]. Automatic Control & Computer Sciences, 2018,49(8):665-672.