Academic Journal of Engineering and Technology Science
ISSN 2616-5667 Vol.2, Issue 5: 77-83, DOI: 10.25236/AJETS.2019.020509

Application Analysis of Computer Information Management Technology in Network Security

Yan Li

Jingdezhen Ceramic Institute,Jingdezhen 333403, China

ABSTRACT: *With the continuous improvement of China's science and technology, computer network security is one of the hidden dangers of computer systems. It has relative importance and function. This article takes network security as an example, discusses the current computer network security issues, proposes preventive measures based on the status quo and security needs, analyzes the application of computer information management technology in network security, and provides relevant academic research and computer system security protection in China. reference.*

KEYWORDS: *Computer; Network security; Development application; Information management*

1. Introduction

Computer information management technology is one of the important means of current network security construction and security assurance, and its important impact is self-evident. However, at this stage, there is relatively little research on the application of computer information management technology in network security. Based on the current situation of this problem, effective methods are required to analyze it, such as virus prevention and optimization technology, application of identity verification technology, and system management and maintenance. The application of technology, the application of information encryption technology, the more advanced virus prevention technology, and the more intelligent network security system, etc. This study has a very important theoretical significance in analyzing the application of computer information management technology in network security.

ISSN 2616-5667 Vol.2, Issue 5: 77-83, DOI: 10.25236/AJETS.2019.020509

2. The significance of network security

With the continuous innovation of China's current network security technology, how to consolidate it has been one of the research topics of many scholars and experts. This chapter analyzes the network information security precautions of hospital computer systems and clarifies their importance. Among them, the issue of network security is very important for the protection of its related fields and industries. At present, China's network information technology continues to be widely applied. Many industries use computer management models to conduct external and business development and internal control management. It has a greater impact on them, mainly including data leakage, confidential theft, and file loss. These will cause great losses to the development of the industry and the survival of enterprises. Therefore, the importance of network security lies in the effective protection of industry information data. In addition, if there are network security problems, it will also have a lot of impacts, that is, third-party damage, such as bank network problems, which will affect the interests of depositors; security problems in the stock market network, which will prevent customers from fast trading. Therefore, it is important to strengthen effective prevention of computer network security.

3. There are major risks in current cyber security

3.1 Computer viruses affect network security

Computer virus is a kind of continuous management system destruction material, which has always been a key threat to computer network security in the world and even in China. Computer viruses will continue to innovate and develop as their technology improves. At present, computer viruses have hidden characteristics, replication characteristics, fast characteristics, and public characteristics. Under normal circumstances, it will not be rapidly developed and effectively controlled. Computer viruses are mostly file-based interventions, which perform rapid retests and infections. They reproduce and rapidly replicate in computer systems, and their infection speed is extremely fast. As a result, the computer management system was quickly paralyzed, such as data loss, black screen, and even the entire system crashed. Of course, computer systems and management software will not run properly. It will seriously affect the company's financial data, treatment technology, personnel files, and medical records. After a risk crisis occurs, these data, information, etc. will be lost, which will also have a great impact on the daily management and operation guarantee of the enterprise. Therefore, from the perspective of the impact of computer viruses, it is very important to effectively prevent and resolve them [1].

ISSN 2616-5667 Vol.2, Issue 5: 77-83, DOI: 10.25236/AJETS.2019.020509

3.2 Hacker invasion affects network security

Hacker intrusion also has certain harmful effects on network security, and has serious illegal and criminal nature. Hackers can easily cause serious damage to computer management systems. For example, the data and materials in the computer management system are stolen. At the same time, hacker attacks generally start from some kind of interest and purpose, which leads to the theft of core secrets of commercial enterprises, which are all caused by hacking. After analysis, it is found that hackers generally use illegal method implantation and Trojan horse implantation methods to destroy computer management systems, that is, firewalls, etc. [2]. It can quickly cause the firewall to crash, and many preventive softwares are not obvious in their preventive effect, let alone prevent them from comprehensive prevention. Therefore, the relevant agencies and departments should be based on the long-term strategic development level to comprehensively control and prevent hackers from malicious invasion.

3.3 Lack of maintenance affects network security

Most managers lack the awareness of network security maintenance and cannot clearly understand the guarantee role of network security system maintenance. The lack of in-depth control and system maintenance in daily computer system management. Many managers often think that computer information management technology is highly practical, and many problems are mostly small matters and small influences. Inability to carry out in-depth maintenance of daily software and program management, which leads to risk loopholes in computer information management systems due to lack of maintenance, which mainly include slow update of protection walls, untimely download of vulnerability patches, irregular maintenance of systems, and virus detection. All have a greater impact on network system security. Therefore, managers fully recognize the importance of management, maintenance, and prevention to network security, and start with small issues to comprehensively improve network system management and maintenance [2].

4. The application analysis of computer information management technology

Network security technology is not a one-sided, simple process, but a more scientific and reasonable system layout. It mainly includes firewall technology, gateway monitoring technology, identity verification technology, virus prevention technology, vulnerability and Trojan horse processing technology, etc., as follows:

4.1 Virus prevention and optimization technology

According to the impact of computer viruses on network security, we should start from the prevention technology level and design and layout them according to

ISSN 2616-5667 Vol.2, Issue 5: 77-83, DOI: 10.25236/AJETS.2019.020509

actual conditions. Strengthen the prevention and control of computer viruses, as follows: First, update the virus database in the system in a timely manner, and update the antivirus software quickly, so that the virus software can identify the virus type, type, format, etc. in a timely manner, and Quick killing [3]. Second, computer managers need to download new virus programs and update the virus patches in a timely and fast manner to ensure the functionality of the virus software and quickly detect and kill popular new viruses. Third, we must do a good job of copying and backing up relevant important file data to be foolproof.

4.2 The application of identity verification technology

Identity verification technology is an important part of computer information management technology. Generally, it mainly deals with hackers and Trojan horses. The current hacking rate is high. Therefore, network security should be effectively prevented. The identity verification technology mainly optimizes the internal network system as follows: First, regularly and regularly upgrade the network security firewall, download vulnerability patches, etc., and comprehensively detect the vulnerability. Of course, it is necessary to make reasonable use of the authentication technology, and in the process, it is necessary to set the computer access permissions, mainly the gateway entry settings, etc. [4]. Visitors must pass key authentication and identity verification before external programs and access applications can enter the network system. In addition, the general process of identity authentication technology is system interface, web page login, information application, etc., to strictly verify the true identity information of the visitor, so as to form an identity detection barrier between the registrant and the applicant [4]. Second, computer gateways, access ports, etc. need to be encrypted to detect whether there are security holes. If gateway failures and illegal access intrusions are discovered, they should be handled in a timely manner. It is recommended to choose Master Lu, Zemin Anti-Virus Surveillance, 360 Security Guard, etc. Third, we must do a good job of backing up relevant important file data and sharing platform data, so as to be foolproof.

4.3 The application of system management and maintenance technology

Network system management and maintenance are also critical to security. Therefore, from the perspective of internal management and scheduled maintenance, the potential safety hazards should be checked. As follows: First, clarify the responsibilities of computer network security managers, that is, job responsibilities. Improve the degree of management staff's attention to network security, and refine and quantify network security management and maintenance. Strictly monitor the existence of illegal access and viruses, build a response prevention mechanism, strengthen system technology applications and security settings, such as 24-hour virus Trojan horse monitoring technology. Second, regular maintenance of the network system should be based on computer operating system, backup system,

ISSN 2616-5667 Vol.2, Issue 5: 77-83, DOI: 10.25236/AJETS.2019.020509

virus software, firewall and gateway detection. If hidden risks and security loopholes are discovered, they must be handled in a timely manner. Third, the network system security management and maintenance process should be incorporated into daily management work [4]. Strengthen relevant leaders' understanding and implementation, so that work is no longer carried out in the form of coping and cutscenes, but is time-efficient, fast and implemented [5].

4.4 Application of information encryption technology

Relevant industries and fields have achieved comprehensive information construction, and computer information management technology has been applied. Most of the "Internet +" management modes are the most common, allowing managers to quickly grasp and understand a large amount of information and content. Based on the current industry and field involving China's network system, it needs to quickly transfer, share and use a large amount of data information, data pictures, etc., of course, it is very easy to cause risks such as information data leakage [6]. Therefore, it is very important to encrypt enterprise information data and data pictures [8]. Information encryption technology uses keys, encryption and other means to design passwords for pictures, videos, and data in corporate network systems. Once a hacker wants to steal it during transmission sharing, it needs to be decrypted. Information encryption technology is the current defense of computer network security and prevention of new protection modes.

5. The development direction of future computer information management technology

5.1 Advanced virus prevention technology

The development of anti-virus technology is an important core substance for consolidating the overall computer network security. At present, the national defense virus technology is still mainly for killing and killing network system viruses. It is targeted at hackers and viruses in network security threats [7]. The current virus protection technology is mostly traditional, lagging, and lacks ineffectiveness. Mostly to cope with the existing network system viruses, it is not possible to identify and kill viruses that have not entered the network system [6]. Therefore, anti-virus technology will definitely be more proactive and timely in the future, and anti-virus technology will be integrated with its anti-hacking system in the future. That is, it is presented as a barrier at the client side of the computer network, effectively blocking and processing virus files, software, etc., and intercepting hackers' attacks in advance.

ISSN 2616-5667 Vol.2, Issue 5: 77-83, DOI: 10.25236/AJETS.2019.020509

5.2 The network security system is more intelligent

With the continuous innovation and development of computer network technology in China, the formation of artificial intelligence has shown its future development trend, which means that the intelligent implementation of computer network technology will no longer be far away. Of course, artificial intelligence and virtual simulation are also the development trends of computer network security protection technology in the future. In the future, if there is a problem with the security of the computer network, the intelligent management system will be activated to effectively manage and manage risk. Therefore, it is necessary to vigorously develop intelligent security management software and build an intelligent security management system. It is necessary to reduce personnel investment as much as possible, and also to continuously improve the efficiency of security management, in line with the overall development trend of computer network technology.

6. Conclusion

In summary, by analyzing and researching the application of computer information management technology in network security, the problems of network system security are clarified from various aspects and angles. According to the actual situation and development needs, relevant optimization countermeasures are proposed, mainly including virus prevention and optimization technology, application of identity verification technology, application of system management and maintenance technology, application of information encryption technology, virus prevention technology is more advanced and advanced, and network security The system is more intelligent, which lays the foundation for the next step.

References

[1] Min Xing (2019). Research on the Application Strategy of Computer Information Management Technology in Maintaining Network Security. Information and Computer, no.9, pp.7-8.

[2] Zhang Shali, Hong Yue, Han Liu (2019). Research on Application Strategy of Computer Information Management Technology in Maintaining Network Security . China New Telecommunications, no.8, pp.6-7.

[3] Dong Hui (2019). Application of computer information management technology in maintaining network security. Wireless Internet Technology, no.12, pp.137-138.

[4] Wei Daling (2019). Discussion on Computer Network Information and Network Security and Its Protection Strategy. Information System Engineering, no.2, pp.60-61.

[5] Zhang Wanbin (2019). Computer Application Analysis under Network Information Security Technology Management. Information Recording Materials, no.3, pp.78-79.

ISSN 2616-5667 Vol.2, Issue 5: 77-83, DOI: 10.25236/AJETS.2019.020509

[6] Jia Tao (2019). Analysis of the main hidden dangers and management measures of computer network security. Wireless Internet Technology, no.13, pp.19-20.
[7] Li Ruiping (2019). Research on Computer Network Security Maintenance and Management Measures in the Big Data Era. Computer Products and Distribution, no.5, pp. 38-38.