

THOUGHTS ON THE APPLICATION OF COMPUTER INFORMATION TECHNOLOGY IN THE INTERNET

Raja Moses

Department of MIS, Faculty of Economics and Admin, King Abdulaziz University, Jeddah, Saudi Arabia.

Abstract: With the continuous development of economy and science and technology, China's Internet technology has reached a new height. At present, people's economic level and livelihood After the living requirements have improved, Internet technology has gradually entered every family, and computer information technology has become indispensable for every family. a part of. At present, every part of life is inseparable from the Internet and information technology. While the Internet is becoming more and more important in life, mutual The responsibilities assumed by the Internet are even more important. As a result, network security issues have aroused widespread concern in society. computer information technology As a guarantee of Internet security, it plays an increasingly important role in the Internet. This article discusses the security and application issues of the Internet. Analyzed the role that computer information technology plays in the Internet.

Keywords: Internet; Computer information technology; Application

1 INTRODUCTION

Internet technology has played an increasingly important role in life, and all kinds of small things in life are inseparable from the support of the Internet. In this era when Internet information technology is the main trend, people store more and more information in In the Internet, it is loved by most people because of its convenience and speed. However, as people pay more attention to the Internet, network hackers also appear. With the advancement of technology, the skills of cyber thieves are also constantly improving. This shows that although Internet technology is developed and fast, there is still the risk of information loss and theft. In this case, computer information technology, as a guarantee technology for Internet security, plays an important role in maintaining Internet security.

2 INTERNET AND CYBERSECURITY

After continuous development, the Internet has now entered a mature stage. In daily life, the Internet is now the main way for people to communicate, entertain, and work. People have become dependent on the Internet and are gradually inseparable from the support of the Internet. With the continuous innovation and exploration of Internet technology, the network has become an important way of communication between people, realizing the perfect integration of computers and production and life. However, driven by computer communication technology and information technology, massive network attacks have followed. The privacy and security of computer user data are being threatened. Furthermore, stimulated by network technology, society has The network attack technology on the Internet is also advancing with science and technology[1].

In the Internet, thousands of devices are connected through a network and become a taken-for-granted whole. No matter who it is, no matter how far away they are, they can get in touch and communicate in this network. The information they want to obtain can be obtained through the network. Access can also be quickly obtained via the Internet. The Internet has made people more closely connected. At the same time, every country and human being has gradually become transparent, and the transmission of information has become more and more developed and rapid. In an environment full of networks, network security issues have also been a concern since the development of respective networks. Since people are increasingly dependent on the Internet, the protection of the Internet must be more cautious. Network security also includes many aspects. The first is the applied anti-virus system, computer firewall system, etc. This is a well-known network security technology. In addition, there are also network security detection systems and virus elimination systems such as network monitoring and information auditing. The network information age is different from the traditional communication age. Once a network intrusion occurs, all information will be leaked. At the same time, the computer system itself will also be compromised and cannot be used normally. In computer network technology, network information and security are very important. If a network system is to be secure, it must be protected by firewalls and network defense systems. There is a large amount of valuable information in the network information system, just like a password safe. From a small enterprise to a large country, confidential information is stored in network information. If you want to keep this information well and prevent other hackers from taking advantage of it, you must build network information and security well. Traditional network information and security technology can effectively resist previous network intrusions from external hackers. However, with the continuous development of technology, hackers' skills in breaking through network defense lines are also constantly improving.

Simple traditional network defense systems are no longer able to resist well. Instead of being attacked by hackers, network information was stolen and the network system collapsed. In this case, the network security system must be reformed accordingly.

3 THE MAIN CAUSES OF NETWORK SECURITY PROBLEMS

As a strict and complex system, the network is prone to network security problems without a properly skilled and capable technical staff to operate it. In the network, there are many reasons for security problems, which mainly include the following aspects.

(1) Operating system vulnerabilities are the easiest way to cause network security problems. Although network information technology has appeared in society for a long time, network operating systems will always have vulnerabilities due to the flaws in the network system itself. Certain loopholes appear. Due to the computer itself, there are some technical loopholes that are difficult for current technicians to make up for. When developing a system, there may be certain errors in every step. This is an inherent error of the operating system, although developers try to avoid loopholes during system development. At the same time, with the continuous development of technology, technicians are working hard to fill loopholes, but there will always be loopholes that will be leaked out under certain circumstances, giving network hackers certain opportunities, which has caused the emergence of network security problems.

(2) The incompleteness of the TCP/IP protocol is also a major cause of network security problems. TCP/IP is the key information for obtaining network addresses. Most personal information on the network is stored in TCP/IP. Once the computer's TCP/IP address is obtained, there will be the risk of information leakage and computer system paralysis. In the TCP /IP protocol, due to the lack of IP address protection during development, the TCP/IP system has a certain degree of openness, which creates a breach in security issues and threatens the security of network information. In addition, the existence of computer viruses threatens the security of computer systems at all times. Computer viruses are the most familiar form of computer intrusion. Computer viruses also appear as computer intrusions in the form of computer system vulnerabilities. However, unlike operating system vulnerabilities, computer viruses target the computer system itself. Computer viruses There are many types, and Trojan horse viruses are the most famous. Once a Trojan horse invades a computer system, The vast majority of computers will be paralyzed, the system will crash and cannot be used normally[2].

(3) The characteristics of the network structure also have an impact on security. The Internet can be regarded as a network system formed by different local area networks under certain connections. In this system, if you want to realize mutual information transmission, then Two hosts in different LANs are required to communicate, and multiple different devices are required in the middle, so direct transmission in the true sense cannot be achieved. Then during such a process, if an external attacker attacks any of the host devices, it will eventually cause damage and impact on the transmitted information, thereby intercepting information and data. Once such problems occur, it will It shows that the Internet environment is damaged and cannot have extremely high confidentiality and security.

4 APPLICATION OF COMPUTER INFORMATION TECHNOLOGY IN THE INTERNET

As an indispensable form in the new era, the Internet has gained a decisive position in life. With a small network environment and various forms of terminals, the use of TVs, computers, tablets and other applications has become a The development of the Internet provides an environment. But at the same time, diversified Internet application forms will eventually lead to increased security risks. Once there is a problem with the emission source, the entire information system will collapse, and all application terminals will be destroyed. Therefore, it is very important to take good security protection measures for computer information technology. With the rapid development of our country's national economy and society, the advancement of science and technology has gradually integrated computer information technology and the Internet. Since information technology has been widely promoted in various industries, more and more countries and departments have gradually increased the development and application of computers and information technology. The development trend of information technology focuses on the development and application of Internet technology, and the security of the Internet and network is particularly important. Computer information technology provides protection for the security and stable use of the Internet, avoids some network security risks caused by systematic vulnerabilities, viruses, hacker attacks, etc., lays the foundation for the security and stable operation of the Internet, and leads the trend of scientific and technological development[3].

4.1 Application of Information Technology in Network Anti-Virus

Among computer viruses, they are famous for their speed of transmission and ability to reproduce. Computer viruses spread very fast. They do not just spread on one computer. If the intruder learns the entire IP address of the computer, the virus will It can enter the computer system covered by the entire IP network environment, and the speed of spread is very fast. If a virus spread source is discovered, basically no computer in the entire environment will survive[4]. In addition, computer viruses are also very capable of reproducing. When a virus cell breaks through the computer's virus firewall, the virus will reproduce at an alarming rate. One second the computer was still in normal use, and the next

second it System crash due to flooding of viruses. In this case, the protective role of computer information technology is brought into full play. If you want to avoid computer viruses from invading computers, you must strengthen the protection of wireless LANs. When setting passwords for wireless LANs, try to set complex passwords to avoid deciphering by technical operators. At the same time, when using a LAN, you should hide the IP address of the LAN and not easily disclose your IP address. Otherwise, once the virus invades, all devices covered by the LAN will be unavoidable. In addition to external protective measures, the internal protection of the computer must also be done well. Trustworthy anti-virus application software must be used to protect the computer system. The types and types of virus detection and killing by anti-virus software must be increased to comprehensively protect the computer system. Organize virus intrusion.

4.2 Firewall Applications for Information Technology

Firewalls are currently the most effective method of Internet protection. Firewalls are widely used to protect important files because of their powerful blocking capabilities against viruses. The main function of a computer system firewall is to help users "control the traffic allowed in and out of the network or device", which means that the main function of the firewall is to "control the network" and "control device traffic" to ensure the security of users' computer use to a certain extent. When the firewall is turned on, any requests that are not authorized or permitted will be restricted and intercepted, which can block the intrusion of viruses or Trojans to a certain extent. The setting of the firewall is mainly to prevent the computer system from leaking vulnerabilities during application development, and to prevent the outside world from observing the internal vulnerabilities of the computer and thereby intruding the computer as a network protection measure[5]. Computer information technology is the prerequisite for the normal operation of the firewall. Firewall technology integrates the IP of the LAN through the layers of obstacles in the information LAN, making it difficult for the outside world to determine the specific location of the firewall. At the same time, the firewall can also use its unique method to hide the IP of the computer LAN to a certain extent, so that the outside world cannot discover the specific location of the computer immediately, greatly reducing the risk of the computer system, thereby reducing the risk of the computer system. Risk of infestation. At the same time, the possibility of information being stolen and leaked will be greatly reduced. The setting of the firewall effectively avoids the public nature of the computer network system itself and improves the access of external signals to this website. At the same time, non-interference from the outside also improves the security of the internal network environment and protects the computer environment under the LAN.

4.3 Application of Vulnerability Scanning Technology

Vulnerabilities are an inevitable factor in the development of computer systems, and they can only be found where the vulnerabilities are located. However, with current methods and technologies, the loopholes cannot yet be eliminated. Therefore, when dealing with vulnerabilities, finding the location of the vulnerability is the most important step. There are quite a lot of subroutines in a huge computer system. It is basically impossible to detect vulnerabilities in each subroutine by relying solely on the human brain. If you want to inspect vulnerabilities, you must rely on computer information technology. to fulfill. In computer information technology, vulnerability scanning technology is a better technology for vulnerability detection. Vulnerability scanning technology is an important type of network security technology. It cooperates with firewalls and intrusion detection systems. It can effectively improve the security of the network. By scanning the network, network administrators can understand the network's security settings and running application services, discover security vulnerabilities in a timely manner, and objectively assess network risk levels. Network administrators can correct network security vulnerabilities and incorrect settings in the system based on the scan results to prevent hackers from attacking.

If firewalls and network monitoring systems are passive defense methods, then security scanning is a proactive preventive measure that can effectively avoid hacker attacks and nip problems in the bud. Vulnerability scanning technology can reasonably configure the system inside the computer and integrate the data of each subroutine. At the same time, scan the system for internal problems. Vulnerability scanning technology is a professional scanning technology system that can scan the entire computer hard disk for vulnerabilities. It is the same as the scanning of anti-virus software. It is very fast and can quickly report problems that occur in the system and troubleshoot system problems. Make corresponding amends. The use of vulnerability scanning technology greatly reduces the security risks of computer network systems. Once viruses and hackers invade, the scanning system can report the location of the problem as quickly as possible. At the same time, it cooperates with relevant network defense systems and virus killing systems to intercept problematic data, which greatly improves the security of the network environment and computer systems[6].

4.4 Strengthen Training for Professionals

In the design and composition of network base stations in computer network technology, the requirements for the professional capabilities of the staff are very high. In terms of professional study, the study of network computer

languages, code programming software and other majors is indispensable. In this regard, computer network technology must be more stringent in the selection of staff and managers. Information technology is of great importance to the Internet. If there are no excellent technologies and methods for virus protection, a virus may invade accidentally. From this point of view, the staff working in the computer information technology protection system must be highly skilled. In order to protect the confidentiality of important company and country information, programmers with considerable experience must be hired[7]. At the same time, staff must have a strong sense of responsibility to avoid job-hopping. Once it betrays its position, the entire network system will be dealt a fatal blow. In addition, enterprises and companies also need to develop special incentive and reward and punishment systems for employees, and interconnect the daily work content and performance of staff with such reward and punishment systems, so that employees' work enthusiasm and work responsibilities will be Mental health can be effectively improved, thereby effectively improving the overall work quality and efficiency.

5 CONCLUSION

To sum up, computer network technology, as a leading project for information transmission, must be analyzed and researched from many aspects and angles in the development of technology. As China's high-tech fields continue to achieve new developments, computer network technology has also developed rapidly. Artificial intelligence technology and mobile computer network technology have gradually become common among computer network technologies across the country through the technological and information revolution. The development of computer network technology and the great cause of national economic development are the foundation of China's informatization. Therefore, it is a very important choice to improve the integrity of computer network technology and utilize Internet protection and system protection into computer network technology.

COMPETING INTERESTS

The authors have no relevant financial or non-financial interests to disclose.

REFERENCES

- [1] Zhang Baohua. Application of computer information technology from the perspective of the Internet. *Information and Computers (Theoretical Edition)*, 2019(9): 1-2.
- [2] Yu Miao. Trial on computer hardware maintenance technology and troubleshooting. *Computer Programming Skills and Maintenance*, 2022(1): 159-160+163.
- [3] Wang Shutong, Kong Lingzhi. Research and practice on the application of blended teaching in computer hardware and network courses. *Electronic Journal of the New Education Era (Student Edition)*, 2015(2): 198- 198, 199.
- [4] Yang Jisong. Research on the prevention and management of hidden dangers of confidentiality leakage in computer network applications. *Information Systems Engineering*, 2018(2): 62.
- [5] Zang Keli. Analysis on the effective application of computer information technology in the Internet. *Information Construction*, 2016(2): 37.
- [6] Peng Jia. Application of computer information technology in Internet security. *Electronic Technology and Software Engineering*, 2019(9): 202.
- [7] Li Zhenbo. Discussion on modern technology and future development of electronic information engineering. *Electronic Components and Information Technology*. 2020(3): 91-93.