Discussion on Computer Network Security Prevention Based on Big Data Era

Lixian Sun
Chaoyang Teachers College Liaoning Province, China Zip code: 122000
Email: tg667788@xzestudio.com

Abstract. With the continuous development of reform and opening up and the continuous development of science and technology, information and communication industry has also achieved rapid progress. Certain problems will also be encountered in the development of computer technology. The most important problem is about computer network security. Some people are likely to be attacked by viruses and Trojan horses while using computers, leading to a lot of core damaging information. Some network hackers may also use computer loopholes to steal relevant information. Strengthening computer network security management is very important. This article will focus on computer network security in the era of big data as the main topic and discuss the relevant content.

1. Introduction
With the continuous improvement of people’s quality of life, people have changed their traditional ways of life. People now rely more on information technology, which can better improve their work and study efficiency. Nowadays, network security issues are emerging one after another, threatening people’s property safety. Big data technology can bring a very convenient function in the process of personal use. Big data collection and storage functions are very comprehensive, but in the actual network use process, it will also be affected by security. This article will mainly focus on computer network security for a detailed discussion for the reference of relevant personnel.

2. Analysis of the main factors affecting computer network security
Nowadays, people’s lives are inseparable from computer technology. People use computers more and more frequently. However, in the process of computer network systems, some security problems are particularly prone to occur. If it cannot be solved in time, it will have a serious impact on the entire system. In order to better ensure its efficiency, it is necessary to continuously strengthen the computer network security system. The following will analyze the main influencing factors.

2.1. Factors affecting nature
The computer itself is an external machine, and it will be affected by surrounding external forces during its normal use. If people use the computer violently, it is likely to cause the computer to be in a state of paralysis. If the computer is accidentally used by people, it may cause the entire system to crash. Therefore, it is also very important to protect the computer from external forces. In the process of using the computer, the relevant personnel must strictly control the surrounding environment of the computer to perform routine maintenance to prevent some force majeure factors from being affected. It can reduce the impact of some natural disasters on the computer network system and ensure the smooth operation of the system.
2.2. Factors affecting network
The computer network itself has a certain degree of openness. Because of its openness, it faces a very wide range of network and is particularly vulnerable to attacks from some foreign viruses. Generally, the user’s own IP is relatively fragile, and the stability of the system is not particularly good. Therefore, the efficiency of the overall IP protocol is relatively low, and the normal operation of the overall network cannot be guaranteed. In addition, there are many Hackers will deliberately attack users’ computers and steal their private information. So it is likely that the overall computer network is in an unstable state.

2.3. Factors affecting human
With the continuous development of modern science and technology, the computer system is constantly updated and improved. The characteristics of artificial intelligence that emerged at the historic moment are also quite prominent, and relevant users need to perform corresponding operations on them in accordance with corresponding functional requirements. Most modern computer users do not have a particularly deep understanding of artificial intelligence, and the relevant operating level is not particularly high, and they are particularly prone to some human errors, making the computer network system unable to operate rationally. No matter in the process of computer operation and development, it will produce adverse effects, which is also the main reason for the frequent occurrence of computer security risks. Some users are not particularly high in security awareness. Scientific and reasonable design of computer network systems can better formulate comprehensive management measures and reduce system security risks.

2.4. Factors affecting hackers
Some computer hackers will conduct malicious attacks on computer networks to steal private information. With the emergence of malicious competition among modern enterprises, this phenomenon is also increasing. Therefore, some hackers will destroy the computer network system, which greatly reduces the security of the entire system. All operations performed by the user on the computer may be stolen and attacked by hackers, including some private information of enterprises or some private information and data. If hackers steal these company secrets, it will bring heavy economic losses to the company. The main forms of hackers through network attacks are divided into active attacks and software installation attacks. Active attack is now the main intrusion method of hackers, and it is also a form of invasion with a strong purpose. After being attacked, the entire computer system will have current faults. Under normal circumstances, these faults are difficult to solve, which will cause the entire computer to run not particularly smoothly. Secondly, some hackers will also guide people to install some software to steal some data, and attack users’ computers through corresponding network nodes. As a result, customer information cannot be effectively protected, resulting in certain economic losses.

2.5. Factors affecting management
With the continuous development of modern information technology, people use computers more and more, and computer network management is also a very important content. Scientific and rational management can better ensure the smooth operation of the entire computer. Computer networks cannot guarantee the final results in such a non-strict management atmosphere, and many computer users do not have the awareness of computer management, which leads to endless computer stability and security problems. It can actively face the hidden dangers of computer security, and let the computer implement more efficient and strict management mechanism in the normal operation process, which can better guarantee the security of the final data and improve the security awareness of users. If there is a lack of a more complete computer network management mechanism, the ultimate network security cannot be guaranteed, and the functions performed by the computer will also be restricted.

3. Concrete measures of computer network security prevention
Through the understanding of the above, it is easy to understand the problems that exist in the process of computer network security. Relevant personnel should actively take corresponding measures against
these problems to better ensure the stability of the entire computer network. The following will discuss specific measures for computer network security.

3.1. Improve the security monitoring system to reduce the impact of network risk
The users of computer networks are now mainly facing the influence of viruses and hackers. In the specific practice, companies need to do a good job in the direction of computer network management. If it is found that hackers have stolen relevant data and information, it is a heavy economic loss for the enterprise. Therefore, the relevant personnel of the enterprise must build a safety monitoring system to deal with the more dangerous factors and carry out corresponding prevention. In the safety monitoring system, it is necessary to carry out corresponding defenses against some dangerous factors, and relevant technical personnel can also construct corresponding firewalls. It ensures that the staff can download the relevant software under safe conditions to prevent the staff from bringing some viruses into the working computer in the process of information transmission. In addition, the staff can also install relevant anti-virus software on the computer. Relevant personnel can divide the network into internal and external, and use different security monitoring systems for them. Relevant personnel also need to perform virus detection on the contents of the U disk in a timely manner to build a safer and more stable external environment.

3.2. Check system vulnerabilities regularly
A computer network system is usually composed of internal software and external hardware. The external hardware is more sensitive, so people must repair and maintain it during use. The load carried by the entire computer is relatively large. At this time, the technicians should pay more attention to the inspection of the computer software and hardware, and timely discover the problems in the computer hardware and repair them in time. In particular, some bugs that often appear during use may be caused by certain viruses, and they must be disinfected completely. Usually the bugs in the system are caused by viruses and hackers. Technicians should pay attention to the software situation of the network platform, discover the vulnerabilities in time and actively apply corresponding patches to these vulnerabilities. At the same time, it is necessary to ensure the safety and stability of the software network platform, prevent the intrusion of some dangerous factors, and better improve the stability of the overall equipment operation. The relevant hardware must be actively replaced and repaired, and the hardware must be updated accordingly to improve the level of the computer.
3.3. Develop more comprehensive information dissemination principles
In the context of the current big data, the relevant security monitoring system must not only ensure the information security of the entire computer at the network level, but also have a comprehensive understanding of the virus check and good operation of the relevant software to improve the smoothness. At this time, it is not only necessary for relevant personnel to formulate and improve the corresponding safety monitoring system, but also formulate download transmission rules to better improve the safety protection awareness. For example, when transferring some private information of an enterprise, a grading method can be adopted. For some relatively high-level information, the staff must not be taken away from the company. Regarding some information and data that are not private to the company, the transfer of information between employees should also be regulated to prevent information leakage. At the same time, it is necessary to sign corresponding confidentiality agreements with employees to prevent them from appearing in disloyal behaviors and situations. When transferring some confidential information, senior management can transfer the information in cipher text. This can effectively reduce the theft of some criminals during the delivery process. At the same time, it can better protect enterprises from economic losses caused by information loss, greatly improve the security of enterprise data and promote the long-term development of enterprises.

3.4. Use network technology to set up early warning system
In order to better exert the effect of the network early warning system in actual work, a large amount of data must be collected and analyzed. If only manual data analysis is used, work efficiency is not high. At this time, big data mining technology can be used to store and manage the corresponding data. At the same time, intelligent algorithms, neural networks, etc. can also be used to model the data and convert it into a data vector, which can better facilitate data storage. It is necessary to conduct various training on the data and set an expected value for the data, which will be more convenient in the process of big data processing, so as to better realize the intelligent analysis and management of massive data. In addition, relevant personnel also need to conduct in-depth analysis of some abnormal data, analyze its existing problems, effectively carry out risk assessment, set up a risk warning system, and improve the overall computer level.
4. Conclusion
The advent of computer technology has changed people’s lifestyles and greatly improved work efficiency. But in the process of actual computer use, there will be certain security problems. Some lawbreakers will steal the confidential information of the enterprise, which will cause serious economic losses. It is urgent to strengthen the security management of computer networks, and relevant personnel should take measures to ensure network security.

References
[1] Liang Feng. Discussion on the prevention of computer network security based on big data age [J.] Network Security Technology and Applications, No.234(06): 88-90.(2020)
[2] Ye Jianwei, Ye Jianfang. Threats to information security and prevention strategies[J]. Educational Information Technology, (11): 51-54.
[3] Yi Wenjing. A study on computer network security prevention in the big data age [J.] Computer knowledge and Technology 13(012):19-20.(2017)
[4] Xu Hongwei. Discussion on the prevention of computer network security based on big data age [J.] South farm machinery. v.51;No.345(05): 227-227.(2020)
[5] Zhang Jingfang Research on computer network security in the big data Era[J]. Science and Technology Innovation and Application, (14): 84.(2017)
[6] Zhu Guangjun, Meng Zidong. Research on network information security and protection strategies based on the background of big data era[J]. China New Telecommunications, (2): 63-64.(2018)