Security Analysis of Computer Information Processing Technology under the Background of Big Data Era

LUO Le, FANG Zhimiao, WU Zhenghan
1Department Of Public Security Intelligence, Chongqing Police College, Chongqing,401331, China
2Department Of Basic Course, Chongqing Police College, Chongqing,401331, China

Abstract: With the development of science and technology, society has entered the era of big data, and data information has been shown to be open, which has played a role in optimizing data calculation mode and improving data utilization efficiency. At the same time, computer information processing problems are also suffering attention. This paper will take the school computer information processing technology security work as an example to analyze the computer information processing technology security management scheme under the background of big data era, and put forward personal opinions, hoping to provide reference solutions for computer information processing technology security management.

1. Introduction
Big data technology is an emerging product in the network era. It can use new thinking modes to process massive data information, innovate data processing methods, improve information technology systems, correct data errors, and improve data management efficiency. However, it is impossible to ignore the computer information security management problem under the background of the big data era. To solve this problem, it is necessary to scientifically set up a computer network protection system, comprehensively optimize access control technology, strengthen the monitoring of computer information network systems, and continuously improve the virtual private network. This paper will briefly analyze the causes of the security problems of computer information processing technology, and layer by layer the security management plan of computer information processing technology under the background of big data era.

2. Reasons for The Security of Computer Information Processing Technology

2.1. Network Virus Threat
At present, there are nine kinds of network viruses that threaten the security of computer information processing technology - Trojan virus, bundler virus, worm virus, web virus, mobile virus, macro virus, virus destruction, complex virus, hacker virus [1]. Among them, the prefix of the Trojan virus is Trojan. This virus often spoofs the virus through the loopholes of the network system to spread the virus. It is not negligible that the Trojan virus is very concealed, often without the user's knowledge. Stealing computer information in the state. The prefix of the bundler virus is Binder. It has a commonality with the Trojan virus, which is extremely concealed. This virus is often bundled in QQ, browser, WeChat, input method and various common video software, and rapidly developed into The new virus program is very harmful to computer network systems. The worm's prefix is Worm. Its propagation script is HTM file and MIRC. This virus spreads very fast and often spreads with the defects of email and
network systems and spreads automatically. It should be noted that the worm is often difficult to be completely killed. Once the computer is invaded by the virus, it will cause the network system to crash in a short time. Moreover, worms that have not been completely killed will be reborn twice, again forming a network security risk. Web viruses are often in the form of malicious code on a web page. The prefix is the script. This virus maliciously tampers with the user's registration table, destroys the original network system, steals computer information, and causes internal disks to be formatted. As early as 1999, the macro virus was called "beautiful killer". This virus is usually parasitic in the macro of Word documents and uses the macro programming language to automatically edit the virus program. If a Word document is infected with a macro virus, the user is After opening the document, the macro virus is activated, and the document also increases the spread of macro viruses during the transfer. The infection of mobile phone viruses is a smart phone. This virus often uses mobile phone text messages, games, QQ phones and WeChat voice to spread the virus. Compared with other viruses, the speed of transmission is very fast. The prefix that destroys the virus is Harm. Its prominent feature is that it is destructive and strong. Therefore, it is called “destroying the virus”. If the computer is invaded by this virus, it is easy to find the memory to be formatted during the running process. The characteristic of the composite virus is "complexity". This virus has both the danger of the Trojan virus and the worm, and it is very difficult to kill. The hacker virus mainly comes from hacker attacks. At present, many criminals attack the user's computer for profit and steal secrets and malicious retaliation, and use computer network systems to steal information and deliberately disclose data confidentiality, which seriously harms network security. Like "Panda burning incense virus", "blackmail virus" are all offensive viruses spread by hackers. Once the computer is invaded by such viruses, it will cause the network system to smash and secretly leak [2].

2.2. Impact of Network Openness

The era of big data is open and inclusive. It can effectively solve the problem of information integration and processing in a short period of time, and effectively improve the efficiency of data information management. However, the era of big data also brings cyber security problems that cannot be ignored. Many criminals will Driven by interests, they use unfair means to steal valuable information and embark on the path of illegal crime. At present, computer systems will also use the internal IP technology to carry out virus defense and self-protection, but in the face of extremely devastating viruses, the self-protection ability of computer systems is still weak [3].

2.3. Improper Manual Operation

Throughout the whole, most of the current users have a weak awareness of network protection. In the process of computer operation, there are inevitable negligence and mistakes. Some users will disclose personal information such as bank cards, ID cards, personal photos, etc. in the process of using computers, which leads to Information disclosure and bank card funds were stolen.

2.4. System Vulnerability

From the perspective of the overall structure, the computer network system under the background of the big data era is not perfect. Both Windows and Limux have certain defects, so it is difficult to avoid multiple security risks. In addition, user preferences can also increase vulnerability issues, ultimately leading to the destruction of computer systems.

3. Computer Information Processing Technology Security Management Scheme under the Background of Big Data Era

3.1. Scientific Setting of Computer Network Protection System

To strengthen the security management of computer information processing technology in the context of the data age, we must first scientifically set up a computer network protection system and build a network security protection wall to avoid illegal access. A university has set up a high-intensity
firewall to prevent external users from illegally accessing the network. In addition, the school regularly optimizes firewall presets to ensure the secure transmission of data, avoiding malicious elements stealing data and blocking data transmission, thus creating a secure campus network [4].

3.2. Fully Optimized Access Control Technology

To comprehensively do a good job in the security management of computer information processing technology under the background of the big data era, and to build a civilized, pure and secure campus network, we must focus on optimizing access control technology. At present, there are three kinds of state-of-the-art access control technologies, namely T-ABAC model, mandatory access control technology and user behavior evidence collection technology. Among them, the T-ABAC model (Trust and Attribute-Based Access Control) is based on the ABAC model. With the support of big data technology, the T-ABAC model mainly uses the ABAC model method to implement dynamic access control and fine-grained access control. From the microscopic point of view, the T-ABAC model has many attributes, including subject attributes, object attributes, trust attributes, action attributes and environment attributes. These attributes can be combined to meet the fine-grained access requirements in the network environment. Moreover, the T-ABAC model combination is divided into three modules, namely a user identity verification module, an access judgment module and a trust evaluation module, wherein the user identity verification module is mainly used to process the user identity authentication management service, and in the authentication process, the user You must properly log in to the computing environment under the support of big data technology to access the web page. The network platform will play the role of authentication technology to accurately verify the authenticity of the user's identity, and prohibit illegal users from accessing web pages and data information. The access judgment module is mainly used to process the user's access request and provide and restrict access according to the requested content. The trust evaluation module is an adjustment to the trust attribute and can enhance the management of the attribute access mechanism. In addition, the T-ABAC model belongs to the quintuple, which are S, O, E, A, and T, respectively, where S is the abbreviation of the subject (subject), O is the object (object), and E is the environment (environment), A On behalf of action (action), T is the abbreviation of trust (trust), these five combinations play their respective roles, help to build a secure network environment, and thus effectively improve the security management of computer information processing technology. The mandatory access control technology is supported by a mandatory access control technology system (MAC). The full name of the system is Mandatory Access Control, which is mainly used to access user control requirements and set security fixed policies and management rights for computers. In addition, the core of the Access Control Technology System (MAC) is to protect the computer information system, avoid data leakage, and set the access basis for the web page. Moreover, the Mandatory Access Control Technology System (MAC) sets up security controls and "write-on" and "read-down" executions to ensure that subjects and objects can be safely executed and operated. User behavior evidence collection technology is mainly for the record of user login, access request and access content. This technology can regulate user behavior, strengthen security access rights management, prohibit illegal users from accessing confidential information, and maintain the security of computer systems and data information.

3.3. Strengthen the Monitoring of Computer Information Network System

In the context of the era of big data, the increase of network viruses has intensified the problem of computer information security management. To this end, it is necessary to comprehensively strengthen the monitoring of computer information network systems, and use various security management technologies to set up a comprehensive protection system and security passwords to avoid network access. Virus erosion, do a good job in network security monitoring, so as to continuously improve computer performance, reduce power configuration, speed up computer startup speed and running speed, and do a good job in computer network maintenance. Secondly, it is necessary to comprehensively improve the computer network intrusion monitoring technology, prevent illegal intrusion in a timely manner, regularly repair computer vulnerabilities, and eliminate various insecure
factors. On the other hand, we must vigorously enhance the five functions of computer network anti-virus software: First, comprehensively monitor the network operation status and eliminate the virus program in the budding stage. Second, regularly upgrade anti-virus software, optimize the network virus database, and basically kill the network virus. Third, strengthen the virus removal function of anti-virus software and improve the anti-virus program in the network system. Fourth, fully integrate and optimize the network resources owned by anti-virus software, and improve the automatic enabling function of anti-virus software. Fifth, enhance the automatic identification function of the anti-virus software, so that the anti-virus software will automatically kill and clear the virus immediately after identifying the network virus.

3.4. Improve Virtual Private Network
For the problem of computer information security management, it can be alleviated by setting up a virtual private network. This method mainly refers to constructing and matching a dedicated network system for the public network architecture system. Generally, such a dedicated network system is not independent. It is a secure network system based on the public network architecture. In short, the foundation for building a virtual private network is to play the role of a communication protocol. At the same time, the network system is used to build a professional, secure and multi-protocol virtual private line between the intranet and the client. An effective connection between the intranet and the client, and the use of the network system to implement covert communication processing, thereby preventing data information from being leaked. A college is to build a virtual private network between the campus intranet and remote clients to improve the security of computer information processing and create a secure campus network [5].

3.5. Strengthen Network Security Management Mechanism
To comprehensively improve the quality of computer information processing technology security management under the background of the big data era, we must attach importance to strengthening the network security management mechanism and construct a network security technology model. At the same time, we must do a good job in the vocational training of relevant talents, in order to do a good job in the era of big data. Under the background, the computer information processing technology security management work cultivates a high-quality management team. Second, the national government and relevant departments should vigorously promote the network security management mechanism in the context of the big data era to ensure the smooth implementation of the mechanism. Thirdly, we should vigorously strengthen the propaganda of cybersecurity knowledge, comprehensively improve the cyber security awareness of users, and teach them to protect important information and comply with network discipline. On the other hand, the national government needs to improve relevant laws and regulations while improving the network security mechanism, formulate effective network security rules and regulations, and crack down on illegal crimes that endanger network security.

4. Conclusion
In summary, to optimize the computer information processing technology security management solution under the background of the big data era, to do a good job in network security management, we must scientifically set up a computer network protection system, build a network security protection wall, avoid illegal access, and create a civilization. A secure network environment will continuously improve network security access control technology, accurately verify the authenticity of user identity, prohibit illegal users from accessing web pages and data information, scientifically process user access requests, and provide and restrict access based on requested content; strengthen computer information network system monitoring efforts to avoid network erosion by viruses; improve virtual private networks to protect important information; strengthen network security management mechanisms, build network security technology models, improve relevant laws and regulations, and crack down on cybercrime in accordance with the law.
Acknowledgments
This research was partially supported by
Scientific and Technological Research Program of Chongqing Municipal Education Commission (Grant number: KJZD-K201801701 and Grant number: KJQN 201801704)
Research Program of Chongqing Police College (Grant number: JY201501)
Chongqing Research Program of Basic Research and Frontier Technology (Grant number: cstc2016jcyjA0270)
Social Science Research Program of Chongqing Municipal Education Commission (Grant numbers: 17SKG301 and 18SKGH165)

References:
[1] Yan Dan. Analysis of Computer Information Processing Technology under the Background of "Big Data"[J]. Computer and Information Technology, 2018(12:1).
[2] Zhu Fulei. Analysis of computer information processing technology in the context of "big data" era[J]. Digital Communication World, 2018 (12:2).
[3] Fan Xiaojing. Application of Computer Information Technology in Network Security under the Background of “Big Data”[J]. Changzhou Tourism Business College, 2018(12:3).
[4] Zhao Yuhua. Analysis of Computer Information Processing Technology under the Background of “Big Data”[J]. Information Technology and Informatization, 2018(11:4).
[5] Deng Qing. Research on Computer Information Processing Technology in the Age of Big Data[J]. Information Technology and Informatization, 2018(11:5).