Journal of Electronic Research and Application, 2024, Volume 8, Issue 6
http://ojs.bbwpublisher.com/index.php/JERA
ISSN Online: 2208-3510
ISSN Print: 2208-3502

Computer Network and Database Security Technology Optimization

Kachen Zhang*

Guizhou Police College, Guiyang 550005, China

Corresponding author: Kachen Zhang, 13985168310@163.com

Abstract: With the continuous development of computer network technology, its applications in daily life and work have become increasingly widespread, greatly improving efficiency. However, certain security risks remain. To ensure the security of computer networks and databases, it is essential to enhance the security of both through optimization of technology. This includes improving management practices, optimizing data processing methods, and establishing comprehensive laws and regulations. This paper analyzes the current security risks in computer networks and databases and proposes corresponding solutions, offering reference points for relevant personnel.

Keywords: Computer network and database; Security technology; Optimized path

Online publication: November 29, 2024

1. Introduction

As an important part of computer applications, computer networks and databases can provide convenient and quick services for people and bring huge economic benefits to enterprises [1]. With the continuous acceleration of China's economic construction, social production, and people's lives are more dependent on computer networks and databases. But from the point of the current situation, the computer network and database in the development of our country still have some problems to be solved in the process. Therefore, it is of great practical significance and value to strengthen the exploration of the optimization path of computer network and database security technology [2].

2. The importance of computer network and database security

Firstly, database security is crucial not only for the vital interests of enterprises but also for national information security. Recognizing the security needs of important national information systems, the country has placed significant emphasis on database security. Ensuring database security is essential for safeguarding

national information and maintaining overall stability.

Secondly, enterprise databases store a vast amount of commercial secrets, customer information, and confidential data. If this data is compromised, it can lead to significant economic and reputational losses. To address this, a new security management approach for databases is proposed. Establishing a robust database security and protection system will provide reliable support for enterprises, facilitating digital transformation and enhancing competitiveness [3]. Strengthening database security is essential to reduce operational risks from data breaches, improve service reliability, and ensure survival in a highly competitive market. Moreover, the widespread use of big data has led to numerous incidents of personal information leakage, greatly impacting daily life. Strengthening database protection to safeguard personal information rights is crucial for maintaining social harmony and stability.

Finally, the security of the database is not only related to the protection of data but also related to the use and management of data. Therefore, to effectively prevent data leakage, it is necessary to strengthen the security of the database, standardize its management, and avoid the abuse of data and improper leakage, to realize the effective use of data. The security of databases is one of the most important problems in the world, and it is also the key to the protection of operating systems [4]. In order to ensure the security of the computer network database, it is necessary to monitor and repair it in a full range. In this way, the system defects in the system can be timely detected and treated, reducing the safety risk system.

3. Computer networks and databases in the current status of development

3.1. Security issues

With the continuous development of computer network and database technology, more computer users begin to obtain information through the network, and the information obtained by these users will exist in the form of electronic data in the computer network and database system, so this data information is vulnerable to hackers and other criminals, resulting in users cannot use the database system normally. For example, at present, there are many enterprises in China within the application of computer networks and database systems that did not carry out reasonable planning and design, resulting in many security problems in the application process [5].

3.2. Laws and regulations are not perfect

Although a series of laws and regulations have been formulated for the use of computer networks and databases in China, there are still some problems in implementing these laws and regulations. On the one hand, China has formulated relevant laws and regulations on the use of computer networks and databases, but because some of these laws and regulations are old, they cannot adapt to the current development requirements of computer networks and database management systems [6]. On the other hand, our country on the use of computer networks and databases also has certain vulnerabilities. Due to the lack of corresponding laws and regulations for the use of computer networks and databases in China, some criminals use these loopholes for illegal activities, which has had a great impact on Chinese society.

3.3. Backward management mode

In the current process of the use of computer networks and databases, to ensure the security of data information, many enterprises have adopted the more backward manual management mode, this management mode not only has certain security risks but also poses a huge threat to the security of data information.

Especially in the current network environment that continues to develop, the problem of network vulnerabilities is becoming more serious, which requires enterprises to strengthen the computer network and database security technology optimization, to ensure the security of data information.

4. The current computer network and database security risks exist

4.1. The impact of viruses on computer networks and databases

A computer virus is a special program that exists in the computer system. Once there is a virus in the computer system, it will have a serious impact on the computer network and database, which is mainly manifested in the following aspects. Firstly, there are a large number of viruses in computer networks and databases. These viruses will not only destroy computer networks and databases but also greatly reduce their own operating ability. Additionally, these viruses will cause damage to the data in the database after entering the computer networks and databases.

Secondly, there are a large number of Trojan horse programs in computer networks and databases. These Trojan horse programs can not only track and record the user but also pose a threat to the user's privacy. Finally, there are a large number of vulnerabilities and information leakage problems in computer networks and databases. Once these problems occur, the user's personal information will be leaked. Moreover, there are a large number of hacker invasion methods in the current computer network and database, which will not only attack the computer network and database but also steal the user's personal information and other operations [7].

4.2. The threat of hacker attacks on computer networks and databases

The threat of hacker attacks on computer networks and databases mainly lies in the following aspects. Firstly, hackers steal user information by using vulnerabilities in computer networks and databases. Once hackers use the vulnerabilities to obtain user information, it seriously violates the user's privacy. Secondly, hackers will destroy the computer network and database after invading the computer network and database. These hackers obtain user information by destroying the files in the computer network and database. At present, there are a large number of hacker attacks on computer networks and databases. After these hackers invade computer networks and databases, they will not only destroy them but also cause certain threats to computer networks and databases [8].

5. Computer network and database security technology optimization path

5.1. Establish awareness of computer network and database security management

Firstly, fully realize the importance of computer network and database security management. "Without network security, there is no national security." As one of the important components of society, enterprises are an important foundation to ensure the stable operation of society and economic development. Therefore, when enterprises carry out network construction, they must adhere to the idea of "network security is benefit," clear the principle of "who is in charge, who is responsible" and effectively manage and control the network system [9]. Simultaneously, during the network construction process, it is essential to continually improve the network management system and clearly define the responsibilities and tasks of relevant personnel to ensure the normal operation of the network.

Secondly, strengthen the training of relevant personnel. As one of the main bodies of society, enterprises should pay attention to the professional knowledge and skills training of employees in network construction

and management, and guide employees to establish a correct awareness of computer network and database security management. To achieve this goal, enterprises should effectively promote awareness of the importance of computer network and database security management for operational and developmental success. Utilizing various methods and channels, training can serve as one of the most effective means to educate employees. In the training process, the enterprise should pay attention to grasping the training content and the actual work of the degree of combination. For example, when discussing "financial data management," it is beneficial to integrate financial data with computer information management. Additionally, in training sessions for enterprise leaders, we can combine their understanding of computer networks and database security management with practical applications in their work.

5.2. Improve the technical prevention capabilities of management personnel

Network security capability primarily refers to the technical prevention skills of personnel responsible for managing enterprise computer networks and database security. In practice, these personnel should fully utilize advanced technical methods to ensure robust protection for the enterprise's network security.

On the one hand, enterprises should focus on strengthening the professional and technical training of information technology personnel. Given the high level of professionalism and technical expertise required for computer network and database security management, improving these skills must begin with the personnel themselves. In practice, enterprises should enhance the training of their information technology (IT) staff, providing systematic and comprehensive instruction in both theoretical knowledge and practical operations [10].

Simultaneously, it is essential to encourage information technology personnel to participate in professional skills examinations to continuously improve their professional skills and security capabilities. Furthermore, enterprises should actively strengthen cooperation with relevant departments and industries. With the rapid development of the Internet, various network security challenges have emerged. To address these issues, enterprises must establish an industry information-sharing mechanism to maintain contact with other relevant departments and industries. This approach will enhance information exchange and communication between enterprises and external stakeholders, enabling them to stay informed about network security risks and related information promptly [11].

5.3. Strengthen technical preventive measures for network security

Network security technical preventive measures mainly include:

(1) Utilizing advanced network information security technologies, such as constructing firewalls and intrusion detection systems, to provide comprehensive and reliable protection for internal servers, operating systems, databases, and other critical equipment and information systems.
(2) Establishing a data backup mechanism to enhance the safety and reliability of data backups.
(3) Implementing various technical measures to strengthen the protection of employee and financial information, ensuring that data is not stolen or leaked.
(4) Establishing a robust log management system to record and analyze system operations, allowing for timely identification and resolution of security risks.
(5) Enhancing network information security education to improve employees' awareness and understanding of network security.

Firstly, it is essential to strengthen the implementation of intrusion detection and data encryption

technologies. The primary function of intrusion detection technology is to help managers promptly detect network anomalies. When abnormalities are detected, alarm procedures are activated, enabling network managers to take targeted measures to effectively prevent viruses or other malicious programs. Data encryption technology plays a crucial role in protecting enterprise privacy and sensitive information. By regularly optimizing and upgrading encryption technology, enterprises can enhance the security of their data. Additionally, they can implement various encryption methods to ensure that files on the computer are safeguarded against damage or unauthorized access through multiple layers of protection.

Secondly, establishing a robust internal management mechanism is essential. Enterprises should develop and enhance their internal management systems, standardize work processes, clarify the division of responsibilities, and strengthen the supervision of relevant personnel to prevent mistakes, dereliction of duty, and malfeasance. Moreover, a corresponding reward and punishment system, along with an assessment mechanism, should be implemented to recognize and commend employees for outstanding performance while addressing issues of underperformance or negligence [12].

5.4. Build and improve the system's emergency response mechanism

Enterprises should enhance their capacity to handle emergencies related to computer and information system security incidents. When an emergency occurs, the emergency plan must be activated promptly, ensuring that the incident is managed effectively and in a timely manner.

In view of the emergency plan for network security incidents, a robust emergency response mechanism should be established [13]. Firstly, the enterprise should formulate and improve the emergency response mechanism following the enterprise network security incident emergency plan, ensuring it is consistent with the actual situation of the organization and operates in strict adherence to the "Information Security Incident Emergency Plan Management Measures." Secondly, the enterprise's network security incident emergency response plan should be reviewed regularly to ensure its scientific validity and practicality. Moreover, based on the nature of the network security incident, its degree of harm, and its scope of influence, appropriate emergency response measures should be formulated. Finally, effective communication channels should be established to ensure that various departments can collaborate, allowing for timely reporting of network security incidents to the relevant departments [14].

At the same time, it is essential to conduct network security emergency drills. Firstly, the network security emergency plan implemented within the enterprise should be rehearsed. Through these drills, issues in the plan can be identified, allowing for timely measures to be taken to resolve them and continuously enhance the effectiveness of the drills. Secondly, employees should be organized to learn network security-related knowledge and skills, enabling them to identify, respond to, and manage various network risks and threats [15].

6. Conclusion

With the rapid development and widespread application of Internet technology, computer network and database security management are facing new situations, tasks, and challenges. Therefore, in the context of the new era, enterprises should fully recognize the importance and urgency of computer network and database security management. They must establish and improve their security management systems and working mechanisms, increase investment in security measures, and actively implement effective strategies to enhance the technical

prevention capabilities of their personnel. This will improve the level of computer network and database security management and work efficiency, thereby laying a solid foundation for the sustainable development of enterprises.

Disclosure statement

The author declares no conflict of interest.

References

[1] Dai X, 2022, Optimization of Computer Network and Database Security Technology. Computer Enthusiast (Popular Edition), 2022(8): 4–6.

[2] Qin R, 2023, Analysis of Security Management Technology of Computer Network and Database. Application of Integrated Circuits, 40(1): 122–123.

[3] Ren H, 2020, Research and Application of Computer Network Database Security Management Technology. Science and Technology Information, 18(36): 22–24.

[4] Zhang T, 2023, Research on the Application of Security Management Technology in Computer Network Database. Computer Knowledge and Technology, 19(7): 92–94.

[5] Deng J, 2024, Security Management Technology of Computer Network and Database. Digital Design, 2024(7): 56–58.

[6] Wu J, 2024, Application Research of Security Management Technology in Computer Network Database. Information & Computer, 36(4): 175–177.

[7] Dai X, 2022, Optimization of Computer Network and Database Security Technology. Computer Enthusiast (Popular Edition), 2022(8): 4–6.

[8] Wang H, 2022, Research on Security Management Technology of Computer Network database. Proceedings of the First Education, Teaching and Practice Research Forum, 202: 1–6.

[9] Cao F, 2022, Analysis of Security Threats and Countermeasures in Computer Network Database. China Strategic Emerging Industries, 2022(8): 92–94.

[10] Qiao Z, 2012, Research on Security Management Technology Based on Computer Network Database. Information Record Material, 23(1): 83–85.

[11] Li L, 2016, Security Threats and Countermeasures of Computer Network Database. Network Security Technology and Application, 2016(10): 80–81.

[12] Ye J, 2022, Discussion on the Security Problems and Solutions of Computer Network Databases. China Management Informatization, 2022(14): 208–211.

[13] Jia S, 2012, Research on Security Management Technology of Computer Network Database. Electronic Components and Information Technology, 6(4): 164–167 + 178.

[14] Lin T, 2012, Analysis of Computer Network Security Problems and Countermeasures Under the Background of Big Data. Computer Knowledge and Technology, 18(12): 28–30.

[15] Luo Y, 2018, Analysis of Security Threats and Countermeasures in Computer Network Database. Computer Fan, 2018(8): 38.