TEST Engineering & Management

July-August 2020
ISSN: 0193-4120 Page No. 5226 - 5230

Analysis of Security Guard Technology of Information Database Based on Computer Modeling

Wenyan Deng[1,*]

[1]InformationTechnology Department, Shanxi Professional College of Finance, Taiyuan, Shanxi, China, 030024

Article Info
Volume 83
Page Number: 5226 - 5230
Publication Issue:
July - August 2020

Article History
Article Received: *25 April 2020*
Revised: *29 May 2020*
Accepted: *20 June 2020*
Publication: *28 August 2020*

Abstract

With the development of social economy and technological level, major changes have taken place in the network and application technology. Network architecture, basic operating systems and information security play an important role in the construction of enterprise informatization and we must optimize it as the focus of the informatization construction process. Enterprise basic network is the foundation and key of enterprise informatization construction and operation. The basic operation system is an operable platform that adapts and satisfies users for data and information exchange. Information security is an act of security protection and control for enterprise data exchange. These three aspects all affect each other's basic informatization degree and network security and also affect the future development direction of enterprise informatization. Therefore, strengthening enterprise computer network database security management technology plays an important role in the development of enterprise informatization. The creators and administrators of computer network databases have imperfect database management systems and the information administrators are concurrently responsible for security management. The information administrators' insufficiency in the technology and level of security management has led to insufficient energy in network security management. In terms of management, there is a lack of implementation efficiency of measures, so this article effectively improves it.

Keywords: *Computer Modeling, Information Database, Security;*

1. Introduction

Strengthen protection measures for all kinds of data in the database to effectively eliminate and reduce the probability of data destruction and leakage, so that the security of database data is effectively protected, so that the security, independence, integrity, availability and authenticity of the data , Auditability is achieved. The security protection for the database includes the security protection of the main computer system and the security of the database itself. In order to ensure the security of the system, effective means must be adopted to avoid serious damage to the system due to computer attacks; at the same time strengthen protection The security of the information system prevents database data information from being stolen or destroyed due to the intrusion of illegal programs. In addition, while effectively protecting the security of computing operating systems, it is also necessary to fully consider the security of peripheral devices such as database servers. The network database is a constantly expanding and improving existence. In the context of the big data era, a large amount of data is constantly generated, transmitted and deleted on the network at any time. The amount of data in the database will inevitably increase with the increase of users. Including a large number of paper documents also need to be converted into digital information to ensure long-term storage without loss of materials due to the life of the paper and other factors. As the amount of data continues to increase, the need for storage space expansion will also arise.

Published by: The Mattingley Publishing Co., Inc.

July-August 2020
ISSN: 0193-4120 Page No. 5226 - 5230

In many cases, a database with a small storage space, or even a single database, cannot meet the information storage needs. The security management technology is a technology that exists to ensure the integrity of the database. The use of security management technology can prevent information loss and tampering in the database. This is the basic requirement for maintaining the integrity of the database[1].

2. Risk analysis of computer database

2.1. Trend of attack diversification

At present, various attacks against databases and information systems are becoming increasingly diverse. In the context of the development of big data technology, the degree of informatization in various industries has been greatly improved, which has also brought about increasingly severe security problems for information systems.

With the application of big data technology, various advanced technologies play an important role in the development of various fields. At the same time, the application of big data also provides more diversified channels and forms for attacks. In addition to the past Trojan horse viruses and hacker attacks, there have also been attacks such as network disconnection attacks and denial of service and the use of mail transmission ports, data collection ports and other ports as attack channels seriously threatens the security of information systems. The computer security system is in the figure below.

Figure1. Computer security system.

2.2. The rapid growth of system vulnerabilities

Among the security risks, it is easy to cause insecure factors in databases and information systems and the reason for the increase in attack behaviors mainly comes from the vulnerabilities in the database and there are many types.

With the continuous advancement of information technology, the vulnerabilities in the database are also increasing; software vendors continue to develop and launch various application software, which brings great convenience to people's life, learning and entertainment, but lacks a unified system framework, Technical specifications and data exchange modes, resulting in increased data and information risks during data access and transmission and increased system security vulnerabilities, which adversely affect the security of data and information systems[2]. The computer security management system is in the figure below.

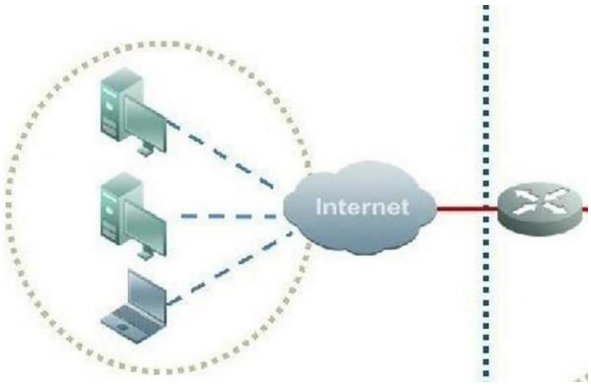

Figure2. Computer security management system.

3. Information database design

3.1. Security management mode

The security management mode in the computer network database is one of its most important prevention and control technologies. The main purpose is to strengthen the integrity of the network database and optimize the security management of the network database. The network database security management mode needs to be implemented more thoroughly. It can effectively improve the security operation level of the network database and prevent possible large-scale information leakage.

Published by: The Mattingley Publishing Co., Inc.

July-August 2020
ISSN: 0193-4120 Page No. 5226 - 5230

Under the mode of security management, the entire network database data is mainly stored in the form of multi-level storage, but because the data types of the databases stored by each information subject are not the same, so in the face of different data types, it adopts data protection The methods are also different. In this way, data classification management can meet actual needs, which is of great significance to the improvement of the security level of data resources and can also improve the optimization of overall data resources[3]. The computer security machine is in the figure below.

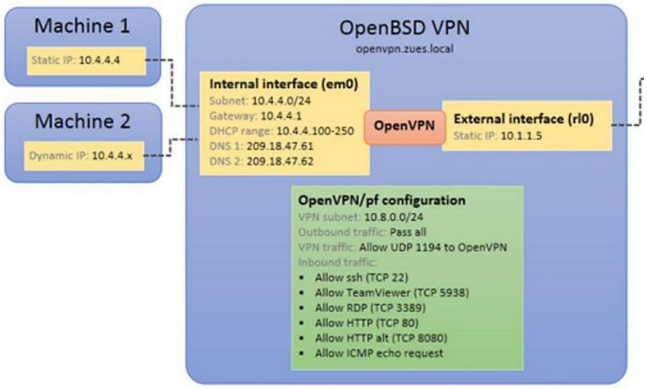

Figure3. Computer security machine.

3.2. Access control technology

The computer must set the access authority during the process of data access. If users want to access the computer network database, they must be authorized or authenticated by the system so that they can access the database. If a non-authenticated user appears in the permission application, the computer network database may involve the corresponding permission binding force in the data reading process.

If non-personnel access to the computer network database is allowed, it may have a serious impact on database resources and directly destroy its database Security. In-depth research on access control technology will be able to effectively improve the targeted effects of such problems, thereby improving the security management of computer network databases. The computer security network is in the figure below.

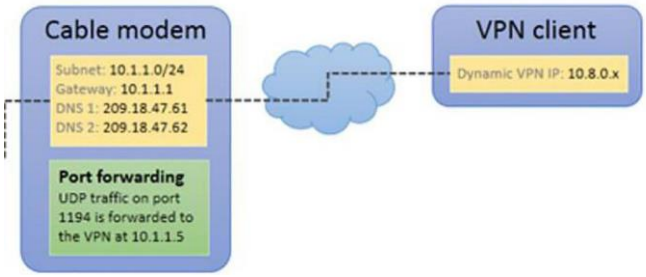

Figure4. Computer security network.

3.3. Data encryption technology

Data encryption technology is now an important technology for computer security management. At the same time, as an efficient security method, it can use different data encryption for specific languages and then carry out detailed data privacy protection work. In this way, all the information in the computer network database can be placed under the safety and reliability standards, thereby effectively promoting the normal operation of the computer network database. In recent years, the data encryption technology in the network database has been greatly improved and the function of encryption in advance has been added. At the same time, the data can be encrypted in detail, comprehensively used and the computer network database can be encrypted in a reasonable way. Ensure the security of the database[4]. The computer security firewall is in the figure below.

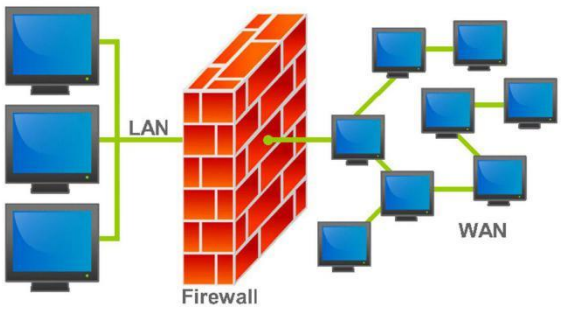

Figure5. Computer security firewall.

4. Security precautions of information database

4.1. Scientific use of virus killing technology

During the operation of the computer network database, hackers may use computer viruses to

Published by: The Mattingley Publishing Co., Inc.

July-August 2020
ISSN: 0193-4120 Page No. 5226 - 5230

invade the computer system, allowing the information and data in the database to be stolen. With the updating and upgrading of computer technology, the spread of computer viruses has accelerated.

Once infected, computer viruses will spread rapidly and the concealment of computer viruses will increase, with the characteristics of cross infection and strong replication capabilities. Affected by the characteristics of computer viruses, it is difficult to detect and kill them in time and effectively remove them, which poses a huge threat to the security of computer network databases. Since there are relatively many viruses in computer network databases, it is difficult for technicians to check and kill viruses in all directions. Installing anti-virus software will help improve the quality and efficiency of virus checking and killing.

After using the anti-virus software to carry out the virus detection and killing work, it is necessary to conduct a comprehensive inspection of the virus detection and killing results, analyze whether the virus detection is comprehensive and clean, find out the missing viruses in time and adopt effective virus detection and killing techniques.

When a computer system is infected with a Trojan horse virus, there will be many variants of the Trojan horse virus. It is often difficult to effectively eliminate the Trojan horse virus if the traditional method of detecting and killing the Trojan horse is simply adopted. In response to this situation, the Trojan horse detection technology developed by a professional security technology company can be used and then a sound and complete Trojan horse analysis and processing system can be constructed. Based on the files submitted by users with hidden security risks, the Trojan horse virus can be quickly analyzed and committed to creating safety and security. Suitable computer network environment[5]. The computer security wireless system is in the figure below.

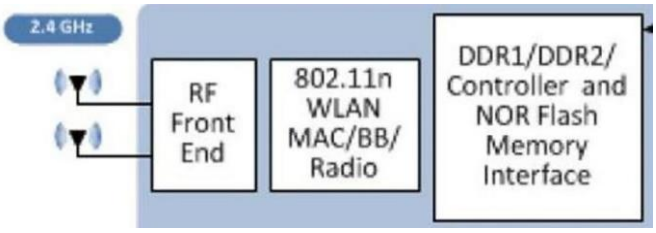

Figure6. Computer security wireless system.

4.2. Reasonable use of safety management model

In the implementation of computer network database security management, security management mode is an extremely important link. In order to effectively enhance the security performance of the computer network database, the security management model must be used scientifically to optimize the computer network database. Computer network databases involve internal and external networks and have a relatively wide operating range, which increases the number of factors that threaten the security of the database. For this reason, when carrying out safety management work, it is necessary to comprehensively analyze each element. By rationally using the safe network management model, effective management methods and countermeasures can be adopted to maintain the security of the computer network database, so that the security performance of the computer network database can be enhanced. By analyzing the current security management model, it can be seen that there are mainly three models: static hierarchical model, centralized management model and distributed management model. The second one has a relatively broad application scope. Based on the security management model, it can carry out classified storage and management of computer data information and implement differentiated security management mechanisms under the guidance of data levels, so that the security performance of computer network databases can be improved.

4.3. Scientifically use encryption technology among them

In order to maintain computer information security, it is necessary to scientifically use data encryption technology. By using this network security

Published by: The Mattingley Publishing Co., Inc.

July-August 2020
ISSN: 0193-4120 Page No. 5226 - 5230

technology, it can effectively prevent computer viruses. With the aid of data encryption technology, the corresponding language program can be applied to the computer to carry out encryption processing on the computer network database. With the rapid development of science and technology, a variety of information encryption technologies have been developed. Confidential communication and computer keys are very common encryption techniques. Encryption technology can enhance the ability of computer network databases to resist virus intrusion, prevent information leakage and other problems and effectively maintain the security of information and data transmission. Relevant technical personnel must clarify the necessity of database encryption, scientifically use multi-level division, screening and other forms to carry out encryption processing and operations, so as to improve the quality of security management and maintain the security of computer network databases[6].

5. Conclusion

Computer network database is the basic technology of network platform construction under the background of big data and its important influence penetrates various platforms. Governments, enterprises and institutions and individual users all need to rely on network databases to collect, store and delete important information. But it is precisely because a lot of important information, even information related to national security, is stored in the database, we must pay more attention to the application research of computer network database security management technology, through continuous research, to ensure that the advantages of network databases are reflected. Meet the needs of the public in production and life.

References

[1] Newly Independent States; Lukashenko claims to have assigned security guards to protect Tikhanovskaya staff overnight[J]. Interfax: Russia & CIS Military Information Weekly,2020.

[2] Lukashenko claims to have assigned security guards to protect Tikhanovskaya staff overnight[J]. Interfax: Russia & CIS Military Newswire,2020.

[3] Wiwynn Corporation; "Firmware Security Guarding Method And Electronic System Using The Same" in Patent Application Approval Process (USPTO 20200226262)[J]. Computer Technology Journal,2020.

[4] Wiwynn Corporation; "Firmware Security Guarding Method And Electronic System Using The Same" in Patent Application Approval Process (USPTO 20200226262)[J]. Computer Technology Journal,2020.

[5] Badger Technologies; Badger Technologies Introduces PatrolBot Autonomous Robot for Security Guard Industry[J]. Computer Technology Journal,2020.

[6] Daniel Best,Gavin Blisset. The Marine Security Guards and the Evacuation of U.S. Embassy Caracas[J]. Leatherneck,2020,103(7).

Published by: The Mattingley Publishing Co., Inc.