Advances in Computer, Signals and Systems (2023)
Clausius Scientific Press, Canada

DOI: 10.23977/acss.2023.070405
ISSN 2371-8838 Vol. 7 Num. 4

Research on Network Security Management Technology

Yuan Yuan

Xinjiang University of Political Science and Law, Tumushuk, 844000, China

Keywords: Network security, management technology, study

Abstract: Network security management technology mainly refers to a technical form to protect the data and information security of computer networks when transmitting and storing information. It has been widely used with the popularization of computers. However, in this context, computer networks have also encountered many security threats, which has gradually attracted people's attention to computer network security management technology to ensure computer network security. In view of this, this paper will analyze the computer network security management technology for your reference only.

1. Introduction

Network security will not only affect the interests of individual users, but also affect government agencies, enterprises and financial institutions. In the past, it was difficult to control and manage products in a centralized way, which would greatly affect the actual effect of safety management. When threatened by network security, the previous security management products are scattered and heterogeneous products, and it is difficult for them to achieve high-level linkage, which will greatly increase the effectiveness of network security prevention. In order to better ensure network security, people should pay attention to the research of network security management technology and constantly improve the comprehensive level of network security management technology, so as to create a better network environment.

2. Overview of Network Security Management Technology

2.1. Concept Analysis of Network Security

Network security is a broader concept, which not only refers to the security of the network, but also involves the security of various software, hardware and data levels during the use of the Internet. Network security is the basis of information security transmission, and it is also an important means for network users to safeguard their legitimate rights and interests. In network security management, personal data information has the characteristics of confidentiality, authenticity and integrity. If people want to achieve this goal, network security must be ensured and avoid such information from being infringed by criminals.

2.2. Development of Network Security Management Technology

Network security management technology mainly refers to the technical means used when transmitting and storing data and information. At the beginning of the development of network security management technology, people paid more attention to its convenience and spread the technology on this basis.[1] However, this will also lead to some deficiencies in network security management technology, and it is difficult to provide a strong guarantee for network security management. With the development of the times, people's application of network is more common, and the threat of network security problems to people is also increasing. In order to better cope with this change, people should pay attention to the innovation and optimization of network security management technology. After a period of development, network security management technology has integrated identity authentication technology, data encryption technology, firewall technology and security management technology, and built it into a more perfect security technology system. In the network security management technology, security vulnerability scanning technology is also very important. With this technical means, people can automatically scan the vulnerabilities of computer networks, complete the corresponding vulnerability repair, and better protect the security of computer networks. However, many current network security management technologies are difficult to achieve technical connectivity when they are threatened, which will greatly affect the preventive effect of network security.

3. Problems Existing in Network Security Management

3.1. There are Management Loopholes

In the past network security management, there were some loopholes in many websites and servers. For the website, there are many loopholes. Although enterprises can fix them, it is difficult to eliminate all the loopholes, which will lead to a great threat to the safety of the website. Due to management loopholes, it is easy to lead to the disclosure of personal information on the website, which is used by criminals to launch fraud activities with the help of leaked information.

3.2. Telecom Operators' Subjective Consciousness is not Strong

To improve the level of network security management, telecom operators need to participate actively, because operators should not only provide Internet access services, but also bear the responsibility of network security. In the network security management, the role played by telecom operators cannot be ignored. However, at present, many telecom operators pay more attention to the development of their own business, and will focus on the pursuit of interests, ignoring the network security management. If there is a loophole in the telecommunications system, the information security and privacy of users will be greatly threatened, resulting in immeasurable losses.

3.3. The Level of Management Technology needs to be Improved

In recent years, China's mobile Internet has developed rapidly, and the corresponding number of users has greatly increased. By the end of 2022, China's mobile Internet users accounted for 98.6% of the total number of Internet users, which also proved the rapid development of the mobile Internet. In practice, the mobile Internet is mainly divided into three levels, terminal level, application level and software level, and there will be certain network security risks in different levels. Taking the terminal level as an example, many tablets and mobile phones will be invaded by Trojan virus, and it is difficult to thoroughly understand them by current technical means. At the application level, some software will get a lot of permissions when it is installed. Some permissions are not related to the functions of the software, and even involve the privacy of users. These authorizations will greatly affect network security.

3.4. Network Security Management is Lagging Behind

With the wider application of the network, the number of network users has been greatly improved. Under the background of the era of big data, all kinds of data are updated quickly, which leads to a certain lag in network security management. In recent years, in various industries, the application of big data has become more and more extensive, and it has become a key technology for the long-term development of many industries. In the network security management, big data has also been deeply applied. At present, there is a strong lag in network security management technology. On the one hand, the management department ignores the development of corresponding technical means. On the other hand, many management software manufacturers are highly dependent on technology, and if there is a problem, if there is poor communication with the manufacturers, it will increase the effect of affecting network security management. In addition, the current network security management lacks foresight, and it is difficult to accurately predict the possible network security problems, which will make it difficult for network security management to keep up with the development pace of network security threats, and many problems can only be dealt with afterwards, which will make it difficult for it to grasp the development direction of the information of the times, which is not conducive to the improvement of network security management level.

3.5. Influenced by Human Factors

Among the network security factors, human factor is one of the most important factors, and many network security problems are caused by human factors. Generally speaking, human factors are mainly divided into intentional and unintentional. Unintentional human factors are usually users' own negligence, such as users' weak awareness of network security, too simple user passwords and accounts, and even lending their user names and passwords to others, which will greatly increase network security risks. Intentional human factors mainly refer to consciously launching cyber-attacks, such as hackers. Hackers usually attack other people's network information consciously and purposefully for their own personal interests, thus destroying the authenticity and integrity of website information or stealing important information from users. When a network attack is launched, it will probably lead to the collapse of the user's network system, which will not only affect the work of the system, but also lead to the loss of some system information.

4. Typical Security Management Architecture

4.1. Multi-Agent Structure

This structure is widely used in network security management, and it is a structure based on mobile proxy server method. Under the distributed system, agents will be divided into different types, and then combined with different modes, so that agents can cooperate with each other to ensure the security of the network system. For the multi-agent structure, having the corresponding self-care function is its main feature. With the help of this function, the system can selectively process messages, thus ensuring the stability of system performance and improving the efficiency of system security management.

4.2. Web Based Management

In fact, the network security management system is a form based on the network management mode, and the network security management itself is closely related to the network. Therefore, people can try to create a network security management system with the network management mode. This mode can provide better network information and information links for the system with the help of the network management system more efficiently, and then lay a solid foundation for the expansion of the safety management system and make it better realize various safety management functions.

4.3. Modular Construction

Modular structure belongs to a new architecture, which is characterized by greater flexibility. It is constructed by different plug-ins, components and components. Modular structure can effectively provide security services, processing services and other functions, and also has certain decision-making statistics functions. In addition, the modular structure is very convenient for assembly and disassembly, which has great advantages in practical application. In the construction of network security management system, people can combine the actual needs to organize and combine the modules, and then the corresponding network security management function can be realized.

4.4. Hierarchical Model Structure

Hierarchical model structure belongs to a vertical design system, and it is also one of the forms of network security management system. In the design, the hierarchical model structure should start with the network protocol and start the system design work. Through the hierarchical model structure, people can effectively solve various problems of heterogeneous and distributed network systems. In the design practice, people can use the corresponding security nodes to deal with heterogeneous problems among various protocol layers. Hierarchical model structure needs the help of global security management system to play a better role, and it also has strong flexibility. It can reconfigure the protocol layer according to actual needs. In order to better cope with security threats, it can deploy the protocol layer under complex conditions, which greatly improves the application effectiveness of the model structure.

5. Research on Security Strategy

5.1. Policy Model Layer

When developing the safety management system, people should pay attention to the research on the strategy model, which is also an important basis for developing a high-quality safety management system. [2]By developing the strategic model, the information and management framework in the security management model can be accurately described by combining the policy grammar, thus ensuring the reasonable realization of the corresponding business functions. At the same time, on this basis, the information of strategic architecture can be fed back to the application layer, which lays a solid foundation for policy analysis. In the process of formulating the policy model, detailed policy description information is not required.

5.2. Policy Presentation Layer

The main function of the policy presentation layer is that it can accurately describe the policy structure, and combined with the policy presentation layer, it can better express the policy content, so as to assign the policy to the corresponding service interface more efficiently. Compared with the policy model layer, the policy presentation layer needs a higher level of expression ability, which also indicates that the information in the presentation layer will be more diverse and rich. When developing the strategy presentation layer, many description languages are used, such as event description language and object description language, and some languages are based on logical description. Generally speaking, logical description language has a more perfect structure, but it is difficult to understand and is more difficult in practical application. For example, RDL is a typical logical description language. Ponder is a typical object description language, which has strong expressive characteristics and can make the described object easier to understand.

5.3. Strategic Mechanism

When studying the policy mechanism, people should do a good job in designing the corresponding policy mechanism and analyze the policy effectively, so that the policy analysis can better solve various practical problems, which plays an important role in improving the level of network security management. By analyzing security policies, policy redundancy can be effectively avoided, which ensures that each policy has strong practicability. From the perspective of strategic conflict, its types are very diverse, mainly including formal conflict and service conflict, and strategic analysis can effectively eliminate conflicts between different strategies. When carrying out the strategy analysis activities, if the strategy conflicts are found, the system will give corresponding hints according to the actual situation, and then the staff can eliminate the strategy conflicts manually. In addition, people can also eliminate strategic conflicts through static testing, which is also an important means to improve the effect of eliminating strategic conflicts. Before the actual application of security policies, the system can carry out static test on them. If there are conflicts between different policies, the system will automatically remove them, thus ensuring the security of the system. [3]The reason why the policy mechanism should be formulated is to enable the system to implement the corresponding security policies more efficiently and reasonably, thus ensuring network security.[4-6]

6. Conclusions

To sum up, in the new era, information technology has been more widely used and developed, which will not only bring people more convenience in life, but also effectively promote the further development of social civilization. In this process, many network security problems have appeared, which greatly hindered the healthy development of information technology. In order to ensure people's information security, people should pay attention to the development of network security management, and combine with the corresponding network security threats to create a more reliable, perfect and intelligent network security management system to further improve the level of network security management.

References

[1] Yan Li. Application Analysis of Computer Information Management Technology in Network Security. Academic Journal of Engineering and Technology Science, 2019, 2(5).

[2] Jianlei Zhou. Discussion on the Technology and Method of Computer Network Security Management. IOP Conference Series: Materials Science and Engineering, 2017, 242(1).

[3] Wei Jiang. Study on the application of computing cloud technology in network security management system. Bio Technology: An Indian Journal, 2014, 10(13).

[4] Almorsy M., Grundy J., & Müller I. (2016). An analysis of the cloud computing security problem. arXiv preprint arXiv:1609.01107.

[5] Catteddu D. (2009). Cloud Computing: benefits, risks and recommendations for information security. In Iberic Web Application Security Conference, Springer, Berlin, Heidelberg, 17-17.

[6] Dawoud W., Takouna I., & Meinel C. (2010). Infrastructure as a service security: Challenges and solutions. In the 7th International Conference on Informatics and Systems (INFOS), 1-8.