Research on Innovative Development of Classification Protection System for Information Security in China

Yifan Jin

PLA Information Engineering University，100# Science Avenue, High-Tech Zone, Zhengzhou, Henan, China

Keywords: Information security, Classification protection, Classified protection

Abstract: The system of classification protection of information security is the basic mechanisms, strategies and methods of national information security work. The rages of the Trojan horse and the hacker require the classification protection system for information security to be constantly updated to adapt to the development of the times. From three innovation aspects of grading system, design system and environmental system, this paper expounds the innovation and development of information security classified protection system in China, and gives corresponding safeguard measures to provide some references for the relevant researchers.

1. Introduction

Classification protection system for information security refers to the classified management system of information and information system and the the classified work system of the information security products [1]. According to the degree of importance of information system in national security, economic development, social life, and the information system after the destruction of national security, social order and public interests, and citizens, legal persons and other organizations of the legitimate rights and interests of the damage degree, the information system security levels can be classified into five grades from low to high [2]. At the first level, the destruction of information system will cause damage to the legitimate rights and interests of citizens, legal persons and other organizations, but it will not damage national security, social order and public interests. This level is the user's independent protection level. It is entirely up to the user to determine how to protect the resources and how to protect it. The second level, the destruction of information system will seriously damage the legitimate rights and interests of citizens, legal persons and other organizations, or do harm to social order and public interests, but it will not damage national security. This level is the system audit protection level. The third level, when the information system is damaged, will cause serious damage to the social order and public interests, or damage the national security. This level is a security mark protection level. The fourth level, when the information system is damaged, will cause serious damage to the social order and public interests, or cause serious damage to the national security. This level is a structured protection level. The fifth level, when the information system is damaged, will cause particularly serious damage to the national security. This level is the access verification protection level.

2. System Innovation of Classification Protection for Information Security in China

2.1 Grading System Innovation

We must first perceive what the danger is and what the innovation is. In the implementation of the grading guide, we accurately classify the grading system, starting from the protection of information and computing two dimensional resources. According to the degree of importance in national security, economic development, social life, and the destruction of system factors to determine the level of the harm [3]. To fill in the two tables, the first table is the level of business information and the second table is called the system service level. For the data information, that is, the hardware facilities for the

completion of the computing task, the hierarchy protection system is required. After putting forward the concept of cyberspace, these data information can be global or interconnected data information, and system and equipment platform components for processing and transmitting data information. Therefore, our country has established very early to determine the classification with two dimensions, which is very scientific. So, we see cloud computing, large data, and a system rating from two dimensions, and the cloud computing rating system should have four features. First, the business process is complete; second, hardware equipment is relatively independent; third, unified security management; fourth, multistage interconnection isolation, a lot of different levels of cloud computing system, this system should be isolated. Now with specific design requirements, we can guide our construction work very clearly. At the same time, we need to carry out good grading evaluation work. We should choose not only good rating agencies, but also make evaluation plans, carry out evaluation work, issue evaluation reports, invite experts to conduct reviews, and further improve the system through the evaluation work, find out problems and correct them. After improving the system, it not can protect in the whole process, so we can be do the active response and active defense.

2.2 Design System Innovation

For the first time of the implementation and operation of classified protection, it will inevitably bring about the transformation of the information security management system [4]. We should perfect the information security level protection management system and landing management system for grading protection evaluation. We strictly review top-level design and program. We invite experts in the field of information security level protection to conduct a strict review of the top-level design and solutions to ensure the correctness of the top-level design. The design principle requires that the security design from two aspects of technology and management should be trusted. For the construction of computing resources to protect the environment, the trusted computing base, layer by layer expansion, for the protection of the computing resources, the corresponding service system, equipment must be reliable, not damaged, continued system operation; second, controllable, according to the information resources business application flow control chain construction, to access control as the core, the implementation of the main press rule access object, equipment support data processing should be controlled, strictly control; third, can assure the safety of the resources, we must carry out scientific management, emphasizing the least privilege management, especially the three level system to implement the separation of three rights management system, do not allow a super user. Overall defense, partition isolation. We should strengthen the overall protection of grading object information system, and build the protection architecture of computing environment, regional boundary and communication network supported by the management center, and implement multi-layer isolation and protection, to prevent some weak links from affecting the overall safety. The revision of grade protection standard is to modify other standards according to this framework. The core technology is using hierarchical protection to solve previous passive defense problems. To realize the level protection is to realize the change of passive defense into active defense. The virus, Trojan horse and hacker are isolated under the support of trusted computing technology. At the same time, when we prevent the safety problems of the core technology of the manufacturer, it has a serious impact on the information security of the construction unit.

2.3 Environment System Innovation

Cloud computing means that the information processing process is completed in the cloud computing center. Therefore, the cloud computing center is responsible for the safety and security tasks, and is responsible for the behavior security of the information system users. Using cloud computing services, the user is not aware of the location of the specific hosting server of its own data and which server management is specific. The level of the hardware and software systems is responsible for the cloud computing center, and the business information system level task is responsible for the user, so this is a hotel service model. In the past, users of various industries have set up their own guest houses, each household has its own office automation, and its resources are wasted, but we can focus these services on cloud platforms. Cloud computing center can run multiple

different security level information systems at the same time. The security level of cloud computing center is no less than that of the highest-level information system. The center of cloud computing is the same as the original computing center. The computing task is also achieved through the external network terminals and the cloud computing center resources to complete the computing task. Cloud computing is not the same as the original device, but the service way is different. For each application, each computation task is used to satisfy the users' terminal needs, and the computing task is completed through the network computing environment. Cloud computing has system management and security management as well. However, this model has some differences, the same is the three architectures, but the virtual cloud computing center to solve resources, if used to satisfy the calculation, there must be trust guarantee system, to ensure that the technology equipment distribution can not only meet the calculation, but also conforms to the technical requirements, maintain a credible. The storage of the data in the cloud service is shared, which is not an independent storage area for the user. The data is potentially dangerous. Compared with traditional software, the biggest difference of cloud computing in data is that all data are maintained by third parties. And because of the characteristics of cloud computing architecture, these data may be stored in scattered places and are stored in plaintext form. We need to develop additional data isolation mechanism to ensure the confidentiality of data between each customer and provide the corresponding disaster recovery plan.

3. Safeguard Measures of System Innovation of Classification Protection for Information Security in China

3.1 Enhance Security Awareness

In order to ensure information security management, it is necessary to strengthen the propaganda and investment of the level of information system security. The main method is to regularly carry out information on the staff's information system related meetings, protect the university leaders and related departments of the central content, vigorously promote the importance of information security work, and enhance the safety awareness in the actual information system. Security protection is not an absolute concept. It can only guarantee the safety of information to a certain extent. The reason is that the safety needs come from the security risk, which is the most fundamental definition of risk. Therefore, to reduce people's unnecessary investment in information protection, it is necessary to have a certain understanding of the protection level of information security in advance. Nowadays, there are many models of information security management in our country. The main consideration is the security assessment model of the information level protection. To get more accurately the security risks that the information system is facing or will face, we will establish a scientific safety assessment relationship model according to the relevant regulations of the world and China. The protection of information security level is an essential part of this society. Therefore, learning to protect their information scientifically and rationally has become one of the skills that people must master in the new era. The research in this area has only just begun in recent years, and the research object is mainly focused on the organization structure, the establishment of business system and so on. There is still a lot of space for the establishment of the information security assessment system. However, our government has attached great importance to information security. The opportunities to provide scientific research funds and the opportunity to study abroad are increasing, which indicates a good development trend.

3.2 Increase Research Investment

Without a strong technical group as a pillar, the security of the information system will become an empty talk. In terms of the safety level of protection, especially from the assessment and correction of technological capability, it is very important for two attentions to cultivate and improve technological capability. The establishment of the model is based on risk. It covers all kinds of risks and risks that the information system is facing. The purpose is to find out the risks and vulnerabilities faced by the

information system, and repair them in time to protect the safety of information. At present, the establishment of China's level of risk protection calculation model is mainly used by the comprehensive way, there exists a need for security risk assessment of information assets threats, and even related factors are considered, and then by level multiply calculated to face the problem of risk. The most important part of the information security level protection is to establish the risk assessment method. It runs through the whole process of information security level protection, including two aspects of quantitative analysis and qualitative analysis. Among them, the quantitative analysis is the statistical data information presented in tabular form, to construct a mathematical model, and then according to the established mathematical model to calculate various information indexes needed; and qualitative analysis compared to quantitative analysis, the initiative has stronger. It mainly relies on the intuition and experience of the analysts, and makes a judgement for the nature, characteristics and development rules of the protected objects. The scientific nature is not high, and it is easy to get errors due to the reasons of the evaluators themselves. As a result, it is more suitable for areas with relatively poor economic conditions or uneven data.

3.3 Strengthen Operations Management

We should do well in operation management of computer rooms and important systems and devices, and even establish operation and maintenance monitoring system. At the same time, the measures of network security protection and system disaster tolerance backup are implemented, and emergency response plan is perfected to ensure the security of network, system and host. From the surface to the point, from the details to the whole, the safety protection model is carried out to the whole life cycle of information security. We need to strengthen the protective surface by technology and management measures. Information security is more important than other enterprises and institutions for the government departments that perform administrative functions and powers. Security attack and defense technology and security threats are changing rapidly, making the security and protection work of the government information system difficult to work for once and for all. The work of information security and protection should be given to the dynamic safety planning safety service lifecycle, regular risk assessment, constantly discovering new security threats and vulnerabilities, security architecture and revised measures to increase the establishment of complete safety management system, equipped with full-time security personnel, and establish and improve the responsibility and supervision mechanism, establish a set of management procedures and management system, system monitoring, fault alarm, fault analysis, report, through the collaborative efforts of all parties related to security agencies, government departments jointly safeguard network system security. The standard of safety inspection is not only a large amount of work, but also a more professional content. In the evaluation work, each inspection standard is checked by the project team of the equal insurance evaluation and feedback modification. During the period of the reexamination of safety classification protection, the head office will organize the inspection team, check and confirm the evaluation problems according to the inspection instructions in the inspection specification, and further improve the operability of the inspection specification.

4. Conclusion

With the rapid development of information technology, the international situation of information security is becoming more and more severe. Classification protection system of information security is an information security guarantee that works in the whole life cycle of the information system. We should constantly improve the technical standard system and the implementation of the guarantee mechanism to meet the information security needs in the new situation

References

[1] Yang zhigang, Wang Qiang. Initial construction and application research of information security class field protection [J]. New Technology & New Process, 2017(4): 62-64.

[2] Li Jun. Comparison of CPIS and ISMS [J]. China Quality and Standards Review, 2017(8): 58-63.

[3] Huang Shaoqing, Liu Guowei, Yue Youbao, et al. Discussion on the basic Unit of Network and Information Security Emergency Classification [J]. Computer Security, 2014(11): 56-58.

[4] Xie Maosen, Yang Qing. Application of Fuzzy Comprehensive Evaluation on the Level of Security Classification Information System [J]. Journal of Chongqing Normal University (Natural Science), 2014, 31(5): 89-94.