Research on Information Security Risk Analysis and Preventive Strategies of E-government Based on Hierarchical Structure

Zhijie Li

Guangdong Mechanical & Electrical Polytechnic, 510550, Guangdong, China

Keywords: Informatization Construction; E-government; Economic Development; Government Departments

Abstract: At present, China's information construction has entered an important period of comprehensive promotion and acceleration of development. Information system has become the nerve center of key infrastructure in energy, transportation, finance and other countries. E-government cloud has great advantages in reducing e-government costs, promoting information sharing and business collaboration, and improving the efficiency of e-government deployment. E-government can undoubtedly greatly improve administrative efficiency, but at the same time it makes the government information security face a huge threat. China's e-government has achieved good results in a relatively short period of time, and most units have established a complete infrastructure and numerous application systems. A large number of government departments will be completely unable to carry out normal work and will directly have a huge negative impact on local economic development. In view of the shortcomings and hidden dangers of traditional information security measures in e-government, this paper introduces a new solution for information security platform.

1. Introduction

At present, China's information construction has entered an important period of comprehensive promotion and accelerated development. Information system has become the nerve center of key infrastructure in energy, transportation, finance and other countries [1]. The essence of e-government is to move towards public government, that is, the government will turn itself into a service-oriented government. Strengthening the construction of e-government is of great significance to improving public service ability and social management level, and we must pay enough attention to it [2]. The construction of E-government information system must be consistent with the functions of government agencies at all levels, and the information security measures adopted are consistent with the security requirements of the basic operating system of government agencies at all levels [3]. China's e-government has achieved good results in a relatively short period of time, and most units have established a complete infrastructure and numerous application systems. E-government is the use of modern network communication and computer technology by government agencies. The internal and external management and service functions have been streamlined, optimized, and reorganized to the network [4]. The demand for security in e-government is comprehensive, and trust and authorization services are also difficult in the traditional way.

National critical infrastructure and important information systems are increasingly dependent on the network, and administrative and public services at all levels of government are increasingly being implemented through networks [5]. The rapid development of e-government is of great significance for promoting the transformation of government functions, increasing administrative transparency, improving work efficiency, and reducing administrative costs [6]. To understand the security needs of e-government, we must first understand the relationship between government affairs, e-government and information security needs. Traditionally, the construction mode of engineering and construction projects has generally caused problems such as low resource utilization, poor data sharing and business coordination, and difficulties in system management and maintenance [7]. If the lack of electronic information technology means, or if the security problems

lead to the normal operation of e-government system. A large number of government departments will be completely unable to carry out normal work, which will directly bring huge negative impact on local economic development [8]. Traditional technical solutions are often based on foreign hardware platforms and operating systems, so it is fundamentally unable to provide adequate security.

2. The Importance of Information Security in E-government System

In e-government systems, there is a general lack of good digital signature measures. Many systems are simply designed to enter names to indicate signatures. Since the operation of e-government is mainly supported by network and information technology, the core content of E-government security is information security. With the construction and wide application of e-government system, information technology plays an increasingly important role in the normal operation of government organs. Some systems use handwriting, while others use email senders to authenticate. At present, there are some problems in information security in China's e-government. The e-government network is relatively fragile and various security risks are widespread. In order to speed up the need for informatization construction, the state has introduced a large number of foreign basic equipment and lacked effective management and technological transformation of the introduced information and technology. Judging from the current situation of the e-government network, it should be said that the destruction of physical isolation is the most harmful security damage. With the development of information technology, information security issues are becoming more and more complicated. The existing information security legal framework has been difficult to adapt to the requirements of e-government development.

In the construction of a specific e-government system. The specific information security must be based on the analysis of the characteristics of specific government services. Security threats that exist in the system's operating environment must be considered. Accelerating the construction and application of the e-government cloud platform is a phased and important task to promote the healthy and orderly development of e-government. The trust service system mainly provides a reference for the network information space to establish a trust relationship between the user entity and the user roles in the virtual network space [9]. In order to transplant the trust relationship in the real physical world into the virtual cyberspace. A lot of security protection is based on the assumption that the government intranet is physically isolated from the government extranet, and the government extranet is logically isolated from the Internet. Once physical isolation is destroyed, the security of e-government network will be greatly compromised. Although China has issued some laws and regulations related to network security, the current policies and regulations are still difficult to meet the needs of network development. Safety requirements put forward by government business are the basic basis for determining functional safety requirements. The analysis of the threat to the system's operating environment is the basis for determining the specific parameters of functional safety requirements and their own safety requirements.

In order to implement the decision-making at the decision-making level, we need a management level to manage the daily work and an executive maintenance level responsible for implementing the security plan and decision-making. Thus, a hierarchical information security organization is formed, which is directly led by the Chief Information Officer. The security organization includes the organization decision-making layer, the management control layer and the execution and maintenance layer, as shown in Figure 1.

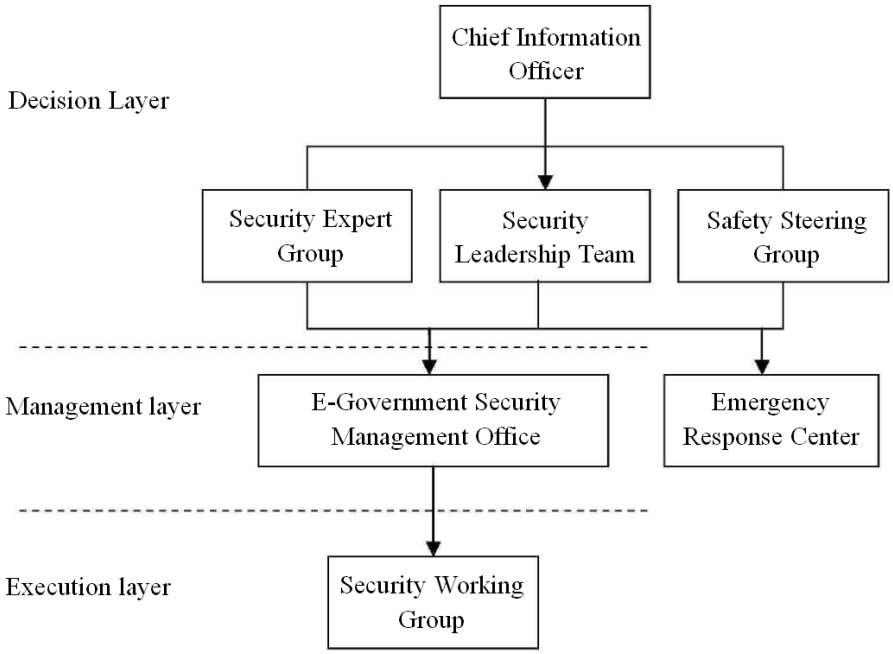

Fig. 1 Hierarchical Information Security Organization

E-government systems are operating in a certain geographical environment, and the threat of natural disasters to information systems is also very serious. Perfecting the legal norms of information security guarantee is not only the means and methods to improve the ability of information security guarantee, but also the premise and guarantee of improving information security technology. At present, the country lacks an information security planning and management organization with the highest authority, which can undertake the planning and management of information security projects consistent with the national information process. Like all technologies, information technology is not perfect, there are limitations, loopholes and defects. E-government refers to the use of modern network communication and computer technology by government agencies. The government management and service functions are implemented on the Internet through streamlining, optimization, integration, and restructuring. Because the main leadership work of various departments is very much, the informationization work is only a part of its many work, and it is impossible to put all the energy into it. It is necessary to improve the quality of safety management personnel and strengthen the education and management of personnel and network users within the system.

3. Problems in E-government Information Security

The organizational system of E-government security is an important foundation to ensure the implementation of security. The establishment of an organizational system should be complete and efficient. The network is very fragile, and various security risks are common. People who have mastered certain technology can easily obtain user account information and password files on the network server. In order to ensure the normal performance of the functions of government organs, it is a basic requirement to ensure the confidentiality of information. Compared with the traditional e-government system, the security problem of e-government cloud is more serious, and the consequences caused by the failure of security measures are more serious. The authentication system provides access authentication services for local government network. It can be a separate network device that uses a disconnected way to connect the local network to other networks [10]. The informatization leading group is led by the main leaders of all levels of departments, and governments at all levels attach great importance to informationization. Its position plays an important role in information security, especially as China's information technology is relatively backward. Although China has formulated some policies and regulations for illegal information such as computer viruses, information infringement and cybercrime. However, due to poor

implementation, the effect is not obvious.

The security of e-government as a part of maintaining the order of cyberspace requires relevant regulations. To protect and coordinate the interests of various network application subjects, we must aim to guarantee the order of the real world. The use of advanced and reliable security technology is a powerful guarantee for maintaining information security. Most security incidents and security risks occur not so much as technical reasons, but rather because of management. There are different levels of network security vulnerabilities in mainstream operating systems, and most network communication protocols are not designed for secure communication. In recent years, the practice of E-government in the world has made developing countries realize that e-government is not only an opportunity for economic and social development, but also a tool to achieve leapfrog development. In practice, special attention should be paid to distinguishing which requirements are determined by business characteristics and which are determined by traditional business operation modes. E-government is an important means for the government to transform its functions and improve its administrative efficiency. It is also an important part of the public service system.

In their information security laws and policies, all countries have clearly defined the responsibilities of the national information security management agencies and various agencies. At all levels, we strive to achieve division of labor, responsibility and responsibility. In order to effectively implement these security measures and have the legal basis for their implementation, it is particularly necessary to formulate laws and regulations to guarantee network security. Operating system provides users with convenient communication functions and sharing settings, but also provides opportunities for illegal elements. Non-malicious threats are attacks on the government information system caused by the unintentional behavior of legitimate users. They do not intentionally destroy information and systems. The authentication system issues a request for the certificate to the address, and the user submits the certificate to the authentication system upon receiving the request. Only authenticated users are allowed to enter the local network. Strengthening the construction of e-government is of great significance to improving public service capacity and social management level, and must be given sufficient attention. E-government is a combination of technological innovation and management and institutional innovation. The development of government-led e-government will bring profound changes to the government's management style.

4. Conclusion

Security is the guarantee of the application, and security is for the application. When designing an e-government information security system, it should be based on practical applications. From the construction process of the local isomorphic rootless authentication system, it can be seen that the system can be constructed from any part. The construction of an e-government system information security system is a complex system engineering. When formulating policies and laws, we must pay special attention to compatibility with existing international rules, including compatibility with legislative ideas, methods, and specific legal provisions. E-government information system is a large-scale system engineering, it must work according to certain standards as far as possible. At present, only the authorization process for government staff is considered in the corresponding task authorization stage, and the process is task-driven. By means of combining management with technology, we can improve the overall defense capability of E-government information system and ensure the information security of E-government effectively. We should strengthen the research and development of independent intellectual property security equipment, speed up the process of localization of security equipment, and change the situation of dependence on foreign security technology and equipment.

References

[1] Ismailova, Rita. Web site accessibility, usability and security: a survey of government web sites in Kyrgyz Republic[J]. Universal Access in the Information Society, 2017, 16(1):257-264.

[2] Yoo J, Chang H. Public IT service strategy for social information security in the intelligence all-things environment[J]. Electronic Commerce Research, 2014, 14(3):293-319.

[3] Fan J, Zhang P, Yen D C. G2G information sharing among government agencies[J]. Information & Management, 2014, 51(1):120-128.

[4] Boyle M J, Horowitz M C, Kreps S E, et al. Debating Drone Proliferation[J]. International Security, 2018, 42(3):178-182.

[5] Osman I H, Anouze A L, Irani Z, et al. COBRA framework to evaluate e-government services: A citizen-centric perspective[J]. Government Information Quarterly, 2014, 31(2):243-256.

[6] Alawneh A, Al-Refai H, Batiha K. Measuring user satisfaction from e-Government services: Lessons from Jordan[J]. Government Information Quarterly, 2013, 30(3):277-288.

[7] Susanto T D, Goodwin R. User acceptance of SMS-based e-government services: Differences between adopters and non-adopters[J]. Government Information Quarterly, 2013, 30(4):486-497.

[8] The imperative of influencing citizen attitude toward e-government adoption and use[J]. Computers in Human Behavior, 2015, 53:189-203.

[9] Fernandez E B, La Red D L, Peláez, José I. A conceptual approach to secure electronic elections based on patterns[J]. Government Information Quarterly, 2013, 30(1):64-73.

[10] Leuprecht C, Skillicorn D B, Tait V E. Beyond the Castle Model of cyber-risk and cyber-security[J]. Government Information Quarterly, 2016, 33(2):250-257.