Study on the Protection of E-Government External Network Level Protection

Changxu Cai ¹

¹Qujing normal college, yunnan qujing city kirin sanjiang avenue, 6550111
495546192@qq.com

Keywords: E-Government external network; Class protection; Grade protection assessment

Abstract. Information system level protection system is one of the important measures to strengthen the information system security protection in our country, e-government network running public services of e-government, the protection level protection and level measurement is very necessary. In this paper, the author discusses the grade protection evaluation of the network system in the external network system, discusses the grading of grade protection, the selection of the evaluation object and the evaluation institution, and the safety rectification.

Background of National E-Government External Network Level Protection

Government affairs outside the network security of e-government applications and carried by the data to provide the network load and safety protection, from the external network attacks, viruses and abnormal traffic monitoring, and constantly improve the network and information security emergency disposal and emergency response capacity ^[1]. For further national e-government network outside the network and information security work, improve the capability and level of e-government network outside the network security, should actively carry out e-government network protection grade, grade protection system, national information security protection system to implement step by step to the outside of the e-government network planning, construction, test and operation maintenance and application and so on each link, make government affairs outside the network security capacity of security protection grade of ^[2].

Information security rank protection work is the main content of the information system (including network) according to the importance and the dangers of after suffering damage is divided into five levels of security and protection (from the first level to level five, increased step by step). After the grade is determined, the above information system shall be filed with the public security organ for the record, and the public security organ shall issue the record certificate after the examination. According to the security level of the information system, the unit shall carry out safety construction rectification according to national policies and standards. The public security organ directs the secondary information system and conducts regular supervision and inspection on the third and fourth information systems ^[3].

The Necessity of the Evaluation of E-Government External Network Level Protection

Measurement of the level of protection is assessment institutions according to the information security rank protection regulations of the state, in accordance with the relevant management norms and technical standards, to involve state secrets the grading information system security protection for testing activities. For protecting assessment level is an important measures to improve the service level of e-government, by conducting assessment is a master e-government network information system security situation, screening system safety hidden trouble and weakness, clear information system security construction improvement needs; The second is to be able to measure whether the security protection measures of the information system meet the basic requirements of grade protection, and whether they have the corresponding level of security protection ability.

Discussion on the Evaluation of E-Government External Network Level Protection

Protection Level

The key to the protection of external network level is wan and all levels. The class is an important system of network and security system, network management system, security management center (SOC), DNS, etc. Government affairs, the central government to the province, to network (city) wide area network and the central, provincial, (city) man should meet the requirements of security rank protection the third level, county (city) to for wan and man at least above ground (city) level to protect the second requirement. According to the national requirements and specific e-government network, a network system for the government the network level 3, e-government network, a network management system for the second to the public security bureau of organs for the record, and elevate the grading scheme of state information center.

Determination of the Evaluation Object

According to requirements, grade protection class system will be conducted once a year of protection measure, accept the supervision and inspection, more than one will put on record for level 3 of outside the net a network system for evaluation. The evaluation time is to carry out the grade assessment before the construction rectification, the current situation analysis. Assessment project main objective is to use professional qualifications of bidders and the safety management of project implementation experience, with reference to national standards and industry characteristics and security requirements, a network system level protection in government affairs outside the net assessment, dig potential safety hazard and vulnerability, appropriate safety recommendations, through the relevant units and special reinforcement of manufacturer's technical personnel set up e-government network outside the network system security management system, promote e-government network security ability and the level of safety management, gradually will be outside the e-government network security situation to meet the requirements of the state government affairs outside net protection level 3.

Evaluation scope: (1) the scope of network and node: government affairs at the provincial level to the local wide-area networks outside the backbone, transverse metropolitan area network at the provincial level (including core node at the provincial level, provincial and municipal convergence node); (2) external network management system; (3) related equipment of security management system and safety protection related to the network system of the external network system (such as firewalls, IPS, security audit, etc.).

Selection of Evaluation Institutions

According to industry evaluation institutions within the industry to carry out the assessment in principle, measurement of the local agency in principle at the request of the local to carry out the assessment, released from the public security organs of the catalogue of national information security rank protection assessment agencies recommend selecting national and provincial level protection work coordination group office (led) is recommended, and familiar with e-government assessment institution, and asked to participate in the evaluation, The engineer has the information security rating center identified by the ministry of public security information security assessment center and senior qualification evaluation teacher quality.

Evaluation Contents and Methods

The key to the protection of external network level is wan and all levels. The class is the network and security system, the network management system, the security management center (SOC), etc. The object of this evaluation is machine room, network interconnect equipment, safety equipment, safety management system and so on. According to the information system security level protection evaluation criterion, on-site assessment methods include inspection, interview and test three categories, such as a variety of evaluation methods have their own advantages, have their own focus, the evaluation of the three kinds of comprehensive use of assessment method.

Interview is assessment personnel by people (individual/group) in connection with the information system for communication, discussion and other activities, obtain evidence to illustrate the effectiveness of information system security level protection measures a way; Check is different from the administrative law enforcement in the sense of the supervision and inspection, "means the

assessment object through the assessment activities, such as observation, inspection, analysis, to obtain evidence to illustrate the effectiveness of information system security level protection measures a way; Test is assessment personnel through to the evaluation object according to the predetermined method/tool to produce the activities, such as specific behavior view, analyzing the output, obtain evidence to prove that information system security level protection is an effective method.

Configuration check list for all kinds of security vulnerabilities in the system of artificial assessment/vulnerability, it has been listed according to different system for assessment items, to ensure the completeness of artificial assessment data. Automatic test automation system has the characteristics of high efficiency and fast speed.

Specific evaluation content is divided into physical security, network security, the host system security, data security, application security and security management institutions, safety management system, personnel, security management, system construction and management and operations management aspects.

Key Network System Vulnerability Test

There are different security domains in the e-government external network, different security domains exposed to different levels of security are different, and it is necessary to test the vulnerabilities exposed between different security domains. A network system to test the government the network backbone network vulnerabilities, need a permeability test, between the same security domain, low security domain to high security domain, low security domain to high security domain between vulnerability exposure test, design test the following path:

In the city A node scan other local B node network interconnection equipment, can verify the same level different security domain network equipment vulnerability exposure situation.

In the cities of core network equipment at the provincial level D C node scanned from lower security domain to high security domain scanning equipment, can test the protective ability of the core layer equipment external attack.

At the provincial core backbone equipment E node, the scanning of the ground city node F is to directly test the security holes of the network equipment exposed to the core network directly in the core layer. The number of holes detected in this spot should be the most, indicating the security situation of network equipment without network security protection.

Safety Rectification and Filing

Through on-site assessment, risk analysis, and preparation of assessment reports, the assessment agencies should provide a preliminary assessment report. Safety rectification is a gradual process, can't do all at one time repair reinforcement with system security vulnerabilities, according to the preliminary assessment report and safety recommendations, to network hole configuration vulnerability, host system configuration and security system, operating system vulnerabilities, vulnerability database system, on the issue of safety management system of the safety measures, and repeatedly requires a security assessment institution improvement effect assessment, check whether safety has reached the expected goal. After many safety rectification and after inspection, complete the XX government affairs outside a network system level protection assessment report and the XX government affairs outside a network system level protection measure safety recommendations ", protection grade assessment projects through the panel after acceptance, the dependency assessment report to the public security organ for the record.

References

- [1] national e-government external network management center. National e-government external network security implementation guide (trial), December 2013.
- [2] national e-government external network management center. Notice of speeding up the promotion of the protection of the security level of the national e-government external network [2011] no. 15, 2011.
- [3] chil-chyuan kuo. State information security protection system, and the main contents and requirements of <http://wenku.baidu.com/view/5a4ef8c54028915f804dc279.html>, in October 2013.