Research on Classified and Hierarchical Grid Enterprise Operational Data Security Management

Xin Jiang

Information and Communication Branch of State Grid Fujian Electric Power Co., Ltd., Fuzhou, Fujian, 350001, China

Keywords: Data security management, Hierarchical grid enterprise operation, Information

Abstract: The safety of power information system and power production safety are equally important. With the rapid development of communication technology and information technology, power companies have already realized informatization of production and operation, automation of grid dispatching, marketization of network operations, and modern management, all of which have provided great convenience to the operation and development of power companies. At the same time, the negative impact of the network has penetrated into all aspects of power companies and power production. Information security issues still occur from time to time, posing a serious threat to the safe, stable and high-quality operation of the power system. This article summarizes and analyzes the problems of power system information security threats and information operation, and discusses the countermeasures of power information security from the aspects of power information system security education, security management and technical measures.

1. Introduction

The operation data of power grid enterprises is a true reflection of various resource inputs, process conditions and output effects of business management activities such as planning and design, investment construction, power grid operation, marketing services, etc., involving a large number of trade secrets and user privacy information. With the rapid development of advanced technologies such as “Big Cloud Mobility”, the sources of operational data are more abundant, the acquisition is more convenient, and the dissemination is faster. The extensive application of big data analysis and mining technology enables deep mining of the rich information contained in operational data. If it is not effectively protected, it is likely to cause the leakage of corporate trade secrets and sensitive information, and damage the corporate image and even the interests of users. In order to effectively cope with new technical challenges, it is necessary to conduct systematic research on the confidentiality management methods of operational data, effectively strengthen the protection of data assets of power grid enterprises, and avoid data loss and leakage incidents while meeting the necessary internal and external needs.

2. Analysis of Security Threats Faced by Electric Power Information Systems

The computer information network system in the power system has covered all links of the entire power enterprise. Computer viruses are no stranger to everyone. They can attach themselves to various types of files, and when files are copied or transferred from one user to another, they spread along with the files. It is fast and difficult to eradicate. Therefore, computer users of the power system may be attacked by viruses at any time when they exchange and share a variety of information and data.

One is malicious intrusion. Some people use network attacks to invade the power system network, commit fraud, theft, malicious destruction, malicious code, and infringe on the privacy of others. Achieve your own evil purpose. The second is malicious web pages. There are many web pages that have the function of Trojan horses. When users of power system computers browse the web to find useful information for themselves, the machines are planted with Trojan horses, which leads to information leakage.

DOI: 10.25236/ieesasm.2020.112

Various hidden dangers may be left in the design, manufacture and assembly of power information system components. At the beginning of the design of the Internet, only the issues of interconnection and resource sharing were considered, and it was unable to compatiblely solve a large number of security problems from the Internet. With the use of software, the conditions that the software is exposed to are becoming more and more complex, which exposes its own defects that have not been discovered.

3. Problems in the Safe Operation of Power Information

In recent years, with the rapid development of information network technology, its technology and security have been significantly improved to a large extent. But as far as the application of computer networks in the information systems of our power companies is concerned, the power companies pay attention to the effects of the network, thus ignoring network security. From top to bottom, there is a psychology of fluke, and there is no information security awareness of active prevention and active response. Information security issues still occur from time to time.

The information security management mechanism is not perfect. At present, my country's electric power enterprises attach great importance to the safety of electric power information systems and have begun to take a series of control measures. However, a complete information security management standard has not yet been formed and cannot play a good guiding role for the entire electric power information system.

The system boundary security protection is weak, and security risks still exist. The external security of information networks is the key to the security of power information systems, and it is also one of the important factors that are often ignored by power companies. The replacement of the internal LAN by Internet management has brought speed to the operation of the information management system of electric power enterprises, and also brought security risks. The existence of network threats such as viruses and hackers can easily cause system security problems, and the inattention of power companies can easily cause operational failures.

4. The Construction and Application of a Confidential Management System for the Classification and Classification of Power Grid Enterprise Operating Data

The whole-process confidentiality management of operational data refers to the creation, storage, use, archiving, and destruction of operational data throughout the life cycle. It focuses on confidentiality and aims at zero loss of confidentiality. It establishes a complete organizational system, clarifies confidentiality responsibilities, and controls operational data. A management approach for effective control and prevention of confidential data, confidential personnel, and confidential equipment in each link of the life cycle business process, so as to achieve the purpose of ensuring the security of the company's operational data. The steps for constructing a confidential management system for the entire process of classification and grading of power grid enterprise operating data include the following.

Comprehensively interpret the regulations and clarify data confidentiality requirements. National laws, regulations and policies are the institutional basis for companies to carry out confidential management of business secrets, including operational data. Through detailed interpretation of the confidentiality management related policies of the government, industry and superior companies, the company clarifies the confidentiality management regulations and requirements of business secrets that companies must follow, and combines the current status of the company's own confidentiality management and future development needs to establish confidential management requirements for corporate operating data.

The system identifies data characteristics and determines key management and control nodes. The operation data of power grid companies comes from various professional lines and management fields such as power grid planning, investment and construction, power grid operation and maintenance, and marketing services, and is stored in multiple business systems such as ERP and PMS. Through detailed analysis of the various stages of operation data from generation, circulation, use to archiving or destruction, the main characteristics of each stage of its life cycle are identified, and the initial source, transmission path, involved positions, application value and data application of different types of operation data are determined The frequency and scope of the operation data, and so on, thus clarify the key nodes for carrying out the whole-process confidential management of operational data.

Construct a classification and grading model to refine the evaluation of data confidentiality. In view of the characteristics of multi-field data sets generally used in data analysis applications, starting from the three dimensions of secrecy, confidentiality, and value, the secrecy, value and confidentiality period of each field in the data set are quantitatively evaluated, divided into Three categories 1, 2, and 3; determine the confidentiality level of the entire data set according to the number of fields of 1, 2, and 3 contained in the data set, divided into three levels 1, 2, and 3, and use the decision tree classification method to construct the fields Class-level operational data classification, hierarchical confidentiality evaluation model, solidify evaluation rules, and refine confidentiality standards.

Clarify data confidentiality responsibilities and establish a whole-process confidentiality management system. In order to achieve the goal of zero-leakage confidentiality and effectively organize and carry out the confidential management of operational data, it is also necessary to use scientific management methods and advanced technical tools to establish a full-process confidentiality management system, including a responsibility system, a management control system, and an assessment and evaluation system. Strengthen the prevention and pre-control of the confidentiality risks of operational data. Among them, the responsibility system is the guarantee for implementing the responsibility of the confidentiality management system, clarifying the organization, division of responsibilities, and management of confidential personnel involved in the confidentiality management of operational data; the management and control system is the operating mechanism of the confidentiality management system, which clearly includes daily inspection, supervision, and early warning of leakage The whole process management and continuous improvement mechanism including emergency response and accountability; the assessment and evaluation system is the basis for promoting the implementation of the management and control system, and the assessment and evaluation methods corresponding to the responsibility system are clearly defined. One is to strengthen identity authentication. In the intranet of the electric power enterprise, each user has to enter the computer system with his own password (password) for operation. Users should keep their user names and passwords, so that the passwords meet the requirements and regulations of system management. The second is to choose a suitable vulnerability scanning system. Scan each port of the network system, detect loopholes, and analyze loopholes to find loopholes that may be exploited by hackers. Thereby it can effectively solve the harm caused by the defects of the software itself. Effectively improve the network security level. The third is to configure the firewall reasonably. The firewall is the primary option to ensure the network security of the power system. The third is to isolate different areas of the power information network. Set up a physical isolation device. Prevent hacker attacks. At the same time, an intrusion detection system and a network hidden danger scanning system should be installed in the power network. Check power information security around the clock. Fourth, in order to prevent accidental damage from causing information loss and network paralysis, it is necessary to make a backup of network information and systems in advance. Electric power companies should establish data backup centers to regularly back up power information data and systems. It is necessary to formulate a database failure recovery plan for frequent drills so that it can quickly recover when the system is paralyzed by various natural disasters.

The operation monitoring business of power grid enterprises uses a large amount of cross-professional, cross-departmental, and cross-unit operational data. It is necessary to take the lead in applying the classified and hierarchical whole-process confidentiality management system for the business secrets and work secrets generated or involved in the business development process.

The author elaborated on the classification and evaluation of operational data fields, which vividly demonstrated the process of classification and evaluation of operational data fields. Step 1:

Classify the data fields according to the business content reflected in the existing business operation data fields. Such as industry expansion report installation data, measurement data, customer information data, etc. Step 2: Determine whether the business data is within the confidentiality period based on the time limit for confidentiality of business secrets of the enterprise and the time when the data is generated. Step 3: Evaluate the degree of confidentiality based on the degree to which the data is known to the outside world. Internal operating data that is not known to the outside world has a high degree of secrecy; those that are known to the outside world or the data itself comes from outside have a medium degree of secrecy; those that are widely known to the outside world or need to be disclosed in accordance with relevant laws and regulations have a degree of secrecy. low. Step 4: According to whether the information is sensitive, whether the leakage of secrets has caused the loss of the company or customers, etc., evaluate the value of the business operation data, which is divided into three levels: high, medium and low: once the leakage of secrets, the company’s management or customers and other related parties Those that have a significant impact are “high”, those that have a certain impact are “medium”, and those that have no obvious impact are “low”. Step 5: According to the confidentiality period, confidentiality and value of the business operation data, determine the category of each data field according to the operation data classification evaluation model, and form a classification table of various business operation data.

5. Conclusion

Constructing a hierarchical classification evaluation model based on the characteristics of power grid enterprise operating data can realize field-level confidentiality attribute evaluation, and transform the confidentiality of operational data from qualitative to quantitative. Determine the confidentiality management process, related job responsibilities, assessment methods and evaluation standards according to the circulation links of operational data, positions involved, and potential risks, etc., which can clarify the confidentiality management responsibilities at each stage of the operational data life cycle, and make the confidentiality of operational data from extensive to refined change. The establishment and application of a classified and hierarchical confidential management system for the entire process of operating data will help improve the overall level and work efficiency of corporate confidentiality management of business secrets, strengthen the prevention of risks of loss of confidentiality, and enhance the level of standardization.

References

[1] Chen An, Wang Chong. Whole-process confidential management of grid enterprise operating data based on classification and classification. Chinese and Foreign Entrepreneurs, vol. 2, no. 11, pp. 101-102, 2018.

[2] Zhou Xiang, Xu Jianbing, Li Min, et al. Classification and hierarchical process management and control to ensure controlled use of data-State Grid Shanghai Electric Power Company operational data confidentiality management practice exploration. Confidential Science and Technology, vol. 7, no. 8, pp. 56-59, 2017.

[3] Tao Zhenwei. Discussion on Classification and Management Strategies of Enterprise Sensitive Confidential Data. Modern Industrial Economics and Informatization, vol. 2, no. 9, pp. 23-25, 2019.

[4] Wang Yan, Wang Feng, Liang Dehua, et al. Research on the Security and Confidentiality Management of Computer Networks in Electric Power Enterprises. Commodities & Quality, vol. 2, no. 13, pp. 23., 2018

[5] Liu Yuting, Zhou Jing, Su Yongdong, et al. Research on Data Security of Power Grid Enterprises Based on Business Process Data Sensitivity Level. Mechanical and Electrical Engineering Technology, vol. 2, no. 5, pp. 48-51, 2015.