WEP Warwick Evans Publishing

International Journal of Computer Science and Information Technology

ISSN: 3005-9682 (Print), ISSN: 3005-7140 (Online) | Volume 2, Number 2, Year 2024
DOI: https://doi.org/10.62051/ijcsit.v2n2.26
Journal homepage: https://wepub.org/index.php/IJCSIT/index

Advancing Power System Resilience through Information Network Security

Ziyu Lin

School of Computer Science, Shanghai University, Shanghai, China
Ziyulin292@163.com

ABSTRACT

With the continuous development of informatization in the power industry, the importance of information security is becoming more and more prominent, and the test faced by the increasingly severe. The whole paper analyzes several major sources of threats to the security of the power system and the problems involved in LAN security management, and from the information security technology and management puts forward its ideas and methods to enhance the information security protection capability of the smart grid, enhance the information security of the autonomous and controllable capacity, and to enhance the information security of the power industry.

KEYWORDS

Power System; Network Security; Computer

1. INTRODUCTION

With the development of computer information technology, the dependence of power system on information system has gradually increased, and information network has become an important part of our work[1]. The power MIS system, power marketing system, electric energy and electricity billing system, SAP system, power ISP business, business finance system, human resources system, etc. can be said that the current integration of power resources has completely relied on computer information systems to manage[2].

Therefore, while strengthening the stability of the information system itself, it is also necessary to guard against many security problems on the network, such as attacks using network system vulnerabilities, attacks via e-mail decryption attacks, backdoor software attacks, denial of service attacks, etc.

2. HOW TO DEAL WITH NETWORK AND INFORMATION SECURITY INCIDENTS. TO PLAN INFORMATION SECURITY WELL, WE SHOULD WORK HARD ON BOTH SOFTWARE AND HARDWARE.

First of all, let's talk about the software piece, in fact, this part is mainly refers to the safety and security awareness and coordination of command and operational quality of personnel[3].

As the enterprise information network security architecture, one of the most important part is the enterprise network management system, no equipment and technology to protect 100% of the security of the enterprise network, enterprises should develop a strict network management regulations. Violations of intranet outreach, outside the unit mobile storage media into the intranet and other

behavior should be resolutely investigated and dealt with, and will not be tolerated. Enterprise information network security architecture is not a simple device stacked system, but a dynamic process model, security management issues throughout the dynamic process. Therefore, the network security management system should also be throughout the process[4].

Through the implementation of the policy of "safety first and prevention first", we strengthen the anticipation of network and information system emergencies[5], make preparations for network and information system emergencies, prepare emergency resources and safeguard measures, prepare on-site disposal plans, and form a regular mechanism for regular emergency training and emergency drills, so as to improve the ability of emergency response and comprehensive handling of various types of network and information system emergencies. The emergency response and comprehensive treatment capability for various types of network and information system emergencies are improved.

In accordance with the principles of comprehensive coordination, unified leadership and hierarchical responsibility, establish a systematic and hierarchical emergency organization and command system. It organizes and carries out various emergency response work such as network[6] and information system incident prevention, emergency response, restoration of operation and notification of incidents.

Give full play to the role of the company's expert team and professionals, and effectively improve the business quality of emergency response personnel, regularly participate in the basic knowledge of the grooming and various types of information systems training[7], as well as the assessment mechanism prior to the start of work. To protect the company's normal production, operation, management order, to protect the company's employees information security and confidentiality as a top priority, to minimize the economic losses and damage to the interests caused by emergencies[8].

The hardware part is not only simple network equipment, server minicomputers, UPS and other hardware equipment, but also includes various information systems and network resources required for power production.

Every detail of the above information equipment, information system and the entire network architecture is directly related to the stability of the system operation. In order to ensure the stability of the information system, in recent years, we have gradually increased our investment in hardware equipment[9].

In the purchase of network equipment, we have always selected CISCO brand switches and routers, bandwidth throughput of CISCO switches, IPV6 routing, multicast routing and access control lists (ACLs) The stability of CISCO CATALYS intelligent power management and other technologies is the best among products of the same level. Server minicomputers are mainly IBM, HP and DELL. In terms of server selection, try to be a brand with outstanding reputation in the society to ensure the stability of its operation. Similarly, in terms of software development, it also cooperates with domestic well-known software companies to develop various application systems needed for production, such as the firewall of Zhongruan, the network management software of Beita, and the OA system of ORACLE[10].

In the network architecture, the implementation of border protection through the firewall, as an important part of network security, the firewall is one of the protagonists in the entire network security construction is indispensable, and almost all network security company brand firewall. In the firewall parameters, the most commonly seen is the number of concurrent connections, forget the throughput of two indicators.

The number of concurrent connections refers to the firewall or proxy server on its business information flow processing capacity, is the firewall can simultaneously handle the maximum number of point-to-point connections, he reflects the firewall equipment for multiple connections to the access control capabilities and connection status tracking capabilities, the size of this parameter has a direct impact on the maximum number of points of information that the firewall can support. The size of the throughput is mainly by the firewall card, and program[11].

The efficiency of sequential algorithms, especially program algorithms, will make the firewall system carry out a large number of operations, and the traffic will be greatly discounted. For our large state-owned enterprises, of course, we still choose a 1000M firewall to ensure traffic.

According to the objectives and requirements of "strong logical isolation" of the State Grid Corporation for the construction of the external network, a set of physical external network is re-established in the provincial and municipal power supply companies and units directly under them, which is physically isolated from the existing internal network, and physical isolation devices are installed between the two networks. The Internet exit is located in the provincial electric power company, and the local and municipal power supply companies and directly subordinate units are unified to access the Internet from the exit of the provincial electric power company; after the transformation, the access to the application system of the external network and the related system of the internal network must be carried out through the isolation device.

Access control identifies and verifies users and limits users to authorized activities and resources. This is the basic function that access control security mechanism should achieve. Access control security mechanism can screen and filter malicious access users at the network entrance, which greatly ensures the reliability of network access users. The implementation of access control should first consider the verification of legitimate users, then the selection and management of control policies, and finally the management of no illegal users or unauthorized operations. Therefore, access control includes authentication, control policy implementation, and audit.

At present, the mainstream control technologies include Role based Access (RBAC), Task based Access Control Model (TBAC Model) and Object based Access Control Model (OBAC Model).

Data transmission security requires the protection of information being transmitted over a network against both passive and active intrusion. This is mainly done through file encryption and electronic signatures. Encryption on the network can be divided into three layers: the first layer is the data link layer encryption, that is, before and after the transmission of data in the line of encryption and decryption, so as to reduce the risk of being stolen on the transmission line.

The second layer is the encryption of the transmission layer, so that the data in the network transmission during the encryption state; the third layer of the application layer of encryption, so that the network application program to encrypt and decrypt the data. Often used to make the three layers of comprehensive encryption, in order to enhance the security and reliability of information. Electronic signature is the recipient of the data used to confirm that the sender of the data is indeed a method of error, he is mainly through the encryption algorithms and verification protocols to achieve.

Threats from the network is also a very important point is the danger of viruses. Virus itself is a computer program, but it is used to damage and interfere with the normal use of the computer system or network, through the preparation of the so-called malicious code, to control or spy on computer resources or paralyze the entire network. Computer viruses can be said to be indefensible, summarized the spread of viruses is mainly through the following ways: 1. through the CD-ROM, floppy disk transmission; 2. through the mobile storage media transmission; 3. through the network transmission.

So we can monitor viruses in real time by installing anti-virus software semantic and updating the latest virus database, and deal with them as soon as they are found. Ensure a good network environment.

3. SUMMARY

The application of information technology in the power system is with the development of enterprises and the continuous development of information network security is also a dynamic process, the need for regular assessment of the security status of the information network, improve the security program,

adjust the security strategy. We can not guarantee that we can eliminate all kinds of threats and attacks from the information network, but I believe that through the sense of responsibility and sense of mission of all electric power, we will be able to maximize the protection of power information network security, better service for power production, better service for the whole society.

REFERENCES

[1] Alimi, O. A., Ouahada, K., & Abu-Mahfouz, A. M. (2020). A review of machine learning approaches to power system security and stability. IEEE Access, 8, 113512-113531.

[2] Miraftabzadeh, S. M., Foiadelli, F., Longo, M., & Pasetti, M. (2019, June). A survey of machine learning applications for power system analytics. In 2019 IEEE International Conference on Environment and Electrical Engineering and 2019 IEEE Industrial and Commercial Power Systems Europe (EEEIC/I&CPS Europe) (pp. 1-5). IEEE.

[3] Liang, Y., Wang, X., Wu, Y. C., Fu, H., & Zhou, M. (2023). A Study on Blockchain Sandwich Attack Strategies Based on Mechanism Design Game Theory. Electronics, 12(21), 4417.

[4] Li, X., Wang, X., Chen, X., Lu, Y., Fu, H., & Wu, Y. C. (2024). Unlabeled data selection for active learning in image classification. Scientific Reports, 14(1), 424.

[5] Guo, H., Ma, Z., Chen, X., Wang, X., Xu, J., & Zheng, Y. (2024). Generating Artistic Portraits from Face Photos with Feature Disentanglement and Reconstruction. Electronics, 13(5), 955.

[6] Lee, Z., Wu, Y. C., & Wang, X. (2023, October). Automated Machine Learning in Waste Classification: A Revolutionary Approach to Efficiency and Accuracy. In Proceedings of the 2023 12th International Conference on Computing and Pattern Recognition (pp. 299-303).

[7] Hink, R. C. B., Beaver, J. M., Buckner, M. A., Morris, T., Adhikari, U., & Pan, S. (2014, August). Machine learning for power system disturbance and cyber-attack discrimination. In 2014 7th International symposium on resilient control systems (ISRCS) (pp. 1-8). IEEE.

[8] Ibrahim, M. S., Dong, W., & Yang, Q. (2020). Machine learning driven smart electric power systems: Current trends and new perspectives. Applied Energy, 272, 115237.

[9] Vaish, R., Dwivedi, U. D., Tewari, S., & Tripathi, S. M. (2021). Machine learning applications in power system fault diagnosis: Research advancements and perspectives. Engineering Applications of Artificial Intelligence, 106, 104504.

[10] Belagoune, S., Bali, N., Bakdi, A., Baadji, B., & Atif, K. (2021). Deep learning through LSTM classification and regression for transmission line fault detection, diagnosis and location in large-scale multi-machine power systems. Measurement, 177, 109330.

[11] Azad, S., Sabrina, F., & Wasimi, S. (2019, November). Transformation of smart grid using machine learning. In 2019 29th Australasian Universities Power Engineering Conference (AUPEC) (pp. 1-6). IEEE.