Journal of Computing and Electronic Information Management
ISSN: 2413-1660 | Vol. 12, No. 3, 2024

Critical Infrastructures at Risk Addressing Information Security in Power Systems

Temia Temeglio, Ram Gei

Università Bocconi, Italy

Abstract: According to the power system network security risks and problems, this paper presents the work of information security and the general principles of information security from a technical and safety management put forward the idea of addressing security issues and methods of analysis of local area network security management related to issues, and according to their own experience of a relatively effective way of thinking.

Keywords: Information network; Security management.

1. Introduction

With the development of computer information technology, greatly increasing the power system on the dependence of the information system, the network has become an important part of our work. But when we enjoy the convenience and speed of the network at the same time, but also to face the network open to the data security aspects of the new challenges and new dangers. The spread of viruses is becoming more and more rampant, hacker attacks are also more and more, to the management of LAN data, network security has brought a lot of problems.

It may surprise you to know that every minute, two companies in the world go out of business because of information security problems, and eleven companies have suffered direct economic losses of more than eight million dollars because of information security problems. This is an era in which details determine the success or failure of competition, and a key piece of information can shape the fate of an enterprise. The issue of information security not only involves the survival and development of enterprises, but also involves the economic, scientific and social security of the country, and even jeopardizes national defence, political and cultural security.

However, looking at these many problems, people are the key factor in information security, and at the same time, they are also the weakest link in information security. When the network of hardware and software technology in the era of development of the mainstream level, upgrading the system has been unable to significantly enhance the level of network information security, information systems often depend on the security of the weakest link in the system - people. In fact, many network security problems are caused by the lack of effective implementation of security management, so security management is the core of information security.

2. The main problems of power system information network security

1) Low security awareness

Enterprise personnel are busy using the network to work and study, and have no time to pay attention to the security of network information, and their awareness of security is rather weak. Power enterprises focus on the network effect, but the investment and management of the security field is far from meeting the requirements of security prevention, and the network information security is in a passive state of blocking and blocking leakage.

From the top to the bottom of the general existence of a sense of fluke, did not form active prevention, active response to the national consciousness, more fundamentally unable to improve the network monitoring, protection, response, recovery and anti-attack ability.

2) Informatization institutions and system construction need to be further improved

The information sector has not received the attention it deserves. Information department in the power company does not have a specialized agency configuration, there is no standardized structure and positions, information department attached to the production technology department, some as a science and technology department under the section, some in the general manager of the department under the work of the general manager, there is only set up a "information technology special responsibility" personnel.

Informatization as a systematic project, the need for specialized institutions to promote and enterprise departments to cooperate. This situation will not be able to adapt to the requirements of informatization of talents and institutions.

3) The main manifestations of network information security risks in electric power enterprises

A. The network is not well structured

Power companies according to the relevant provisions of the network is divided into intranet and extra net, internal and external networks to implement physical isolation, but the network structure there are some unreasonable places. Commonly: the core switch selection is unreasonable. Many enterprise network core switch is a layer 2 switch, so that all network users in the network status will be equal, security issues can only be resolved through the application system.

B. Risks from the Internet

Almost all electric power enterprise network is connected to the Internet in various ways, enterprise users can directly access the Internet resources, which brings great convenience to the enterprise workers; Similarly, any user can go on the Internet can also access the resources of the enterprise network, which is very good for publicizing the enterprise, expanding the influence of the enterprise and visibility.

However, in bringing convenience at the same time, also brings security risks. Some users on the Internet for a variety of motives, the power company's network of computer systems and equipment connected to the invasion, attack, etc., affecting the transmission of information on the network, damage to software systems and data, theft of business secrets and confidential information, illegal use of network resources, etc., to the enterprise caused huge losses. What's more, a very small number of people utilize the network to carry out illegal activities that affect the stability and unity of the country, causing a very bad influence.

C. Risks from within the enterprise

For the network of electric power enterprises, the risk from the internal is the main security risk. With the development of network technology, the power system information network has been from the past a small range of local area networks, the development of network terminals tens of thousands of large-scale wide area networks.

Jiangsu Electric Power Company information application centralized integration of the gradual promotion of various applications, including office automation, financial management system, power marketing system, such as production, operation of important systems into online operation, more and more important data and confidential information through the enterprise's internal wide-area.

The information transmitted in the network is subject to various security risks. The information transmitted in the network faces various security risks, such as being intercepted by illegal users, thus leaking enterprise secrets; being illegally tampered with, resulting in data confusion, information errors, thus causing work errors. Illegal users may also pretend to be legitimate, send false information, bring chaos to the normal production and operation order, causing damage and loss.

Therefore, the security of information transmission is becoming an important part of enterprise information security. Internal personnel (especially network managers) on the network structure, application systems are very familiar with the inadvertent leakage of important information, will probably become the most deadly security threats leading to attacks on the system.

D. Virus attack

The threat of computer viruses is the most widespread: computer viruses since its creation, has been the computer system's number one enemy, in the electric power enterprise information security problems, computer viruses occur frequently, the impact of the surface of the broad, and the damage and losses caused by all security threats are listed in the first. Virus infection causes network communication blockage, system data and file system damage, the system can not provide services or even can not be recovered after the destruction, especially the loss of important data accumulated in the system for many years, the loss is catastrophic.

Under the current conditions of local area networks (LANs) and wide area networks (WANs), the spread of computer viruses is even more rapid, and a computer infected with a virus can infect all computer systems in the region within a short period of time. The speed of virus propagation and the scale of infection and damage are several orders of magnitude higher than when the networks were not yet connected.

E. Management quality risk

Many electric power enterprise network exists heavy construction, heavy technology, light management tendency. Practice has proved that the security management system is not perfect, the quality of personnel is one of the important sources of network risk. For example, the network administrator is improperly equipped, the enterprise staff security awareness is not strong, the user password set unreasonable, etc., will bring serious threats to information security.

F. Security risks to the system

The security risk of the system mainly refers to the security risk of the operating system, database system and various application systems. Regardless of which operating system is used, there are a large number of known and unknown vulnerabilities, which can lead to intruders obtaining administrator privileges and can be used to implement denial-of-service attacks.

3. The basic principles for solving cyber security problems in power systems

1) Doing a good job of assessing security risks

The construction of security systems, the first must do a good job of security assessment and analysis of the situation, the assessment should be hired professional authority of the information security consulting agencies, and the organization of internal information personnel and professionals in-depth participation in a comprehensive risk assessment of information security, to identify the problem, determine the needs, formulate a strategy, and then to implement the implementation of the completion of the implementation of the regular assessment and improvement.

The construction of information security systems focuses on security and stability, and mature technologies and products should be adopted as far as possible, rather than being overly ambitious.

The training of information security specialists and the strengthening of information security management must be synchronized with the construction of information security protection systems in order to truly bring into play the role of information security protection systems and equipment.

2) Adoption of new information security technologies and establishment of an information security protection system

Enterprise information security is facing a lot of problems, we can be based on the priority of security needs, to solve the security problems related to the maturity of the information security technology to consider, step by step implementation. Mature technology, can quickly see the results of the first implementation of the security system

A. Establishment of a computerized anti-virus system

Computer antivirus system is the longest development of information security technology, from hardware antivirus card, stand-alone antivirus software to network antivirus software, to enterprise antivirus software, technology is mature and the application of the effect is very obvious. The application of anti-virus software system can basically prevent and control most of the computer viruses and guarantee the security of information system.

In the current network environment, can provide centralized management, automatic server upgrades, automatic update of the client virus definition code, support for a variety of

operating system platforms, a variety of application platforms anti-virus enterprise version of the anti-virus software is the first choice for large enterprises such as power grid companies.

B. Establishment of a network security protection system

The security of access to information resources is an important element of information security, in the design phase of information system construction, it is necessary to carefully analyze and design a reasonable, flexible user management and access control mechanisms, clear access to the scope of information resources, and formulate access strategies for information resources.

For information systems that have already been put into use, it is possible to enhance the user management of the original system and the control of access to information resources, as well as to realize the function of single sign-on access to any system, etc., by increasing the method of security access gateway.

This way basically does not need to change the original system, the implementation of the technical difficulties are relatively small. For the new system, it is better to adopt the unified identity authentication platform technology to realize user management and access control of different systems through the same user management platform.

3) Improvement of safety management in accordance with regulations and standards

The management of information security includes the stipulation of laws and regulations, the division of responsibilities, the planning of strategies, the formulation of policies, the production of processes, the consideration of operations, etc. Although the expression "seven parts management, three parts technology" is not very accurate, the role of management can be seen. Although the information security "seven parts management, three parts technology" is not very accurate, but the role of management can be seen.

4. Measures to Strengthen Cyber security of Power Systems

1) Emphasizing security planning

The purpose of enterprise network security planning is to have a comprehensive thinking about the network security issues, to consider security issues from a systematic point of view. To carry out effective security management, must establish a systematic and comprehensive information security management system.

2) Rationalization of security domains

Power enterprises are completely physically isolated enterprise network, the intranet should still be reasonably divided into security domains. According to the overall security planning and information security level, from the logical division of the core key preventive areas, general preventive areas and open areas, and the use of strict access control policies.

The key prevention area is the core of network security. This area is not directly accessible by ordinary users and has a high security level. All kinds of important data, servers and database servers shall be placed in this area, and all kinds of application systems, OA systems, etc. shall operate in this area.

3) Strengthening security management

In order to ensure the security of enterprise network information, it is necessary to consider enterprise network information security as a systematic project. Therefore, the security of the enterprise network, security management and system construction is very important (especially the intranet). The following recommendations are made.

A. Strengthening log management and security auditing

General firewalls and intrusion detection systems have an audit function, to make full use of their audit function, do a good job of network log management and security audit. Audit data should be strictly managed, do not allow anyone to modify, delete audit records.

B. Establishment of a unified authentication system for the intranet

Authentication is one of the key technologies of network information security, and its purpose is to realize identity identification services, access control services, confidentiality services and non-repudiation services.

C. Establishment of protection systems

Install an anti-virus system on the corporate network. Anti-virus software system should have remote installation, remote alarm, centralized management and other functions. Second, to establish anti-virus management system. Can not arbitrarily download the data on the Internet to the intranet host copy, from an unknown source of mobile storage devices can not be arbitrarily used in the network computer, staff should be proficient in the discovery of viruses after the disposal of the method.

Deployment of Microsoft Update Server on LAN. Many viruses and hackers in the network lead to data corruption and even system crash of the computer, the reason, the operating system, the vulnerability of itself is exploited and attacked by malicious code, which is one of the important reasons for system instability.

Therefore, the immediate improvement of the operating system has become the primary task in the current computer maintenance work. As the system with the largest number of users at present, Microsoft's Windows operating system is also the most concerned and infringed by all kinds of operating systems. In view of the fact that Microsoft's operating system update server is abroad, which results in slow download of updated patches. At the same time, for the large number of LAN users, updating on each machine will bring heavy repetitive operations, Therefore, setting up and deploying a centralized Microsoft software update server in the local LAN has become one of the most effective methods to ensure the timely update of Windows operating systems.

4) Emphasizing the development of network management systems

A. Leaders should attach great importance to the issue of network information security

Enterprise leaders should attach great importance to the construction of security management and security system, and should not regard security management and system construction as the business of technical departments. Enterprises should set up an information security leading group, by the leaders in charge of network security work, and clarify their responsibilities and work system. It is necessary to formulate procedures for handling security incidents and contingency plans.

B. Strengthening the management and construction of infrastructure and operating environment

The management of the enterprise network of computer systems such as computer rooms, distribution rooms and other important infrastructure should be strictly managed, equipped with anti-theft, fire prevention, waterproofing and other facilities, should be installed monitoring systems, monitoring and alarm devices. The establishment of strict equipment operating logs, record equipment operating conditions. To standardize operating procedures to ensure the safe and reliable operation of computer systems.

C. Establishment of the necessary safety management system

The central computer room of the enterprise network and the computer system of each business department should establish a computer system use management system, network system administrators, security officers, heads of business departments and computer operators of the computer password management regulations and other internal control and management system, the modification of the important data of the application system should be authorized and be the responsibility of a person to register the log. The establishment of a sound data backup system, the core program and data should be strictly confidential, the implementation of special custody.

D. Adhere to the principle of safety management

The principle of multiple responsibility: two or more persons should cooperate with each other and exercise mutual control. At least two persons should be present at each safety activity to keep a record of the work.

The principle of limited tenure: no one will hold a safety-related position for a long period of time. When a person leaves a position, the system should be immediately adjusted for authorization.

Segregation of duties: Do not inquire about, learn about, or participate in any security-related matters outside of your duties, unless authorized by the system manager.

The principle of least privilege: only grant users and system administrators the most basic privileges needed, and super-user privileges should be as small as possible.

E. Regular supervision and inspection of the system

The management system is serious, authoritative and mandatory, and once the management system is formed, it should be strictly implemented. Enterprises should organize the relevant personnel to carry out regular supervision and inspection of the management system to ensure the implementation of the system.

1) Strengthening security awareness education for enterprise employees and network administrators

For network information security, the quality of enterprise employees and network administrators is very important. Information security awareness and related skills education is an important part of enterprise security management, the implementation of which will be directly related to the degree of understanding of the enterprise's security strategy and the effectiveness of its implementation.

In order to ensure the success and effectiveness of information security, should be at all levels of management, users, technical staff of the enterprise security training, all enterprise personnel must understand and strictly implement the enterprise information security strategy, through security education to form an important part of the enterprise security culture, to ensure the smooth realization of security management.

A. There should be a certain hierarchy in the concrete implementation of safety education.

For the senior person in charge of information security or managers at all levels, the focus is on understanding and mastering the overall strategy and objectives of enterprise information security, the composition of the information security system, the establishment of the security management department and the formulation of the management system.

For technicians responsible for information security operation management and maintenance, the focus is on fully understanding the information security management strategy, mastering the basic methods of security assessment, and rationally applying security operation and maintenance techniques.

For all employees, the focus is on learning the various safety procedures, understanding and mastering the safety strategies associated with them, including their own safety responsibilities.

B. Specific safety training for specific personnel

For personnel in key positions and special positions, they are sent to specialized institutions for study and training, so that they can acquire specific security knowledge and skills. Through security training, to ensure that in the power information security system is gradually established in the process, all types of personnel security awareness and technical ability to improve the technical and management capabilities of personnel in various positions with the operation and maintenance of the security system to adapt.

2) Security in development

There is no 100% safe technology and protection system hacking technology, computer viruses and other information security attack technology in the continuous development of people's understanding of them, mastery is not complete, security protection software systems due to the complexity of the technology, in the research and development process will inevitably occur this or that problem, which inevitably determines the security protection systems and equipment can not be 100% defense of a variety of known and unknown information security threats. Unknown threats to information security.

People's understanding of information security issues with the development of technology and applications and gradually improve, it is impossible to find all the security problems at once. Information security manufacturers to produce systems and equipment, but also only to meet some aspects of security needs, not a certain aspect of the information security needs of enterprises, the market has a corresponding mature products, so not all security issues can find effective solutions.

Therefore, it is necessary to establish a long-term security mechanism to solve the problem of network information security, take technology as the main body of security, take management as the soul of security, and seek security in continuous development.

5. Conclusion

The application of informationization of electric 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 information network security situation, improve the security program, adjust the security strategy. It should be emphasized that network security is a systematic project, not a single product or technology can be fully resolved.

This is because network security contains multiple levels, both hierarchical division, structural division, but also to prevent differences in the target. Any one product and technology can not solve all levels of the problem, so a complete security system should be a distributed by a variety of security technologies or products constitute a complex system, both technical factors, but also contains human factors. A better security measures are often the result of a variety of methods properly integrated application. A computer network, including individuals, equipment, software, data and so on.

The status and influence of these links in the network, but also only from the perspective of the system as a whole to view, analyze, in order to obtain effective and feasible measures. That is, computer network security should follow the overall security principles, according to the provisions of the security strategy to develop a reasonable network security architecture. This can truly achieve the security of the entire system. Therefore, the author believes that the power system local area network security is an eternal issue that accompanies the development of information technology applications and development.

References

[1] Guo Hulin. Analysis of Enterprise Network Information Security [J]. Computer Security, 2002 (6).

[2] Yan Bin, Qu Junhua, Qi Linhai. Research on the construction scheme of power enterprise network information security system [J]. Computer Security, 2003 (1).

[3] Feng Dengguo. Computer Communication Network Security [M]. Tsinghua University Press, 2004.

[4] Zhu Guiqiang. On enterprise network information security management.2005(6).

[5] Yang Zanguo. On Enterprise Network Information Security and Prevention Strategies [J]. Computer Security, 2005 (6).

[6] Wang Yingxin, Niu Dongxiao. Research on Network Information Security Management of Electric Power Enterprises [J]. Computer Security, 2007 (3).

[7] 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.

[8] 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.

[9] Lee, Zhitong, Ying Cheng Wu, and Xukang Wang. "Automated Machine Learning in Waste Classification: A Revolutionary Approach to Efficiency and Accuracy." Proceedings of the 2023 12th International Conference on Computing and Pattern Recognition. 2023.

[10] 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.

[11] Wang, X., Wu, Y. C., Ma, Z. (2024). Blockchain in the courtroom: exploring its evidentiary significance and procedural implications in U.S. judicial processes. Frontiers in Blockchain, 7, 1306058.

[12] Strahilevitz, L. J. (2010). Reunifying Privacy Law. Calif. L. Rev., 98, 2007.

[13] Solove, D. J., & Schwartz, P. M. (2020). Information privacy law. Aspen Publishing.

[14] Richards, N. M., & Solove, D. J. (2010). Prosser's privacy law: A mixed legacy. Calif. L. Rev., 98, 1887.

[15] Kephart, J. O., & White, S. R. (1993, May). Measuring and modeling computer virus prevalence. In Proceedings 1993 IEEE Computer Society Symposium on Research in Security and Privacy (pp. 2-15). IEEE.