Research On Service Mode of Information Security in Post-construction Era

Qiyao Tang, Yadong Tang
NARI INFORMATION&COMMUNICATION TECHNOLOGY CO.,LTD JiangSunanjing 210000

Abstract: Based on information security service and its characteristics in the development of information technology, author comprehensively analyzes the current situation and development tendency of the industry. This paper puts forward the business mode of the information security operation, and analyzes its model composition, construction process and difficulties that faced in this process. This article can provide certain model reference and theoretical support for the innovation and sustainable development in this business.

Key words: Information security, Safe operation, Information security consulting, Advisory service

Introduction

With the development of cybersecurity, the strategic importance and practical landing of information security has been concerned by various industries, and with this, great amount of security technical service are desperately needed in various dimensions. Information security services and their attached industries may appear a blowout type development. Since the beginning of this century, after more than ten years of construction and improvement, the domestic information field has entered a brand-new era that construction and operation are both taken into consideration equally. As an information security service worker who has been engaged in information security for nearly ten years, the author believes that it is imperative to study how to realize the parallel development of the availability of the main business and its security guarantee, and fully promote the adjustment of the service industry structure and the transformation of the development mode.

Situation of information security service at present

The prototype of traditional information security service is a fundamental operation and maintenance and information consulting, which has developed for more than ten years. The main work are as follows: risk assessment, multiple-level protection scheme, security reinforcement, security inspection and other groundwork for information system. However, with the rapid development of cloud computing, big data, the Internet of Things and mobility, which has completed structure and widely distribution, and the tendency that types of information security incidence and dependence on information technology are both increasing, drawbacks of traditional security services appear gradually.

Furthermore, from the aspects of the administrative section, it is also faced with many problems, such as: a large number of alarm platforms and dynamic supervision technologies are deployed however they cannot meet the requirement for vulnerability mining at all levels. The same is true when it comes to early warning. Technical service of information security which has been gradually carried out through the mode of equipment patrol inspection and security evaluation, but the breadth and depth of coverage cannot support the elimination of emerging security risks, and cannot form a continuous and effective rectification mechanism. According to the analysis, most of them are caused by the disadvantages of traditional security technical services.

Therefore, whether for the increasingly complex situation of information security protection or the requirement of the administrative section, it is urgent to transform the traditional security technical service to a more realistic, efficient and comprehensive mode, which can be more innovative and safer.

Business trends analysis

Based on the research and analysis results of the demand for security services, it is concluded that the user demand has gradually changed into the following three points: first, comprehensive information security talents are required to provide all-round professional security consulting and give overall solutions for the network operation and maintenance team; Second, more attention has been paid to early warning of information security incidents, continuous elimination of hidden dangers and daily security inspection; Third, it can not only meet the practical needs of superior and subordinate agencies, but also give consideration to the long-term development of informatization.

Therefore, the author fully draws on the basic theory of international best practices and combines the current situation of domestic information security services to propose the concept of “security operation”, that is, the mode of information security services is transformed from the traditional “technology output oriented” to the new “talent output oriented”; Change from scattered and temporary evaluation work to establishment of ancillary mechanism and highly thinking of process management and control. Finally, information security

service people and system operation and maintenance people will undertake responsibilities together and improve the security guarantee of informatization so as to realize the synchronization of service security and business support.

Research and analysis of security operation mode

Security operation support takes high-quality service output as the carrier. It is mainly based on the existing platform environment of the system administrative section. Relying on professional technical methods and construction of enhanced working mechanism, maintainers can inspect various hidden dangers, carrying out the security management and control in a whole system lifecycle.

“platform+service” coordinated monitoring

At present, most enterprises with demand of active security service have built security fundamental platforms. “Platform+service” means that company relies on security service team to realize risk troubleshooting, risk analysis and problem elimination with help of security platform warning. The service teams promote the administrative sections and operation units of the system to identify the weakness of the system, improve the emergency response capability, comprehensively complete fundamental environment, system equipment, data protection and other security assurance work, and gradually attach importance to the establishment of information security incident early warning, continuous elimination of hidden dangers, daily security inspection and other mechanisms. As a result, it can meet the customized security assurance needs.

Advanced advisory service

On the basis of previous normalization of security inspection and closed-loop handling of security events, advanced advisory services are carried out in two categories: one is penetration attack- defense and vulnerability mining, and the other is overall solution design .They can actively adapt to new business development, information security protection requirements and management mechanisms. Penetration attack and defense and vulnerability mining regularly carry out verification and comparative analysis of security vulnerabilities facing multiple layers (application layer, network layer, system layer) by professional technicians.

Construction and improvement of safe operation mode

Fundamental concept

The information security operation mode is planned to divide the security operation into four periods, namely: team building, platform integration, capacity improvement, and industry promotion. The four parts can also be disassembled into four construction dimensions.

(1) Team building. The technical service of most security service teams is aimed at training technical experts; however, this target cannot be easily achieved. It is suggested taking conventional service as the carrier in the early stage of work, combining the support of normal employees with the flexible support of high-level stuff, and improve the practical level of the talent team and gradually establish a free human resource pool through the mode of “choose practice to replace training”. Finally, enterprise can build a “chess game” structure layout of the operation team.

(2) Platform integration. That is to gradually eliminate the business gap between the security operation and maintenance people of the administrative section and the regular security service people, so as to understand and connect the business in both directions. The existing SOC system, network management platform or vulnerability awareness tools will be reasonably used as the information source of security operation business, and the alarm response efficiency will be improved as soon as possible to achieve the synchronization and closed-loop of emergency response. Finally, risks will be detected in advance and the occurrence of information security incidents is going to be reduced effectively.

(3) Ability improvement. In the middle of the safety operation business model, we will continuously improve the management mechanism of safety operation workers, introducing assessment methods and ensuring improvement of service quality; try to integrate security operation with inspection business, implementation of hardware product, and software product deployment, and divide most focused fields and persons in charge to fully support customers’ daily work, reflecting the high added value of security operation;

(4) Industry promotion. This stage is intended to continuously and deeply find needs of the administrative sections, reflect the function of auxiliary decision-making, and effectively guide users to create potential value. At the later stage of the work, we will focus on strengthening the ability to give overall solutions of safety accidents, building a database of security experts, providing internal security consulting and information security emergency response support for front-line operation support, and promoting continuous optimization of security operation.

Difficulties in development

According to the feedback of early research, at this stage, most administrative sections still have the expectation of “instant effect” on information security services. However, it is difficult to achieve this results in a short time on account of the multi-stage and multi-dimensional model construction described in the previous section are not easy to be founde At the same time, most of the security service providers are still at the initial stage in terms of the comprehensive capabilities of advanced security advisory service. They are not competent to provide customers with the expected service such as security early warning, bug repair, etc. In addition, the business model of safety operation belongs to labor-intensive industry, and the input-output of technical service also requires a more comprehensive choice and consideration of service providers.

Conclusion

At present, with a number of relevant laws and policies have been introduced and developing businesses emerge, information security industries are promoted in a good tendency. Many enterprises in the industry are also building their own business models around security services to put forward the transformation and innovation of service models. Technical support business proposed by the author in order to fully integrate business guarantee and talent output, benefit diversified customer groups, and finally establish a multi-dimensional security operation model integrating security protection, operation monitoring, response and disposal, and provide customized overall solutions to support the safe, stable and healthy development of information industry in the future construction.

Reference

[1] Michael Pang. Cybersecurity Law: Multiple level Protection Scheme

[2] Harry Katzan . Cybersecurity Service Model

[3] Huawei Technologies Co., Ltd .Huawei’s Position Paper on Cyber Security

[4]Yamin Wang .Suggestions on Implementation of Railway Information Security Classification Protection

[5] Yukai Wang. The development of network security and informatization has entered a new historical stage