Universe Scientific Publishing

Cyber Security Service Mode Innovation: Comprehensive Operation & Support

Qiyao Tang, Jie Xu

Nari information & communication technology Co.,Ltd. Nanjing 210000, China.

Abstract: With the rapid development of information technology, traditional nation state is faced with challenges from various aspects. However, the state can still lead the internet information security and create a variety of Internet security governance forms based on accepting the uncertainty of Internet security. Countries should focus on the impact of specific information technologies in specific areas and government agencies at specific points in time. This article talks about the cyber security protection and it is mainly focused on implementation schedule of cyber protection and experience exchange during this activity. Also it introduces current support service

Keywords: Security Operations Center; Penetration Test; Hidden Dangers Troubleshooting; Safety Services; Total-Process Safety

Introduction

Protecting the network action is a drill of cyber security attack and defense. It is aimed to discover, expose and solve security problems. This action is a real combat attack and defence activity at the nationwide. It can test the cyber security protection level and emergency handling capacity of China's major enterprises,institutions and the ministries.

According to the experience of cyber security protection over the years, the whole process of network protection has been divided into four stages from the point of time dimension: the first is the preparation stage, the second is the drilling stage, the third the combat stage; and the fourth replay stage. The focuses in each stage are different. Each stage usually carries out specific protection work according to deal with different problems.

1. Experience exchanging

There are several aspects in key work examination. The first is to check border security. The engineers should verify the security equipment configuration. Each security manufacturer shall check the firewall and the isolation devices (checking whether there is a bypass), the strategies of horizontal and vertical firewall . All the operations should follow the principle of risk minimization. Also, vertical encryption device policy should be followed. Access strategy must be specific, and visits between companies of prefecture level city are not allowed. Web firewall should be deployed at the horizontal boundary . In addition, the business relationship in rach safety zone should be clear. It is recommended to disconnect directly if there is no necessary business connection between systems. During the offensive and defensive period, dial-up access and wireless signal connection between provincial companies and prefectural companies should be blocked. Environmental protection data need to be examined by higher department. If the dispatching data network is not deployed, the network will be directly disconnected.

The next is architecture security. Engineers should check secure partitioning of application functions. Whether the security zone of each application in the network topology is reasonable and whether safety protection equipment is deployed in different safety zones are both vital to secure partition. Also remote operation and maintenance should run well and illegal communication with outside is banned. Remote operation and maintenance devices needed to be deployed in the production control area. External extension of service network boundary and its corresponding security management are also needed to be examined. If the network extension is not prohibited, effective security measures must to taken for this network extension. The security configuration of dispatching data network equipment should be checked carefully. The security configuration

of dispatching data network equipment are needed to meet the requirement, which means turning off or limiting network services, avoiding the use of default routes, turning off the OSPF routing function at the network boundary, adopting the network management protocol of security to enhance SNMPv2 and above, setting the trusted network address range, recording device logs, setting high-strength passwords, turning on the access control list, closing idle network ports, etc.

Comprehensive management security is also very vital for devices and network.First engineers should check the construction of management system related to cyber security of electric supervisory system. Whether there is a safety protection scheme for the electric supervisory system and whether there is a safety management system for systems, equipment and personnel and revising it regularly should be ensured. Then, they should check the cyber security risk control in each stage of system infrastructure, operation, operation and maintenance. For example, whether the management system of system infrastructure, operation, operation and maintenance includes relevant requirements for cyber security protection and whether there are risk prevention and control measures related to cyber security.cyber security emergency management system, emergency plan and emergency drill are also very important.cyber security emergency management system and emergency plan are needed to be checked if are made. Emergency drills are recommended to be carried out regularly.

Operators should also check the security management system for the access of external computers and mobile media. These contain whether special debugging equipment and media are equipped, such as special USB flash disk and special debugging notebook, whether the USB ports of security zone and servers are closed and whether the external equipment access management is implemented according to the system. In addition the safety management and protection measures of on-site operation and maintenance personnel and manufacturer's technical support personnel cannot be ignored. For example whether the management system for external operation and maintenance personnel is established and whether the confidentiality agreement is signed and whether there are security control measures such as external personnel login, operation approval and authorization are still advised to be examined. Audit logs of system operation and maintenance are saved in the system and they are vital for the cyber security. The last part is to check the application of cyber security management platform and cyber security supervisory device. cyber security supervisory device needed to be deployed and connected to the cyber security management platform. The monitoring objects (servers, workstations, network equipment, security equipment, etc.) with access conditions are connected to the cyber security supervisory device.

2. Existing support services and program plans

On the basis that the original security consulting services only include consulting services, it is proposed to fully intergrade the security operation and evaluation business, security supervisory platform business, credible product deployment business into a brand-new one. This new business has customized model which can severe for regulatory agencies at all levels. Finally, the establishment of a multi-dimensional safety operation mode, which integrates safety protection, operation supervisory and emergency response, is realized.

2.1 On-Site Service

Each department arrange 1-2 professionals to stay for a long time. These experts work independently and carry out work regularly every week. They Use a variety of technology to scan and test network vulnerabilities every day. They can also cooperate to complete the normalized safety supervision. In addition, they collect statistics and analyze the results of routine safety work every week, and then report to the supervision management department.Sorting out normal safety work records, rectification notices and other documents, and cooperating with the issuance of rectification notices are also daily work.

Maintainers on site cooperate to carry out daily security supervision, including real-time supervisory of sensitive information, malicious website, virus protection, illegal outreach, new access advanced security events, configuration vulnerability and other security events, so as to fully form a linkage mechanism. For the identified information security risks or vulnerabilities, experts assist in the analysis and disposal of various security events and carry out technical support for rectification of known problems and verify the rectification.they also provide professional technical support in the internal inspection of information security by means of special internal security inspection, annual security inspection and surprise

inspection of subordinate units: assist in sorting out information assets and risks, troubleshooting prominent problems and weak links, fill in relevant record forms, and prepare information security inspection analysis report and security suggestions according to the inspection arrangement. Developers participate in the preparation and submission of the company's self inspection report and reporting materials, cooperate with the elimination of information security hidden dangers on the problems found in the inspection, take effective measures to prevent information security risks and effectively improve the level of information security.

2.2 Safety training

According to the needs of customers, provide professional training such as web security, cryptography and CTF through on-site training, video lectures and remote network training operators participate in and cooperate with the company's professional operation and maintenance personnel in organizing competitions and evaluation and then set up a safety training platform to conduct regular online examinations for employees.The professional attack, defense and penetration team regularly organizes the red team to carry out attack and defense drills, and assists in the release, repair and patching of the company's vulnerabilities.The company hold interpretation of cyber security policies and norms, exchange of cutting-edge technologies, publicity and education on security and confidentiality of all staff, and publicize and implement the security awareness and confidentiality awareness of the management.

Our team developed CTF (capture the flag) platform, combined with vulnerability shooting range demonstration and real topic training, and through on-site training, video lectures, remote network training and other methods.also they set up an independent information security awareness training lecture for enterprise management, professional operation and maintenance layer and all employees.With customized training materials, they organize technical exchanges and collaborative operations between departments at all levels of the company, domestic authoritative testing institutions, well-known universities, well-known training institutions and front-line cyber security manufacturers.This can improve frontier technology.

2.3 Attack and defense technology

A number of team members have long been selected in the cyber security penetration team of national (sub) electric supervisory system, and have rich penetration attack and defense talent reserve and knowledge reserve.As a national (sub) penetration team, it normally carries out deep-seated vulnerability mining, cyber security incident technical investigation, major activity guarantee, cyber security attack and defense drill, etc. for the electric supervisory system.The penetration testing team has many years of experience in security testing, and has a large number of self-developed and open source security tools, which combines security methods and security theory, automated tools and manual penetration.Compared with the traditional tool scanning penetration test, it focuses more on the safety problem identification of logical types and the safety problem detection of types requiring manual assistance, which can raise the overall safety level to a new level.

The members of the red team have achieved good ranking in the major CTF attack and defense competitions.

Conclusion

This article introduces the what’s cyber security protection and its meaning to national cyber security. It divide this action into four parts and give detailed introduction to each stage, especially preparation stage. This article summarizes previous experience and underlines what should check during overall examination period. With the development of cyber security and classified security protection 2.0, cyber security engineers participate in this tasks actively. The paper talks about how its safety consulting services change to meet the requirement of cyber security.

References

[1] Leszczyna, Rafal. (2018). A Review of Standards with Cybersecurity Requirements for Smart Grid. Computers & Security. 77.

[2] Song ZW, Liu ZH. (2019). Abnormal detection method of industrial control system based on behavior model. Comput. Secur. 84, C (Jul 2019), 166–178.
[3] Myers D, Suriadi S, Radke K & Foo E (2018) Anomaly detection for industrial control systems using process mining. Computers and Security, 78, pp. 103-125.
[4] Mousavian S, Erol-Kantarci M, Wu L and Ortmeyer T, "A Risk-Based Optimization Model for Electric Vehicle Infrastructure Response to Cyber Attacks," in IEEE Transactions on Smart Grid, vol. 9, no. 6, pp. 6160-6169, Nov. 2018.
[5] Soltan S, Mittal P and Poor HV, "Bayesian Regression for Robust Power Grid State Estimation Following a Cyber-Physical Attack," 2018 IEEE Power & Energy Society General Meeting (PESGM), 2018, pp. 1-5.
[6] Dai Q, Shi L and Ni Y, "Risk Assessment for Cyber Attacks in Feeder Automation System," 2018 IEEE Power & Energy Society General Meeting (PESGM), 2018, pp. 1-5.