Frontiers in Computing and Intelligent Systems
ISSN: 2832-6024 | Vol. 8, No. 1, 2024

Application Analysis of Security Situational Awareness System in Qinghai Provincial Meteorological Network

Yanping Chang [1], Qibin Li [2], Jianan Zhang[1]

[1] Qinghai Provincial Meteorological Information Center, Xining, Qinghai, China
[2] Qinghai Provincial Atmospheric Exploration Technology Assurance Center, Xining, Qinghai, China

Abstract: As the public's demand for the accuracy of meteorological services is increasing, the scale of meteorological network in Qinghai Province is expanding, the depth of the network level is extending, the topology is becoming more and more complex, and the security problems are becoming more and more prominent. Traditional security protection measures are unable to detect the problems in Qinghai Province meteorological network as a whole. Network Security Situational Awareness is an effective means to guarantee the security of meteorological network at the present stage by collecting comprehensive and macro security elements in the network environment and carrying out big data analysis and processing to have a macro and comprehensive judgment of the security situation of the network and to predict the security trend of the network system. This paper mainly focuses on the network security situational awareness system used in Qinghai meteorological network and gives a brief introduction to the deployment of the situational awareness platform and a brief overview of the supporting applications.

Keywords: Security Situational Awareness System; Meteorological Network; Qinghai Province.

1. Introduction

In the age of informationization, network technology has been integrated into all aspects of social life in an all-round way, and the various security threats that abound on the network have also penetrated into all aspects of society, and the importance and status of network security are constantly rising. The term network security situational awareness system [1] is a computer science and technology term published by the National Scientific and Technological Nomenclature Validation Committee in 2018, and the current academic definition of network security situational awareness system [1] is that a network security situational awareness system is a collection of multiple information systems such as antivirus software, firewalls, security auditing systems, firewalls, and other information systems and, based on all of the information collected, it can make an assessment of the current network situation A comprehensive system that evaluates the current network situation based on all the collected information as well as predicts the future trends.

Qinghai Meteorological Network[2] uses a network security situational awareness system designed on the basis of the overall architecture of big data, which is capable of supporting automatic parsing and filtering of the logs of common devices from most domestic and foreign vendors, as well as risk prediction and real-time alarms for the logs of security devices. The data accessed by the system includes network logs, security logs, terminal logs and threat logs. The system is pre-set with more than 400 association rules, covering four types of data sources: network probes, Windows, Linux, and firewalls. Based on this, the system will also output more targeted special security analysis content based on the alarms, events and logs of various third-party security devices.

In recent years, Qinghai meteorological informationization has been developing rapidly, and most of the business systems as well as platforms have been highly clustered and automated, the meteorological disaster prevention and mitigation capability has been greatly improved, and the monitoring and forecasting and early warning capability has been constantly improved, and along with the improvement of the business capability, the network security protection capability of the meteorological information of Qinghai is also constantly being improved. With the high-speed development of the information age, the types of network threats and attack means are also constantly updated, the network security situational awareness system can analyze the network threats and give the corresponding preventive measures, which can effectively improve the dynamic protection capability of Qinghai meteorological information system, which is of profound practical significance for further improving the meteorological business capability.

2. Current Situation of Meteorological Network Security in Qinghai Province

Qinghai provincial Meteorological Wide Area Network (QMWAN) is responsible for the normal operation of meteorological services[2] in Qinghai Province and data sharing among various departments and units. By 2022, more than 5 units have reached data sharing and exchange agreements with Qinghai meteorological information centre, and the demand for meteorological data from various departments, such as water conservancy, army, fire-fighting, etc., is getting higher and higher, so it is undoubtedly very important to ensure the normal operation of Qinghai Meteorological Network.

The structure of Qinghai meteorological network can be described as “wide, deep and aggregated”. Among them, wide for Qinghai meteorological network involves many cities, counties and business nodes, and the network area is not unified in terms of equipment usage and target tasks. Deep for Qinghai meteorological network structure is presented as a tree-like deep network structure, from a macro point of view can be divided into provinces, cities, states and counties 3 layers, and 3 layers of network structure are involved in internal and external network traffic management, border

defense. Poly for Qinghai meteorological network is mainly used to high-performance routers for each other as a backup of the core structure, this structure through the provinces, cities, states and counties in the depth of the 3-layer network, from provincial level to small county level are the core structure.

Qinghai meteorological network structure presents the following network security problems:

Internet boundary defense and control is mainly through technical means to avoid the intranet business systems or personal terminals receive abnormal traffic from the Internet or the threat of attackers, do a good job of Internet boundary defense and control can effectively improve the security level of Qinghai network protection.

Horizontal prevention and control of the intranet refers to the traffic generated by users who may access each other without passing through the core router of the provincial bureau. In reality, when users in cities, states and counties access their own web pages and servers, if the user terminal is attacked by Internet attackers and implanted with Trojan horses, the Trojan horse of this terminal may be directly attacked through the nodes of the cities, states and counties in the meteorological wide area network of the provincial bureau, which will lay hidden dangers for the safety of the whole Qinghai meteorological network.

Meteorological data is one of the national basic data published by the state, and part of the data is confidential, so a large part of the purpose of safeguarding meteorological network is to safeguard the security of meteorological data, safeguard meteorological data in order to lay a solid security foundation for meteorological business, and to make meteorological data better for the public to provide services. At present, the meteorological network in Qinghai Province has a huge amount of data and a single way of data protection, with low invasion defense capability.

The characteristics of Qinghai meteorological network of “wide, deep and aggregation” make the security events of Qinghai meteorological network unable to be discovered in time and centrally managed. Therefore, if the problems can be discovered in time, dealt with, solved and left behind the process of dealing with the problems, then firstly, the threat of network security events to meteorological operation will be greatly reduced, and secondly, the threat of facing the same problems can be eliminated. Secondly, when facing the same problem again, the threat of the same network security event can be eliminated.

3. Network Security Operation and Maintenance based on Security Situational Awareness System

Network security situational awareness system, mainly through the linkage of various security devices, collect traffic information logs, real-time analysis and judgment of threats and security events in the network, timely issuance of policies, through the linkage response to quickly dispose of security events, to ensure network security, and the formation of related logs and reports for operation and maintenance personnel to backtrack or carry out statistical work.

The system provides a variety of data interfaces, not only to support the real-time traffic data analysis of the mirror to the interface, but also to support the equipment to provide offline data files, for the secondary collection of file characteristics. The system supports the collection of a variety of threat detection receipts, including malicious file detection, intelligence detection, intrusion detection, etc., and can generate logs after detecting the relevant threats, real-time generation of alarms, to facilitate the disposal of operation and maintenance personnel and the later retrospective query.

The security perception system[5] used by Qinghai meteorological network mainly deploys network traffic probes by hanging next to the core router, and uploads the traffic of the intranet and Internet outlets to the situational awareness system for analysis through mirror copying, so as to obtain the network security threat status of the intranet and the Internet.

The main function of vulnerability scanning is to analyze and scan the system vulnerabilities of individual terminals or servers; asset management is a device for archiving and managing all assets in the network through asset probes and individual reports; traffic sensor is a traffic probe that mainly copies the destination traffic and uploads it to the NGSOC system together with the logs for corresponding analysis; terminal management is the Tianjing system for the individual terminals of Qinghai Meteorological Administration, which mainly analyzes the whole network and the Internet security threats. The terminal management is the Tianqing system used for personal terminals of Qinghai Meteorology, which is mainly for intensive security management of personal terminals in the whole network; firewall refers to the intelligent firewall deployed at the Internet exit, which is mainly for access control, policy control, and management of ports, services, and protocols for Internet traffic; behavior management system analyzes the mirrored traffic packets to derive the network behaviors of the user terminals or servers, and retains logs; and the gate is an internal and external network data exchange system. The network gate is a data exchange system for internal and external networks.

Devices in Qinghai Meteorological Intranet, no matter servers or personal terminals, no matter computing resources or storage resources, as long as interactive traffic is generated in the meteorological intranet, the process will be monitored by security devices throughout.

According to the problems raised by Qinghai Meteorological Network Security Prevention and Control Difficulties, they can be well solved through the Network Security Situational Awareness System.

Internet border prevention and control as well as intranet horizontal prevention and control difficulties can be combined with the system deployment mode, through the side-mounted traffic probe, so that the intranet Internet traffic mirroring replication to the system for real-time analysis, through the system's rich feature library for comparison, and timely discovery of intranet Internet in the presence of security threats.

Difficulties in data security prevention and control. This issue is also the core issue of meteorological network security, the current Qinghai meteorological network security equipment linkage structure, personal terminal leakage of data behavior will be monitored by the terminal management module, the server and the virtual machine data leakage through the firewall as well as behavioral management module for control, both play an effective role in preventing data leakage from the root cause of the incident.

Response and processing speed difficulties. Network Security Situational Awareness System was initially constructed to solve the problem of untimely response and resolution speed, as can be seen from the linkage structure of

the system, the situational awareness system[4] integrates a series of security equipment functions, and unified planning and management of these functions, the platform for the response speed of network security events compared to the manual query to complete the qualitative enhancement of the artificial search for network security problems may take days Or even more than ten days to query a small problem from the huge scale of data logs, on the contrary, the situational awareness system can identify network security threats in seconds or even milliseconds and behavioral network security logs and threat logs, the processing will be recorded in the logs, to facilitate the management and operation of the operation and maintenance personnel.

4. Conclusion

After the deployment of the situational awareness system, the network security defense level of Qinghai Meteorological Administration has been greatly improved, from the previous passive defense to the active reinforcement and active testing defense, the means of resisting network threats have become more intelligent and diversified, and the response speed and processing speed for network security threats have been greatly improved. Combined with the processing efficiency of real network security incident processing and the previous comparison, the network security incident processing efficiency has been improved exponentially, and the degree of impact of network threats on Qinghai meteorological business has been greatly reduced. Therefore, the deployment and application of situational awareness system is very necessary and effective for Qinghai meteorological network security.

With the advancement of the pace of development of national information technology, the public for the ecological environment and the quality of meteorological forecasting and prediction requirements continue to improve, for a variety of refined service data is also more and more huge, the situation of network security is becoming increasingly serious, the security of meteorological data depends on network security, only the improvement of meteorological network security protection, meteorological data can be safe and secure. The network security situational awareness system used in meteorological system basically solves the security needs of meteorological network from the macro aspect, but in the process of using the system, the system can not monitor the internal process of the business system, and there is the situation of accidentally killing the system process, in view of the phenomenon, I think that the application and deployment of meteorological network security situational awareness system should fully consider the needs of meteorological business in the future, and be able to according to the characteristics of the meteorological business In view of this phenomenon, I think that the application and deployment of meteorological network security situational awareness system should take full account of meteorological business requirements in the future, and be able to manage or monitor the system business and key processes according to the punctuality and completeness of meteorological business.

References

[1] Ou Zhanxiang, Deng Luhua, Chen Jinyuan. Analysis of network security situational awareness and prevention technology [J]. Journal of Xiangnan College,2023,44(05):27-31.

[2] Chen Shu, Meng Jin, Feng Yong, et al. Application of situational awareness technology in provincial meteorological network security protection [J]. Information Technology and Informatization,2020(10):127-129.

[3] Wang Shuai. Technical analysis of Network security situational awareness platform under the background of big Data [J]. Software, 2019,44(04):172-174.

[4] MI Qi. Architecture Design of Network Security Situational awareness Platform [J]. Ordnance Industry Automation, 2021, 40 (01):17-21.

[5] Shao Jiayong, Li Li. Research on Network security situation awareness Platform architecture based on Big Data [J]. Information and Computer (Theoretical Edition), 2019,32(24): 179-181. (in Chinese)