Research and Application of Security Situation Awareness Platform for Large Enterprises

Zhanyu Wang^(✉)

China Mobile Tietong Co. Ltd., Room 1105, Jinze Building, No. 2, Guangningbo Street,
Xicheng District, Beijing 100033, China
wangzhanyu@cmitt.chinamobile.com

Abstract. This paper analyzes the international and domestic security situation and major security threats, including those faced by large enterprises. In order to improve the security management level of large enterprises, the construction of safety management system which takes the safety situation awareness platform as the command core is puts forward. The technical framework, evolution route, main functions, core technologies and three-stage models of detection, perception and prediction, closed-loop rectification, and threat information sharing are discussed. At the same time, the author analyzes the organization mechanism, the research and development guarantee, the sustainable application, the introduction of ecology and so on, and puts forward the solution.

Keywords: Security · Situational awareness · Detection · Prediction · Sharing

1 Introduction

Under the impetus of the fourth industrial revolution, informatization and intellectualization are becoming the core driving force for large enterprises to continuously improve their informatization level and efficiency. It is becoming common that who master information will win the competition. Network security and informatization complement each other; Network security and informatization are two wings of one body and two wheels of one drive. Without network security, there will be no national security, and without informatization, there will be no modernization. The overall development of informatization and information security is indispensable. As the lifeline of national security and national economy, large enterprises have invested a lot of money, manpower and material resources in security, and generally built their own information network, system and information security equipment. However, there are still problems in information security, such as fragmentation, information island and poor perception, It is difficult to deal with complex security problems with one or several security technologies alone. The focus of network security personnel has developed from solving single security problem to studying the security state and its changing trend of the whole network. Building a complete security situation awareness platform is the core of the unified smart security command system of large enterprises. It will lead the overall situation, quickly and quantitatively perceive enterprise security and various threats, and greatly improve the response and disposal level.

2 General Status and Problems of Information Security in Large Enterprises

2.1 General Situation of Information Security in Large Enterprises

With the development and popularization of information technology, most large enterprises are gradually applying the latest information technology to better promote the improvement of work efficiency, making the development of enterprises in line with the development characteristics of the times. At present, China's large enterprises have basically completed the information construction, which is reflected in the corresponding information technology at all stages of the daily operation of enterprises, such as personnel management system, industrial control system, computer room construction, network construction and enterprise portal, involving all aspects of enterprise development. At the same time, large enterprises have added security construction investment for information construction, and issued corresponding management system for the security of technology application.

Different enterprises have different aims of information security protection. The technical system of information security management center needs to contain a variety of elements to play the corresponding role of information protection, including host, terminal, network, information system, technology application and data. The corresponding security products of each link are different. The information security technology architecture can be summarized into seven subsystems: host security, terminal security, application security, 4A security, information system security, data security and network security. The information management security of the whole enterprise can be guaranteed with the joint assistance of multiple subsystems.

In practice, most large enterprises use following equipments to build information security protection system: 4A, VPN, firewall, WAF, IPS/IDS, EDR, sandbox, honeypot, asset management system, anti-virus software, leak scanning system, etc., forming four basic conditions of secure communication network, regional boundary, management center and computing environment, providing enterprises with terminal access, interface security guarantee, application access and management, system security interconnection, safe operation guarantee Safety management ability.

2.2 Analysis of Information Security Situation of Large Enterprises

According to the analysis of China's Internet security situation by the national Internet Emergency Response Center and the statistics of the national information security vulnerability sharing platform, threats and risks such as denial of service attacks, high-risk vulnerabilities, phishing emails, personal information and important data leakage are still prominent in the first half of 2019–2020, and the risks remain high [1, 2].

The key infrastructure of large enterprise has become the key target of network attacks, and the network security risks such as vulnerability attacks and blackmail software are becoming more and more serious. The government, education, medical care, telecommunications, scientific research institutions and other important industries have become the hardest hit areas of network attacks.

From 2019 to the first half of 2020, the risk of personal information leakage continues to increase. In addition to the Internet industry, hotels and other service industries and industrial enterprises have become major risk areas of personal information leakage, and data security is facing serious challenges [1, 2].

Although the network security protection ability of large enterprises has been improved, there is still a certain gap between the security technology innovation and the international advanced level. In particular, with the wide application of emerging technologies such as artificial intelligence and blockchain, new types of network crimes are also escalating. In the face of the increasingly severe situation of attack and defense, the network security protection concept, ideas and technology implementation path of large enterprises need to be integrated and innovated.

For enterprises, the challenges of information security are mainly reflected in the following four aspects:

Decentralized security management; too many network devices; isolated information. The security incidents are analyzed and handled by different departments independently, which is impossible to analyze the security incidents end-to-end and make corresponding decisions.

Internal leakage: driven by interests, internal employees can easily disclose confidential information to competitors. Leakage means such as terminal copy, printing, e-mail delivery, etc.

Internal and external malicious attacks: the enterprise network is becoming more and more complex, and the enterprise terminal, network, server and so on have become the targets of internal and external attacks.

Vires abuse. Operation and maintenance personnel or business management personnel can easily use it system, ultra vires (fake, unauthorized access) access to enterprise confidential information.

2.3 Analysis of Information Security Problems in Large Enterprises

Among many information security problems that need to be solved, the most important one is the intelligent interconnection of various security devices. On the whole, all kinds of security equipment and capabilities are still in the state of decentralized construction and decentralized operation. There is a lack of interconnection between systems. Logs and other data are separated from each other and are actually “isolated islands” of data. It has some effect on the static and low-intensity information security attacks in the past, but it is not enough for the new situation attacks such as APT.

In addition, the sharing of security information with the outside of the enterprise is also an important factor affecting the ability of security protection, mainly because the security threat intelligence, virus database, rule base and other information of authoritative institutions and manufacturers can not enter the enterprise and play a role in a short time.

The lack of deep data correlation and analysis leads to the lack of means for high-level information security events and threats such as persistent and advanced network attacks and leaks. It emphasizes the single, flat and passive security protection, lacks the organic integration of personnel, process and means, and has three-dimensional, multi-dimensional and active cyberspace confrontation thinking. It has no perception of the

attacker's "when to come, when to go, what to do, what to take, why to do and how to do" in the whole process.

The means of operation are out of date. Security protection relies heavily on 4A and the traditional equipments. Enterprise relies on the deployment of firewall, intrusion detection system, vulnerability scanner, and then combines with 4A system for asset management, authentication and access control. The construction of security means is mainly piled up and isolated, and the security system is lack of systematization and coordination, so it is difficult to form an effective response to network threats.

All of these need to build a security situation awareness platform as soon as possible, effectively connect various security devices, and eliminate data islands.

3 Status and Role of Security Situation Awareness Platform

3.1 Relationship Between Security Situation Awareness Platform and Security Management System

The concept of situation awareness (SA) was put forward by Endsley in 1988. SA is the acquisition and understanding of environmental factors in a certain time and space, and the short-term prediction of the future (Fig. 1).

Fig. 1. Three level progressive model of situation awareness.

Security situation awareness is to use all kinds of data from the network and terminals, use the advanced big data architecture, through artificial intelligence algorithm, take the analysis of personnel and terminal behavior as the main line, detect and find the security incidents that threaten the enterprise, and provide a complete evidence chain of traceability and forensics, so as to comprehensively guarantee the enterprise information security.

Security situation awareness platform is a comprehensive solution platform for unified management of network information security situation awareness, security monitoring, notification and early warning, threat intelligence, tracing, traffic detection and emergency response. Through the orderly operation of the platform, enterprises can comprehensively grasp the key information infrastructure, important portal websites, information system network security situation, the dark network traffic within the jurisdiction, trace the source of IP, and carry out early warning, emergency disposal and comprehensive network security management. Network security situation awareness is a means of quantitative analysis of network security and a fine measurement of network security.

Security situation awareness platform, security management platform, security communication network and security equipment together constitute the enterprise security management system, which acts on the enterprise information system and information network, realizes the control command and data interaction, completes the operation of monitoring, warning, testing, configuration and switching, and realizes the corresponding disposal of security threats, security incidents and security. With the security situation awareness platform, it will provide accurate control instructions for the security management platform to achieve effective control. Security situation awareness platform becomes the core of enterprise security management system (Fig. 2).

Fig. 2. Schematic diagram of enterprise security architecture.

3.2 Main Functions of Security Situation Awareness Platform

Comprehensive collection of detailed data based on logs, traffic, etc., to build a basic security information base;

The whole enterprise shares the threat intelligence of social organizations and provides the enterprise security threat intelligence for social organizations;

Basic awareness of external and internal threats to achieve rapid security incident analysis, monitoring and situational awareness;

Comprehensive management and control of exposed assets, dynamic management and control of cyberspace to achieve spatial mapping;

Build enterprise wide intrusion analysis and monitoring capabilities with intrusion monitoring, website attack, self owned app protection and other functions;

Build the ability to analyze and monitor intranet intrusion, such as preventing penetration from all directions, password cracking, illegal information access and unauthorized access;

Provide the whole network linkage interface for emergency disposal to realize the whole process of rapid disposal; Establish a unified network security situation awareness platform and enterprise wide integrated command and dispatch system;

Build the ability of abnormal event traceability based on log and traffic data;

Connect and share with the relevant monitoring and sensing system of the superior unit; Support the security operation and simulation operation for different scenarios such as daily threat, major guarantee and emergency disposal.

Expand the scope of threat monitoring, detect, prevent or limit the network attacks from inside or outside at the key network nodes; And take technical measures to analyze, record information, optimize the ability of technical means, optimize the emergency response mechanism, and improve the monitoring, early warning and disposal level of the whole enterprise.

4 Technology Implementation Scheme and Evolution Route of Security Situation Awareness Platform

4.1 Platform Structure

It is mainly through extracting the network security situation analysis index system, establishing the network security situation analysis and prediction system based on complex network behavior model and simulation, and then obtaining quantitative or qualitative network security situation assessment results, and forecasting the evolution of network security situation in the future by analyzing and modeling the historical situation. In order to make reasonable adjustment and upgrading of the security elements, security equipment and information system in the network by the network security management personnel, and to cope with the changes of the network security situation. The network security situation awareness platform mainly includes six levels, namely data acquisition layer, preprocessing layer, label and storage layer, modeling and analysis prediction layer, visual display layer, application command layer, and two basic levels, knowledge base and rule base. The technical structure is shown in Fig. 3.

Data Acquisition Layer. Data acquisition is connected to different equipment, systems and products through various communication means, and the security data of a wide range and deep level is collected, and the protocol conversion and processing of heterogeneous data are collected, and the data base of enterprise network security situation awareness platform is constructed. The platform has many probe acquisition methods, such as active detection, log collection and flow analysis, to obtain real-time security data. The data collected from the daily management of the equal protection data, threat intelligence data and the third-party standard interface constitute the total data on the data acquisition level. The acquisition system must identify many device protocols such as syslog, SNMP, NetFlow, EDR, VSS, and analyze the protocol in depth, support data collection of various

Fig. 3. Security situational awareness platform architecture.

information including terminal behavior, threat alarm data, log data, and support output to the flat platform in a variety of standard formats.

Pretreatment Layer. The data collected in various formats are pre processed in a standardized and unified way, and abnormal data and duplicate data are eliminated to improve the data quality and improve the efficiency, quality and accuracy of data analysis.

Tagging and Storage Layer. Classify and analyze data, label data according to rule base and knowledge base. Data storage and index can realize data aggregation, storage and index function of detection data, monitoring data and knowledge base resources, and provide open interface for data acquisition at data modeling layer.

Modeling and Analysis and Prediction Layer. The preprocessing data is associated with knowledge base and rule base, and relevant security information data is extracted for modeling. Combined with machine learning and deep learning algorithm, it analyzes the identification information, asset information, attack event, attack trace information, attack path information and attack source header information, and displays threat situation and data association mining.

According to the historical and current status information, the analysis model is established in line with the network and business scenarios, and the situation prediction is carried out based on the combination of network threat and asset situation.

Visual Presentation Layer. The paper presents the quantitative status and prediction results of network situation through data visualization. With the help of powerful processing ability, logical thinking and judgment ability in graphics and images, the paper realizes the artificial global visualization analysis and drilling analysis of enterprise security situation, threat situation, attack source, attack event and asset security status, as well as qualitative judgment and prediction.

Application and Command Layer. The comprehensive analysis of the detection, perception and prediction results of safety events is completed, and the solution is proposed, which is divided into control tasks and control instructions. It is sent to the security management platform through the interface to interact and command the closed-loop rectification process.

Perceptual Knowledge Base. According to the needs of the security management in the industry and the enterprise, we should establish a set of knowledge slices which are structured, easy to operate and easy to use, and are organized to store, organize, manage and use in the system. It includes the theoretical knowledge, fact data, detection, perception, prediction and other verified knowledge related to the field, heuristic knowledge obtained by expert experience, etc. It is helpful to share and exchange knowledge by accelerating the flow of knowledge and information.

Perceptual Rule Base. The rules of detection, perception, prediction and visualization involved in the sensing system are managed by rule base as database management. When business requirements change, it is no longer necessary for programmers to modify individual code, but to manage them in the rule base. It is provided to each system and technical use as the basis of rules.

4.2 Main Capabilities of Network Security Situation Awareness Technology

Threat Intelligence Disposal and Sharing. Collect and dispose threat information data from various sources, and transform the format internally and transfer all to the knowledge base and rule base; the core system of driving detection, perception and prediction dynamically adjusts the processing logic and makes closed-loop correction. To the outside world, the threat information sharing based on internal success cases is provided to external organizations. Threat information includes: IP asset portrait, domain name portrait, lost host data, regional security report, illegal organization and activity threat information.

Network Intrusion Detection. The platform analyzes the intrusion detection of the collected data and gives timely alarm. The intrusion response evaluates the security situation of the system according to the system attack alarm and abnormal alarm perceived by real-time intrusion detection, and makes and implements the optimal security strategy in time to alleviate the impact of intrusion attack. Intrusion response includes two parts: security policy decision and policy execution.

The Analysis of Safety Events and Situation Evaluation. According to the degree of harm and the ability of regional security protection, the paper uses decision tree, Bayesian network and other technologies to analyze the security events comprehensively. Neural network and fuzzy reasoning are introduced into situation assessment. The knowledge base and rule base of network security attributes are used to comprehensively evaluate the status and development trend of security events, and reasonable judgment, decision-making suggestions and protective preparation measures are put forward. Including perception of rigid creeping network, vulnerability situation, etc.

Network Security Situation Forecast. The platform uses the current and historical detailed and massive collection data, knowledge base and rule base to learn and analyze the big data in depth. It finds the rules of hacker invasion. According to the intrusion behavior, the platform predicts the intrusion behavior, the purpose of hacker invasion and the equipment that may be threatened in the future, and takes effective targeted measures to prevent it.

Invasion Tracing. The platform uses the intrusion trace data, the collection data, the knowledge base and the rule base, combined with threat information, to quantitatively and trace the security events, determine the intrusion entrance, path, scope, measures, etc., recover the intrusion process, propose targeted rectification measures and modify the knowledge base, rule base and perception and prediction system.

Disposal and Closed Loop Correction. The platform issues control orders to the safety management platform based on the results of detection, perception and prediction. The safety management platform issues manual and automatic work orders to safety organizations and safety equipment for security defense disposal; The platform conducts closed-loop evaluation based on the completed status of work order and collected data, and the closed-loop correction detection, perception, prediction knowledge base and rule base are closed-loop.

Core Analysis Model of Situation Awareness. Network security situation awareness includes three elements: perception, understanding and prediction. The following four models are mainly used in the analysis process:

Endsley model, which senses the information of the state, attribute and dynamic of the important components in the network environment, and the continuous updating, prediction and evolution process of the integration and sorting of the elements.

OODA model refers to observation, Orient, decision and act, which is a concept in the field of information warfare. OODA is a process of continuously gathering information, assessing decisions and taking action.

The JDL model is to analyze the data and information from different data sources, to identify the target, to estimate the identity, to evaluate the situation and to evaluate the threat. The accuracy of the evaluation is improved by refining the evaluation results.

RPD model (Recognition primed decision) defines situation perception into two stages: perception and evaluation. Perception compares the existing situation with the past to select the past situation with high similarity. Evaluation is the process of analyzing the past to speculate the current situation evolution.

4.3 Platform Evolution Route

Based on the Specific Organization, Complete the Internal Situation Awareness Infrastructure. It includes: data and alarm collection, threat intelligence platform, event analysis platform, internal disposal management platform, and visualization application to present and assist these work. In this way, a complete security operation can be supported within an enterprise. The required security analysts can be obtained by purchasing external services, or they can be trained by themselves.

Establish Vertical Support System and Intelligence Data Sharing System. It includes vertical malicious code analysis center, enhanced event analysis center, intelligence sharing mechanism and vertical Threat Intelligence Center. Malicious code analysis and major event analysis need high-level security analysts to participate in order to achieve the effect. The intelligence sharing mechanism ensures the synchronization of information and social organizations, and enables key intelligence to be used more quickly and effectively in enterprises. Security analyst resources are mainly self-cultivation.

Building Integrated Automatic Defense Capability. With the enhancement of the vertical support system and the overall intelligence analysis ability, when encountering key events, we can carry out integrated protection, more quickly and efficiently suppress attacks, and strive for time to clear attacks. At the same time, security analyst resources have formed a scale and can be provided for external use.

5 Problems Needing Attention

After the completion of the security situation awareness platform, we must strengthen the continuous use and continuous optimization, and pay attention to solve the following problems:

5.1 Organization Mechanism Guarantee, Forming a Virtuous Circle

We should establish a special safety management team to manage in parallel with the information management team, improve the three synchronous principles of synchronous planning, synchronous construction and synchronous operation of the information system and safety system, and realize a good and benign mechanism that can be managed and used well.

Strengthen the training of internal high-level security analyst resources to form a strong personnel base.

5.2 Devops Guarantee

Around the situation awareness platform, the core engine of security management, a technical team integrating development, maintenance and technical support is established to control the R & D quality and agile iteration ability of security business.

5.3 Institutional Constraints to Reduce Employee Risk

Hierarchical protection of business security. We will improve and formulate the business security classification protection system and work standards, and strengthen the business security evaluation management mechanism and technical level.

5.4 Persevere and Introduce Ecology (Good Partner)

Business security process embedding. Realize the whole life-cycle embedding and centralized continuous management of enterprise key business security management and control; Introduce professional consulting agencies and professional security service providers as partners, establish a sound enterprise security situation awareness system, take me as the main, share partner experience, and improve together.

6 Conclusion

Through the construction and deployment of security situation awareness platform, large enterprises will intelligently connect the existing security equipment, form the ability of defense in advance, active management, three-dimensional protection and efficient response, quickly and comprehensively sense the security threats faced by enterprises, comprehensively improve the level of enterprise information security governance, and eliminate all kinds of hidden dangers in the bud. Through long-term operation, the security situation awareness platform has accumulated experience and data, which will continuously improve the comprehensiveness, accuracy, timeliness and judgment of perception, and provide a strong information security guarantee for the development of enterprise informatization and more efficient investment in the tide of digital economy. It will also bring information security revenue for enterprises through data sharing and ecological co construction!

References

1. China Internet Network Security Monitoring Data Analysis Report for 2019. National Computer Network Emergency Response Technical Coordination Center, Beijing (2020)
2. China Internet Network Security Monitoring Data Analysis Report for first half of 2020. National Computer Network Emergency Response Technical Coordination Center, Beijing (2020)

Open Access This chapter is licensed under the terms of the Creative Commons Attribution 4.0 International License (<http://creativecommons.org/licenses/by/4.0/>), which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license and indicate if changes were made.

The images or other third party material in this chapter are included in the chapter's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the chapter's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.