Universe Scientific Publishing

ORIGINAL ARTICLE

Research on Network Security Situational Awareness Technology under Data Fusion

Yuanting Lu

Guizhou Business School, Guiyang 550000, Guizhou, China.

Abstract: While the popularization and application of the Internet brings convenience to people's lives, it also triggers a series of network security issues. However, traditional network security methods can no longer meet the requirements of network security, and network security situational awareness technology integrates security elements from all levels, can fully grasp the network security status as a whole, and give warnings to network security trends to improve the network safety technology level.

Keywords: Data Fusion; Network Security; Perception Technology

Network security situation awareness technology is mainly used in large-scale network environments to collect and process various network data to monitor the network, and provide users with network security situation through the acquired network security history records. In the context of data fusion, the application of network security situational awareness technology has a very important role and value.

1. Problems in the network security protection system

Modern technology is developing very fast, and network technology is constantly being updated and developed to meet the diverse needs of users. However, network security has always been a problem that must be focused on and solved. Although many network security protection technologies are now perfect, they are still subject to various attacks during the specific operation process, which exposes system vulnerabilities. For the previous security protection system, the system is usually based on self-checking, data prevention and control models, etc. Although this type of protection system is widely used, from a technical perspective, there is no protection system on the market. Can guarantee absolute safety. In addition, the security protection systems on the market often counterattack passively, only when they are attacked will they counterattack. And in the process of updating the protection system, it is still passive defense, which provides opportunities for criminals. On the whole, for the traditional security protection system, the information transmission is not timely, and when the independent module is running, the associated module fails to react in the first time, which makes the defense system imperfect. At the same time, the core of the system operation is usually the computer system data center, and its protection function has certain limitations, because in the system, it is unable to perceive the security problems faced in the network environment. In addition, the data information structure has not realized intelligence, and only relies on the set path to operate, which is in a passive protection situation. And the matching degree of data information is not high. When the network system is under attack, traceability analysis can not be implemented, only protection can be carried out, which increases the probability of system vulnerabilities.

2. Analysis of cyber security situational awareness technology under data fusion

doi:10.18686/ahe.v5i8.3895

In the context of data fusion, network situation awareness can accurately interpret various aspects of equipment operating status, network behavior, and simplify processing of various security data information to efficiently identify various network security risks and make security protection more effective. Targeted, scientific, reduce security risks, and create a secure network environment for the majority of users.

2.1 Risk assessment techniques

In the network system, the ways of information dissemination are diversified. The risk assessment technology is mainly given to various transmission nodes to monitor the information structure, such as domain names, etc., combined with the multiple systems in the database, to carry out some hidden problems. Dig deep and analyze the transmission of abnormal data information to achieve the effect of multi-level detection. When detecting dangerous information, it is usually necessary to make a more accurate analysis based on the expected operating conditions of the data, and to integrate multiple technologies such as sequence combination and data linkage, and then to track and monitor the problems that occur. The internal data model is used to record all the intrusion paths with hidden security risk information, evaluate the model, and transmit it to the system processing center. This link is the whole process detection. After the evaluation instruction is completed, the attack behavior that has occurred can be monitored, and the module function can be used to upload to the security situational awareness system to accurately analyze the linkage impact of abnormal data and restore the code intrusion path. At the same time, it can also be based on the virus. The original path was run and the specific location of the attack was analyzed. This technology can achieve the effect of data traceability and provide accurate information and data for the decision-making of relevant technical personnel.

2.2 Heterogeneous fusion technology

When network information data is transmitted, the number of logs, etc., are mainly provided through one or several application systems. Based on the original differences of the system, the various behavioral parameters generated by it will inevitably be different. When the log data is combined, due to the original lack of corresponding benchmark processing parameters, an accurate result cannot be obtained through integrated interpretation. From the perspective of situational awareness technology, it is not only limited to a single network operating system, but after disrupting the existing log data pattern, various parameter information and characteristics are re-set. When the data information is re-formed into a whole, the detection technology will detect the data information as a whole. This form can comprehensively improve the detection efficiency of data information, accurately check each byte and chain block, and ensure the quality and efficiency of detection. In the specific application of this heterogeneous fusion technology, it no longer restricts the single information generated by the log, but integrates the information and data that appear during the operation of the computer system, performs vertical fusion processing on the data, and transmits it. Give the database and store it in a separate unit. Because the data information is recombined after being scrambled, the basis of the information format formed after the reorganization is the same. In the specific detection, it is necessary to deeply explore the value contained in the information through information expansion and correlation, and then implement the integration of network architecture.

2.3 Visualization technology

In fact, visualization technology refers to the visualization function of the data information model, which relies on the data information operation mode to build a three-dimensional framework, so that relevant technical personnel can make a more comprehensive interpretation of the data model. From a technical perspective, visualization is a progressive mode of data, which can be divided into the following stages: The first stage is data conversion. This stage is mainly to detect and process data information, and then display the data information in the form of a table. When data is remapped, the real-time characteristics of the system can be used to realize the data mapping within a short time delay range, and then the data information can be stored in a system preset manner. The second stage is the image mapping stage. This stage is mainly to make measurements on the data tables that have been generated, set system parameters, map the information data in the tables, and use the structure and attributes as the information building platform to complete the conversion of the data tables. The third stage is the conversion of views. In the specific conversion, based on the space coordinates, a certain item of data is determined first, and then the image model is constructed through the image mapping information. At this time, the system will automatically adjust the location of the information, etc., under the control of various parameters , To achieve view conversion.

2.4 Decision-making technology

Decision-making technology is the key technology to be realized by the situational awareness system. It drives the dynamic operating mode of the security system. If there is a security risk in a certain detection link, the system will automatically store and integrate the information facing security issues in an independent spatial structure. Get up, and then make a comprehensive judgment on various internal security information attributes. This process can be referred to as an integrated application mode, which is to analyze the safety problems or the path of the information through the integration and analysis of various information, and locate the dangerous information under the effect of internal control and

self-inspection. Based on the nature of the emergence of network security issues, it is not only through information retrieval and processing, but also through the integration of various linkage behaviors of information. Through the construction of a comprehensive evaluation system, the essential behavior of security issues can be predicted to obtain a more accurate result. The application of decision-making technology often takes the motivation of cyber attacks as the main body, such as the method and purpose of the attack, and then regards the object as the criterion of security information. The object contains network elements, etc., which can build a complete security protection under multi-line control system.

3. Conclusion

In summary, network security is related to the people's property safety, and it is also a key issue that needs to be resolved to promote the healthy development of society. The application of network security situational awareness technology effectively makes up for the shortcomings of traditional security protection systems. It can use data invasion characteristics to realize reverse tracking and automatically attack viruses, which can greatly improve the effectiveness of network security protection.

References

1. Dai X, Zhang S. Research on data fusion technology in big data network security situation awareness. China Information Technology 2020; (04): 81-82.
2. Su X, Xu K. Overview of the application of data fusion algorithms in network security situational awareness. Journal of Hebei Academy of Sciences 2020; 37(02): 37-44.
3. Zhu Y, Yang Y, Li S, et al. Research on network security situation awareness platform for big data environment. Network Security Technology and Application 2018; (11): 52-54.
4. Li J, et al. Research on network security situation awareness models and methods for heterogeneous data sources. Harbin Engineering University 2017.
5. Gong M, Liang J, Yao Y. Research on security situation awareness technology of radio and television networks. Xinhua News Agency Chongqing Branch, Chongqing Daily News Group, Chongqing Radio and Television Group (Headquarters), China Federation of Journalists. China News Technicians Association 2017 Academic Annual Conference Proceedings (Excellent Papers). Xinhua News Agency Chongqing Branch, Chongqing Daily News Group, Chongqing Broadcasting and Television Group (Headquarters), China News Technicians United Meeting: China Federation of Journalists 2017; 7.