International Journal of Enhanced Research in Management & Computer Applications
ISSN: 2319-7471, Vol. 8 Issue 8, August-2019, Impact Factor: 3.578

A Study on "Key Technology of Network Security Situation Awareness of Private Cloud in Enterprises"

P. Ravindra[1], S. Vasu[2], P. L. Ramesh[3]

[1,2,3]K. B. N. College (Autonomous), Vijayawada-520001, Andhra Pradesh, India

ABSTRACT

With the prevalence of private cloud, how to safeguard the private cloud network security has turned into the focal point of an ever increasing number of endeavors. The venture data security framework requirements to incorporate the data security development into the foundation development. Endeavor private cloud network security circumstance is, what is going on administration designing issues, and any private cloud weaknesses might prompt loss of motion of the whole organization. This paper takes the essential organization security circumstance, enormous information security, private cloud network security circumstance as the passage point, examines the important assessment lists, and lays out the assessment framework model and other key advancements, explains on the private cloud network security circumstance in undertakings.

Key Words: Data, Private Cloud; Network Security Situation Awareness; Big Data, Security

INTRODUCTION

With the rapid development of Internet plus, the attacks of hacker are increasing, the security of the large infrastructure enterprise system and communication system is also facing more risks. The most important form is network virus. Hackers can steal information, which can result the paralysis of enterprise internet.

However, defense can not completely protect the data of enterprises, the most effective defense method is warning, the security research of the enterprise network situation is an important issue at the moment. Enterprise network security situation research is based on the security status of enterprise information, and combined with the historical security events of the enterprise [1]. It can prediction the period security state information of the enterprise, and grasp the real security situation of enterprise information.

The Internet Network Security

Network security situation is a macro response to network operation, which reflects the past and current situation of the network, and predicts the possible network state in the next stage [2]. It mainly collects data through network monitoring equipment, network physical equipment and other network equipment, through the data processing, numerical, icon and other ways to respond the actual operation of the network.

Network Security Situational Awareness

Network security situation is a comprehensive research topic. It mainly contains three levels. First, deal with the massive network data, display network security situation with graphics. Secondly, the data are quantitative analysis, the characteristics are abstracted, and the history and current situation of network security are evaluated. Finally, the internal relationship between the collected data and the historical network security events is analyzed, the possibility network security problems in the future are predicted and prevention and response strategies are formulated [3].

THE KEY TECHNOLOGY OF NETWORK SECURITY SITUATIONAL AWARENESS

One of the key technologies of network security situation is the data fusion technology, a unified of different security equipment are collected and transformed into a standard data format which monitors the security log or warning information. As the history of security incidents are analysis, the prediction of network situation are accurate.

After the fusion of network security data, we need to calculate the massive data through a specific mathematical formula, that is, through a specific mathematical formula, a range is obtained, which reflects a value of network security state in a certain period. There are four main calculation methods: analytic hierarchy process (AHP), fuzzy analytic hierarchy process (FAHP), Delphi method and comprehensive analysis method [4].

The Network security situational awareness is based on scientific, the historical security events and network security status are compared and analyzed,and the network security status in the future is predicted and predicted. The kinds of prediction for network security situation are three: qualitative prediction method, time series analysis method and causality prediction method. Combined the current network equipment security status data, the network security threats and hidden dangers in the future period are predicted by the scientific theory and reasonable method.

THE NETWORK SECURITY SITUATION OF PRIVATE CLOUD

With the rapid development of Internet plus, data is the core competitiveness of enterprises. Data have many kinds such as customer information, financial information and other information. At public cloud, the core data of the enterprise is generally stored in the public network storage which provided by the service provider [5]. The data which stored in the network are more and moreopenness and convenience, at the same times more and more no privacy and insecurity. During the enterprise data is transmitted and stored, it is stolen easily. It is particularly concerned about that how toencrypt core data. In order to better protect these data, more and more enterprises have established private cloud. But there are many insecure factors in private cloud networks: data communications insecurity, intentional attack servers, frequent sending of service requests in the short term, which may affect the reliability of private cloud.

Moreover if the private cloud was damage, it will have a fatal impact on the whole enterprise.

The Security of Virtual Cloud Data

With the development of new network technology, the innovation is occurring in the field of cloud computing and big data. In the era of big data, network security can be enhanced from many aspects, such as physical security, host security, information content security, information transmission security, etc...In big data era, it is a huge challenge that how to analyze massive data, prevent the invasion and attack of hackers, improve network security countermeasures by taking more active and effective network security.

In the era of big data, it is a service that how to store and operate the data. The spread of the network viruses is double, the scope is wide. Anti-virus technology is the key technology of big data security. In private cloud big data, the technology of anti-virus are mainly two types: static and dynamic [6]. The static antivirus technology mainly monitors the network equipment through the monitoring equipment, and analyzes the security status of thenetwork according to the state of the equipment. Dynamic anti-virus technology can protect the bottomsystem resources of the private cloud, which can ensure its integrity.

The Key Technologies of Private Cloud Network Security

In the transport layer and storage area, in order to ensure the security of private cloud, the enterprise will develop a series of network security technology. In the transport layer, the transmitted data is encrypted. The transmissible important data areencrypted by technologies; the receivers decrypt the cipher text. After transfer the data security, it is important that how to store these data safely. The security of data storage mainly includes the boundary protection of network data, the mutual isolation of data, the disaster recovery of data, etc... In addition, private cloud can also protect data access through a series of access authentication, including single sign on authentication, collaborative authentication, and resource authentication and so on.

In private cloud data boundaries, a series of targeted protection is needed. The intelligent firewall technology is the most universal. Different from the traditional firewall technology, intelligent firewall technology is a new firewall technology. It uses fuzzy retrieval database, through artificial intelligence technology to dynamically identify the data. Intelligent firewall technology can prevent hackers from scanning network data, which can maintain the information security of the private cloud. There are three defense modes of intelligent firewall: intrusion prevention, cheat prevention and anti scanning.

THE KEY TECHNOLOGY OF NETWORK SECURITY SITUATION IN PRIVATE CLOUD

Private cloud network security can be divided into five levels: device security layer, network security layer, system security layer, application security layer and data security layer. By decomposing the threat of each layer and adopting appropriate security measures, the security goal can be achieved: confidentiality, integrity, availability, controllability and non repudiation.

Network Security Situational Awareness of Private Cloud in the Era of Big Data

Private cloud big data has the followingcharacteristics: Volume (high capacity): the size and amount of data determines the size of the data value and potential information; Variety (type): data types; Velocity (speed): get the data very quickly; Variability: prevent treatment and effectively manage the process of data authenticity; Veracity: data reliability; Complexity: a large amount of data, multiple sources, multiple channels caused by the consumption of complexity of data; Value: rational use of big data reasonable analysis, create high value at low cost.

Analysis of large data private cloud platform network security situation, a variety of network security equipment and network monitoring equipment dataneed to be collected [7]. Vast amounts of data will be presented in various ways such as monitoring methods and security reporting mechanisms, which draw graphics and other reports. Private cloud data have many characteristics: massive log information, redundant information. But error information cannotbe used as a direct source of situation awareness; it must carry out on-line analytical processing and data fusion.

In big data era, it can collect various types of data formats, including log network equipment, security equipment, log, the information stored in private cloud that operated in service system. So we can have more sources of network security situation awareness than ever. Another feature of big data is the rapid processing of massive data. People can deeply analyze the parameters of network traffic and network data [8]. Computational resources need to meet the needs of high intelligence model algorithms. In big data era, there are four main aspects of network security: First, knowledge base can be established by studyingnetwork attack cases, including principle, characteristics, environment, the most common equipment and methods; Second, environment vulnerability knowledge base can be established by analyzing the loopholes of private cloud architecture system vulnerabilities and storage devices; third, environment threat knowledge base can be established by analyzing the architecture topology and equipment of private cloud; Finally, by analyzing and comparing the three kinds of knowledge base horizontally, people can confirm the effectiveness of security incidents[9]. Through analyzing the historical security events, the network attacks that affect the current network will be combed. Ultimately generate security situation assessment elements of private cloud, including the security threats, the vulnerability, the running health status, etc...

The Assessment Index of Network Security Situational Awareness on Private Cloud

To evaluate the security situation of private cloud,we should make a comprehensive study from five aspects, including physical security, host security, network security, data security and content security. The study can reflect the security of the storage disk, the security of the information system, the security of the information itself, the security of the data transmission and the security of the information utilization of private cloud. Among them, the most effective indicator of network security situation is network security index. The network security situation can measure by the network security index. It consists of a three-dimensional network index (Run_{net}, Vul_{net}, $Threat_{net}$).

The Security Situation Warning of Private Cloud Network

At present, the highest level of security defense system is network security situation. In order to analyze the uncertain information in the network for a long time, the advanced analysis technology will be used in the private cloud; the scientific rule will be provided in the network security situation.

In order to build a perfect network security situation forecast trend map, and improve the availability of security situation prediction, it is necessary to establish a long-term monitoring mechanism. With the rapid development of the network, the network security environment is becoming more and more complex, the attack intensity is becoming stronger and stronger, and the threat is also increasing. Nowadays, the threat of Internet is dynamic. In order to provide security policyfor users, correct decision should be made, and dynamic prediction measures should be adopted [10].

The core issue of network security situation warning ishow to predict the network security situation. In the private cloud structure, the network security situation assessment is usually carried out on the storage server side by the fat server - thin client mode.The scanning and evaluation work cannot be completed rapidly when the target scope is large, so the original B/S mode is improved to three layer mode, and deal with the work in intermediate layer which should be done by the server. The intermediate layer can coordinate the resource balance of the whole system and improvethe speed of server disk scan evaluation. The architecture of the network security situation assessment system of private cloud three layers B/S mode as shown in the following Figure. The evaluation system consists of three parts: cloud data center, middleware (Web server andsystem client) and thin client. The working principle isthat the server of cloud data center defines the scanning parameter file, and the thin client accesses it through Web. The scanning server submits and summarizes the scanned parameter files. Thevulnerability information report is sent to the analysis server, which obtain the network security situation assessment.

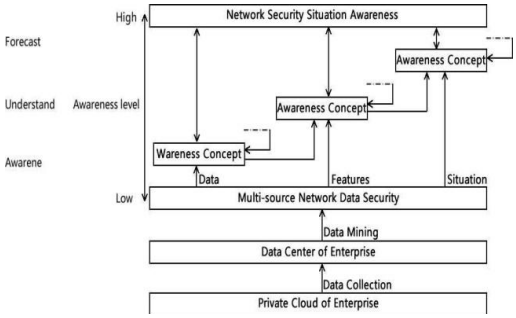

Figure 1 Architecture Graph of Network Security Situation

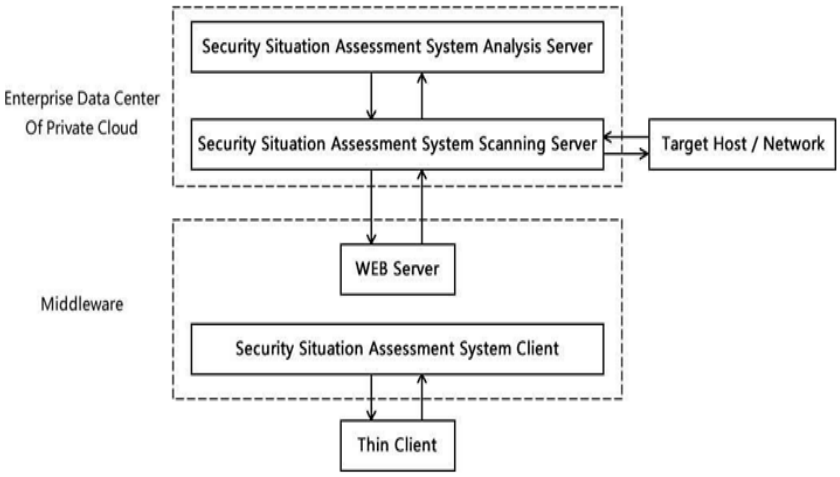

Figure 2 Network Security Situation Assessment Architecture Diagram of Private Cloud Three Layers B/S Mode

CONCLUSION

In the future, based on artificial intelligence and powerful data analysis ability, people can anticipate the danger ahead, kill the cradle really, and greatly enhance the ability of network security defense. With the rapid development of the Internet, the core competitiveness of enterprise data, such as customer information, financial information, and so on, is maintained in the form of information data. Many enterprises have built their own private clouds to ensure the safe storage and use of massive data. In the future, more consideration will be given to the use of artificial intelligence to solve the security problem of enterprise private cloud. It is not overlaying the security equipment simply. The construction of information security system and information security management system also complement each other.

In other words, the core of enterprise information security is the security management strategy which implemented perfectly and strictly. Only the network security has improved, the enterprise can speed up the pace of information construction; people can enjoy the convenience and ease of the network safely; the society can be more rapid and healthy development.

REFERENCES

[1]. Celenk M., Conley T., Willis J., Et Al. Predictive Network Anomaly Detection And Visualization [J]. Ieee Transactions On Information Forensics & Security, 2010, 5(2) :288-299.
[2]. Fireeye. Cybersecurity's Maginot Line: A Real-World Assessment Of The Defense-In-Depth Model [R]. Fireeye,2015.
[3]. Lai J. B., Wang H. Q., Zhu L. Study Of Network Security Situation Awareness Model Based On Simple Additive Weight And Grey Theory[C].//Proceedings Of The International Conference on Computational Intelligence and Security, Guangzhou, China: IEEE Computer Society,2006:1545~1548.
[4]. Lai Y. P., Hsia P. L. Using the vulnerability information of computer systems to improve the network security. Computer Communications.2007, 30(9) :2032-2047
[5]. Sun F. X. Artificial immune danger theory based model for network security evaluation. Journal of Networks.2011, 6(2)
[6]. :255-262.
[7]. Wei Y., Lian Y. F., Feng D. G..A Network Security Situational Awareness Model Based On Information Fusion [J]. Journal Of Computer Research And Development,2009,46(3) :353-362.
[8]. Zaharia M., Chowdhury M., Das T, Et Al. Fast And Interactive Analytics Over Hadoop Data With Spark [J]. Usenix, 2012,37 (4) : 45-51.
[9]. Zhao Y., Zhou F., Shi R.. Net secradar: A Real-Time Visualization System For Network Security: Vast 2012 Mini Challenge. Award: Honorable Mention For Interesting Use Of Radial Visualization Technique [C]// Vast. Proceedings Of The Visual Analytics Science And Technology (Vast), 2012 Ieee Conference On, October 14-19,2012,Seattle, Wa, Usa. New York: Ieee, 2012:281-282.
[10]. Zhang J. F. Research On Key Technologies Of Network Security Assessment [D]. Changsha: National University Of Defense Technology,2013:19-35.
[11]. Zhao L, Xue Z. Synthetic security assessment based on variable consistency dominance-based rough set approach´ High Technology Letters. 2010. 16(4):413-421.