Optimal Design of Data Center Network Security Architecture

*Shaoqing Wang

The University of Queensland, Queensland, Australia
*Email: 1280538273@qq.com

Abstract. In the context of the wide application of Internet, big data and cloud computing technologies, data center as a key infrastructure for information flow, its network security issues become increasingly prominent. This paper deeply analyzes the current situation of data center network security. At present, data centers are facing a variety of network security threats such as distributed denial of service attacks, virus trojans, phishing attacks, and the popularity of iot devices has also brought new attack entry points. There are many problems in the existing network security architecture, including incomplete security protection system, insufficient protection for emerging iot devices, difficult border protection against advanced persistent threat attacks, lax internal network control over employee device access, and defective data security protection. Security devices are improperly configured, such as over-reliance on a single device, improper parameter Settings, and delayed update and maintenance. Safety management is not in place, staff safety awareness is weak, authority management is not fine, the system is imperfect and ineffective implementation, and the emergency response lacks effective plans and drills. In response to these problems, an optimized design scheme is proposed, which follows the principles of integrity, layered protection, dynamic adaptation and compliance, divides network security levels, reasonably allocates security equipment, and implements security management strategies to improve data center network security protection capabilities, ensure data security, and promote the healthy development of information technology.

Keywords: Data center; Network security; Architecture optimization; design

1 INTRODUCTION

In today's era of rapid digital development, advanced technologies such as the Internet, big data, and cloud computing have spread rapidly and penetrated into every corner of society like thriving vines, greatly changing people's way of life and production. As a key support in this digital process, the data center is like a busy information hub, carrying massive data storage, processing and transmission tasks. It is the core of business operations and the data basis for many business decisions. It is also an important node of social information circulation and plays an important role in economic development and social stability. However, cyberattack methods are a constant undercurrent, in-

A. Bhunia et al. (eds.), *Proceedings of the 2024 2nd International Conference on Finance, Trade and Business Management (FTBM 2024)*, Advances in Economics, Business and Management Research 304,
https://doi.org/10.2991/978-94-6463-546-1_43

creasingly new and more sophisticated. Malicious attackers use various vulnerabilities of the system, protocol defects and configuration errors, etc., to launch a round of fierce attacks on the data center. These attacks may not only lead to the theft of critical data and service destruction of enterprises, but also may cause serious impacts on national security and social stability through the key node of the data center. In view of this, scientific and reasonable optimization design of data center network security architecture and strengthening its security protection capability have become the key issues to be solved in front of us. This paper will deeply analyze the status quo and existing problems of data center network security, carefully build a set of feasible optimization design scheme, hoping to provide a strong reference for the construction of China's data center network security, help the steady development of information technology, and protect the security of data center this information treasure house.

2 DATA CENTER NETWORK SECURITY STATUS ANALYSIS

2.1 Network Security Threats

In today's information age, data centers, as the core of information processing and storage, are facing a variety of network security threats[1]. Cyber attackers use a variety of means, such as system vulnerabilities, protocol flaws, and configuration errors, to launch attacks on data centers in an attempt to steal data, disrupt services, or extort ransom. Common cybersecurity threats include, but are not limited to, distributed denial-of-service attacks (DDoS), which flood a target server with massive amounts of spam traffic, leaving legitimate users unable to access the service[2]. Viruses, trojans and phishing attacks are also on the rise, penetrating systems to steal sensitive information or cause damage by masquerading as legitimate software or emails and inducing users to download or click on them. Hackers use social engineering to trick insiders into giving away access, further increasing the risk of data breaches. At the same time, with the popularity of iot devices, attacks against these devices are also increasing, and they can become an entry point for attacks on data centers. In addition, vulnerabilities in system software and application software are constantly being revealed, which can be exploited by attackers to execute arbitrary code, take control of systems, or steal data. In the face of these threats, data center cybersecurity safeguards must be constantly updated and strengthened to protect critical information assets from being compromised[3].

2.2 Problems in the Existing Network Security Architecture

Imperfect Security Protection System. There are many imperfections in the current network security protection system. First, many organizations lack a comprehensive defense strategy in the face of increasingly sophisticated cyberattacks. For example, the security protection of emerging Internet of Things devices is often not paid enough attention, making these devices easy to become a breakthrough for attackers to invade

the network[4]. When it comes to border protection, traditional technologies such as firewalls may not be effective in identifying and blocking some advanced persistent threat (APT) attacks. At the same time, the internal network also has vulnerabilities. For example, the control over employee devices' access to the Intranet is not strict enough. Employees may access mobile devices with potential security risks at will, resulting in viruses and malicious software easily entering the Intranet. In addition, in terms of data security protection, the application of encryption technology may not be comprehensive, and the backup and recovery mechanism for important data is not perfect enough[5]. Once data is damaged or lost, it is difficult to recover quickly and effectively, which brings huge losses to enterprises and organizations.

The Security Device is Improperly Configured. Improper configuration of security devices seriously affects network security. On the one hand, some enterprises over-rely on a certain kind of security equipment. For example, only a large number of firewalls are deployed, while ignoring the synergy of devices such as intrusion detection systems (IDS) and intrusion prevention systems (IPS)[6]. As a result, some attacks that bypass the firewall by means of camouflage cannot be detected and prevented in time. On the other hand, the parameters of the security device may be set improperly. For example, access control lists (ACLs) are configured too loosely, allowing unauthorized access. In addition, security equipment is not updated and maintained in a timely manner, which makes it unable to cope with emerging security threats. Some old security devices may not be able to handle large-scale data traffic and complex attack modes due to performance limitations, and newly purchased security devices may not be able to give full play to their advantages due to improper configuration, causing a waste of resources and reducing the overall efficiency of network security protection.

Inadequate Security Management. Inadequate security management is an important problem facing network security. In terms of personnel management, the safety awareness of employees is generally weak and there is a lack of relevant safety training[7]. They may randomly click on unknown links and download files from unknown sources, which can lead to attacks on the network. The rights management of internal personnel is not fine enough, and some employees have excessive rights, which increases the risk of data leakage and malicious operation of the system. In terms of system management, the safety management system is not perfect, and the implementation is not enough[8]. For example, there is no strict password policy, employees set easy to guess passwords, or do not change passwords for a long time. The inspection system for network devices and systems is not perfect, and potential security risks cannot be discovered in time. Moreover, in terms of emergency response management, there is a lack of effective emergency plans and drills, and when network security incidents are encountered, they cannot be dealt with quickly and effectively, resulting in the expansion of the impact of the incident and serious consequences for enterprises and organizations.

3 DATA CENTER NETWORK SECURITY ARCHITECTURE OPTIMIZATION DESIGN

3.1 Design Principles

A data center is a complex system that includes many hardware devices, software applications, and network connections. The integrity principle requires us to view the data center as an organic whole ecosystem. From physical facilities such as servers and storage devices to software-level operating systems and applications, security requirements must be fully considered. You can't just focus on a single component or local security while ignoring the overall interconnectedness. For example, if a server has a security vulnerability, an attacker may use the vulnerability to further penetrate the entire data center network, affecting the normal operation of other devices and systems, and even threatening the stability of the entire data center[9]. Therefore, when designing the security architecture, it is necessary to start from the whole to ensure the security coordination among all parts.

Layered protection is like building a strong castle. Starting at the network border, this is the first line of defense against external attacks, similar to the walls of a castle. Deploy devices such as firewalls to prevent unauthorized external access. After entering the internal network, different subnets also need to have corresponding security measures, just as each area in the castle has different defense facilities. From the network layer to the system layer to the application layer, different security measures are adopted at different layers. For example, the network layer can ensure communication security through virtual private network (VPN), the system layer strengthens the security protection of the server operating system, such as timely patch updates, and the application layer performs vulnerability scanning and protection for various applications[10]. In this way, even if a certain layer is broken, the subsequent layers can still be blocked, greatly improving the overall security of the data center.

The network security environment is constantly changing, and new attack methods and security vulnerabilities continue to emerge. Security architectures must be dynamically adaptable, adapting and updating in a timely manner to meet new threats. This means regularly updating security policies to adapt to emerging attack patterns and vulnerabilities. At the same time, software versions should be updated in a timely manner, as new versions often fix known security vulnerabilities. For example, when a new form of malware emerges, the security architecture should be able to react quickly, adjust protection policies, and update relevant security software to ensure that the data center can defend against this new threat in a timely manner, rather than powerless in the face of new threats.

Data centers must be operated in strict compliance with relevant laws, regulations and industry standards. This is not only the basis for ensuring the lawful use and protection of data, but also the key to avoiding legal risks caused by illegal operations. For example, in terms of data storage and processing, it is necessary to comply with data protection regulations and properly protect sensitive data such as users' personal information. In terms of network security management, it is necessary to follow industry standards and ensure that network security measures are in line with norms. If the

relevant regulations and standards are violated, data centers can face serious consequences such as fines, reputational damage, and so on. At the same time, compliance also helps to improve the credibility of the data center, enhance user trust in the data center, and promote the sustainable development of the data center.

3.2 Optimize the Design Scheme

Network Security Hierarchy. As the basic security layer, the physical layer covers the physical environment security of the data center. The access control system is an important part of it, which strictly restricts the entry of unauthorized personnel and prevents malicious personnel from directly contacting the equipment. In addition, fire, waterproof, lightning and other facilities can effectively protect equipment from physical disasters. For example, if there is a fire, good fire prevention facilities can put out the fire in time or prevent the spread of the fire, and protect the equipment from being burned. At the same time, appropriate temperature and humidity control is also part of the physical layer security category to ensure that the equipment operates in a suitable environment and extends the life of the equipment.

Network layer security focuses on the security of network communication. The firewall plays a key role at this layer, blocking external malicious attacks and illegal intrusions by setting reasonable access control rules. For example, you can restrict network access based on information such as IP address, port number, and so on. VPN technology provides a secure communication channel for remote users or branches, encrypts data transmission, and prevents data from being stolen or tampered with in the network. At the same time, network traffic monitoring is also an important part of network layer security. By analyzing network traffic patterns, abnormal traffic can be detected in time, such as sudden emergence of a large number of unidentified packets, which may indicate potential network attacks, so that appropriate measures can be taken to prevent them.

Configuring Network Security Devices. In the data center, the reasonable configuration of network security equipment is the key to build a solid security defense line. First, the deployment of high-performance firewalls is indispensable. Strict access control policies must be configured on the firewall to accurately control the incoming and outgoing network traffic based on different network zones and service requirements. For example, you can set the core service area of the data center to allow access to only a specific IP address segment or a specific protocol to prevent unauthorized external access. At the same time, the intrusion detection system (IDS) and intrusion prevention system (IPS) should work with the firewall. IDS monitors abnormal traffic and behavior on the network in real time and issues alerts when suspicious attack patterns are found. The IPS goes a step further and automatically takes measures to block attacks when they are detected, preventing further attacks. For example, when detecting traffic anomalies similar to DDoS attacks, the IPS can quickly cut off related network connections to prevent the influx of attack traffic.

For internal networks, network access control devices should strictly control employee device access. Through device authentication and security check, devices accessing the Intranet meet security standards to prevent viruses and malicious software from entering the Intranet through employee devices. In terms of data storage, encrypted storage devices are used to encrypt and save important data. Even if the data storage device is stolen or accessed illegally, the true data content cannot be obtained without the correct decryption key. In addition, it is essential to establish a unified security management platform. The platform can integrate the information of various security devices to achieve centralized management and monitoring. For example, when the intrusion detection system finds an exception, the security management platform can quickly notify relevant personnel and coordinate other devices to implement joint defense, such as adjusting firewall policies and starting emergency response procedures. These security devices can be properly configured to form a cooperative and closely coordinated security protection system to effectively resist various network security threats and ensure the secure and stable operation of data centers.

Security Management Policy. Security management policy is an important guarantee for data center network security. In terms of personnel management, it is necessary to strengthen the safety training of employees and improve their safety awareness. Regularly organize security knowledge seminars and skills training to keep employees informed of the latest security threats and preventive measures. At the same time, a strict authority management system should be established to assign the minimum necessary authority according to the job responsibilities of employees to prevent the abuse of authority. In terms of system management, a sound security management system should be formulated, including equipment inspection system and password policy. Equipment inspection should be carried out regularly to discover and solve potential security risks in a timely manner. Password policies require employees to set complex and regularly changed passwords. In terms of emergency response, a detailed emergency plan should be formulated to clarify the responsibilities and response processes of various departments in the event of a security incident. And regular emergency drills to improve the ability to respond to security incidents. Through the comprehensive implementation of security management policies, the network security of data centers is ensured from many aspects such as personnel, system and emergency response.

4 CONCLUSION

This paper analyzes the various network security threats faced by data centers and the problems existing in the existing architecture, including the imperfect security protection system, unreasonable security equipment configuration, and inadequate security management. According to the principles of integrity, layered protection, dynamic adaptation and compliance, network security levels are divided, security equipment is reasonably configured, and security management strategies are implemented. Through these measures, the aim is to improve the security protection capability of data centers,

ensure data security, and reduce the occurrence of network security accidents. However, the network security situation is constantly changing, and it is necessary to continue to study and improve the security architecture in the future to adapt to new challenges, and promote the continuous improvement of data center network security construction and the healthy development of information technology.

REFERENCES

1. Yuning Jiang, Manfred A. Jeusfeld, Michael Mosaad, Nay Oo. Enterprise architecture modeling for cybersecurity analysis in critical infrastructures — A systematic literature review[J]. International Journal of Critical Infrastructure Protection, 2024, 46 100700-100700.
2. Ajay Kumar Vyas;Narendra Khatri;Sunil Kumar Jha. 6G Communication Network: Architecture, Security and Applications[M]. CRC Press: 2024-06-13.
3. Oleksandr Kuznetsov, Dmytro Zakharov, Emanuele Frontoni, Andrea Maranesi. AttackNet: Enhancing biometric security via tailored convolutional neural network architectures for liveness detection[J]. Computers & Security, 2024, 141 103828-.
4. Sedjelmaci Hichem, Kaaniche Nesrine, Tourki Kamel. Secure and Resilient 6 G RAN Networks: A Decentralized Approach with Zero Trust Architecture[J]. Journal of Network and Systems Management, 2024, 32 (2):
5. Terzi Sofia, Stamelos Ioannis. Architectural solutions for improving transparency, data quality, and security in eHealth systems by designing and adding blockchain modules, while maintaining interoperability: the eHDSI network case[J]. Health and Technology, 2024, 14 (3): 451-462.
6. Claudio Zanasi, Silvio Russo, Michele Colajanni. Flexible zero trust architecture for the cybersecurity of industrial IoT infrastructures[J]. Ad Hoc Networks, 2024, 156 103414-.
7. Madjid G Tehrani, Eldar Sultanow, William J Buchanan, Malik Amir, Anja Jeschke, Mahkame Houmani, Raymond Chow, Mouad Lemoudden. Stabilized quantum-enhanced SIEM architecture and speed-up through Hoeffding tree algorithms enable quantum cybersecurity analytics in botnet detection.[J]. Scientific reports, 2024, 14 (1): 1732-1732.
8. V Samuthira Pandi, Albert Anitha Juliette, Thapa K. Naresh Kumar, Krishnaprasanna R.. A novel enhanced security architecture for sixth generation (6G) cellular networks using authentication and acknowledgement (AA) approach[J]. Results in Engineering, 2024, 21 101669-.
9. Zhang Yin Sheng. Analysis of OSPU security effect and data assembly verification under semi-network OS architecture[J]. International Journal of Information Security, 2023, 22 (5): 1497-1509.
10. Michael Hart, Rushit Dave, Eric Richardson. Next-Generation Intrusion Detection and Prevention System Performance in Distributed Big Data Network Security Architectures[J]. International Journal of Advanced Computer Science and Applications (IJACSA), 2023, 14 (9):