The Security Design in Data Center Infrastructure Construction

Xiaoming Liu

National Computer Network Emergency Response Technical Team, Coordination Center of China, Beijing, China

liuxm@cert.org.cn

Abstract. Information Technology is becoming very important in modern society and more and more data centers have been built. The infrastructure security is an important part of Data Center security. Data center security is introduced as three aspects in this paper: operational security, network security, and supply security. Accidents in some data centers and statistics on network security risks in recent years are included. Countermeasures for network security risks in infrastructure are also given.

Keywords: security design, data center, infrastructure construction.

1 Introduction

1.1 The Important Role of the Data Center in Modern Society

With the rapid development of society in digitization and intelligence in the past few years, cloud computing, big models, and artificial intelligence are rapidly developing. The demand for Information Technology (IT) is constantly increasing for market and government agencies. More and more data centers have been built as the foundation of the digital economy and technological innovation. According to statistics from the China Academy of Information and Communications Technology, there are more than 6 million rack-mounted servers in China's data centers until 2022. The data flow value was recorded as $2.8 trillion in 2014 [1]. Data centers are the core infrastructure for E-business, social media, online education, and digital operations of government and enterprises, and have been an important component of modern society today [2]. The rapid growth of data volume has led to the large-scale construction of data centers. Risk-threatening data centers are classified into three groups: natural disasters, accidents, and man-made disasters [3]. There are also four metrics for power management: efficiency, stability, robustness, and adaptability [4]. Improving the power supply security of data centers has become an important issue in the current operational security of data centers.

L. Liu et al. (eds.), *Proceedings of the 3rd International Conference on Financial Innovation, FinTech and Information Technology (FFIT 2024)*, Advances in Computer Science Research 118,
https://doi.org/10.2991/978-94-6463-572-0_10

1.2 The Importance of Infrastructure Security of the Data Center

As the foundation for core data storage and processing, the physical form and scale of data centers are constantly changing in recent years. Data centers evolve from ordinary computer rooms to micro-module data centers, and then to liquid-cooled data centers [5]. The number of rack-mounted servers also increases from tens to thousands. Security and reliability are always the top requirements for data centers [6]. The data centers used by the government carry the national economy and people's livelihood, and are extremely important for national information security. Once the data center shuts down, it will cause huge losses, and even damage the government image and social security.

There are many studies about the information security of Data Centers [7-8], involving vulnerabilities evaluating operation and maintenance security, data encryption transmission, data sharing security, management system optimization, network security, disaster response, etc. However, there are also potential safety hazards in equipment such as power supply, refrigeration, and supervision system [9-11]. The power system is an important infrastructure for data centers, and its reliability and safety will directly affect the operation of data centers and the perception of owners. Therefore, it is not only necessary to consider information security at the software level but also to strengthen the security and reliability of the underlying energy infrastructure. Security design in data center infrastructure construction like this can ensure that the data center operates stably, securely, continuously, and efficiently.

2 Infrastructure Security framework of the Data Center

Infrastructure security is essential not only for the growth of the economies but also for achieving better productivity [12]. There is a strong positive correlation between infrastructure and quality of growth and development [13]. Based on years of experience in data center construction and operation, combined with considerations for information security and infrastructure security, the infrastructure security framework should mainly include three aspects: operational security [14], network security [15], and supply security, as shown in Figure 1. Operational security refers to the security of power supply and ancillary systems. Network security refers to the information security in the network environment. And supply security refers to the reliability, sustainability, and localization security of the supply chain.

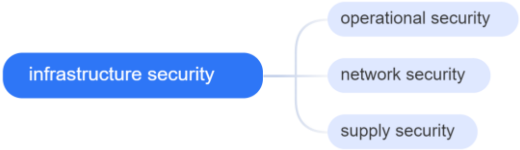

Fig. 1. Architecture of infrastructure security

An emergency response mechanism for network security incidents typically involves several key components and steps. These are designed to mitigate the impact of security breaches, minimize downtime, and restore systems to full functionality as quickly as possible. The following points outline a comprehensive emergency response mechanism, as shown in Figure 2:

1. Incident Identification: Continuously monitor network systems using automated tools and manual processes. Set up alarm systems to notify relevant teams immediately when anomalies are detected. Analyze system logs and security intelligence to identify and classify security events.
2. Emergency Response Plan: Establish a detailed emergency response plan that outlines procedures, roles, and responsibilities. Ensure all relevant stakeholders are familiar with the plan and their roles during an incident.
3. Response Team Activation: Once an incident is confirmed, activate the emergency response team consisting of security experts, system administrators, and network administrators. Coordinate efforts with other teams such as IT support, legal, and communications.
4. Threat Assessment: Collect detailed information about the incident, including affected systems, sources of the attack, and methods used. Preserve evidence for future investigation and legal action. Assess the severity of the threat and potential impact on the organization.
5. Containment, Eradication, and Recovery: Isolate infected systems to prevent further spread of the incident. Identify and remove the root cause of the incident, whether it be a malicious program, a vulnerable system component, or a misconfigured network device. Restore affected systems to a known good state, applying patches and updates if necessary.

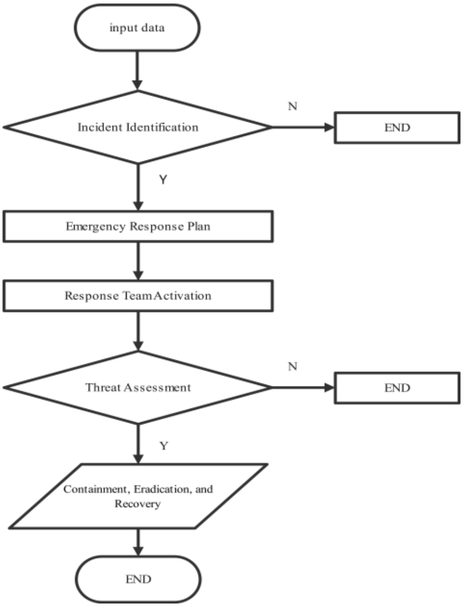

Fig. 2. Outline of an emergency response mechanism

2.1 Operational Security

Frequent accidents occur during the operation of data centers. These accidents include power failures, refrigeration failures, natural disasters, etc. The accidents result in serious consequences such as data loss, system interruption, and business interruption and have caused great losses to the users.

Data is one of the core assets of modern governments and enterprises, so frequent incidents will lead to data loss, data damage, and service disruption, and reduce production efficiency and operational capabilities as a result. This not only causes economic losses to governments and enterprises, but may also have a negative impact on their reputation and customer trust, or even lead to legal issues. Table 1 shows accidents in some data centers in recent years.

In order to reduce operational accidents and the impact of these accidents, a series of measures should be carried out

Table 1. Accidents in some data centers in recent years

Company	***Date***	***Reason***	***Consequences***
Telstra (UK)	2021(Q3)	UPS failure	The London hosting data center caught fire and rack-mounted servers shutdown.
Microsoft (USA)	2022 (Q2)	Power failure	Users can not login or access accounts for 12 hours.
Google (USA)	2022(Q3)	Power accidents	3 electricians were burned. Google Maps and Google Search cannot be used in more than 40 countries and regions. At least 1338 servers were affected.
Oracle (UK)	2022(Q3)	Refrigeration failure	A part of computing facilities shut down for protection. Customers are unable to access resources in time.
AWS (USA)	2022(Q3)	Power failure	The power failure lasted for 20 minutes. Services and applications failed in three hours.
SK (Korea)	2022(Q4)	Battery fire	Tens of millions users have been affected. Approximately 32000 servers have crashed
Alibaba (Hong Kong)	2022 (Q4)	Refrigeration failure	The computer room has been shut down for more than 10 hours. Customers like Monetary Authority of Macao are unable to use it.
Guangzhou Telecom	2023 (Q1)	Refrigeration failure	Tencent and VIPS's service stop for more than 3 hours.
Microsoft (Australia)	2023 (Q2)	Power failure of refrigeration	The power failure lasted for more than 24 hours and partial hardware was damaged.

To strengthen security management in different aspects, such as physical security, design security, and operation and maintenance security, as shown in Figure 3.

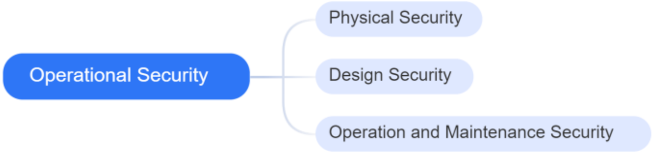

Fig. 3. Architecture of operational security

a) Physical Security: Physical security refers to protecting the physical environment of data centers. Site selection of data centers, access control system of personnel, equipment anti-theft, and physical protection of equipment are all part of physical security. Security and monitoring measures such as access control, video surveillance, smoke detectors, temperature sensors, humidity sensors, and fire-fighting equipment can all enhance physical security. Access control can restrict personnel from entering the data center, video surveillance can remotely monitor the condition of the data center, smoke detectors can detect fires in a timely manner, temperature and humidity control can ensure the normal operation of equipment, and fire-fighting equipment can prevent the spread of fires. Equipment failures are inevitable, but intelligent proactive warning can identify faults in advance, and redundant design in architecture can reduce the impact of faults, thereby ensuring operational safety [16].

b) Design Security: According to the importance of the data center, the power supply and cooling of the data center need to be designed with redundancies. Modular design architecture can achieve physical isolation and area division, thereby reducing the risk of single failure. Equipment failures are inevitable, but intelligent proactive warning can identify faults in advance and redundant design in architecture can reduce the impact of faults. These security considerations during the design process can improve operational safety.

c) Operation and Maintenance Security: Comprehensive operation and maintenance system should be established in terms of operation and maintenance security. Establishing and enforcing strict security policies and operating procedures, such as regular equipment maintenance and testing, regular emergency drills, security audits, and vulnerability scanning, can assist staff in ensuring the reliability of infrastructure operation, and promptly identifying and resolving potential safety hazards. Staff training should be enhanced to strengthen their safety awareness. At the same time, with the increase in device intelligence, the device has stronger monitoring ability and even has the ability to predict risks. Such device can detect and eliminate risks in advance.

2.2 Network Security

Network security refers to protecting the network of data centers, such as preventing hacker attacks and virus infections. The infrastructure system of data centers has entered the era of digitization and intelligence, but digitization and intelligence are double-edged swords. Along with the development of intelligence, there are also threats to network security. Network security involves all aspects of data centers. Not only networks and computers, but infrastructure devices are also connected to the network, and there are also network security risks, as shown in Figure 4. Attackers can install programs to view, modify, delete data, and create new accounts with full user privileges. Attackers can exploit security vulnerabilities in various devices of the data center to control and shut down power and cooling equipment. If the infrastructure and computers are on the same network, there is even a risk of critical user data being leaked through the infrastructure network. Table 2 shows statistics on network security risks in some infrastructure in recent years.

In order to prevent network attacks from damaging data center equipment, stealing information or deleting data, protective measures should be taken in some aspects as shown in Table 3.

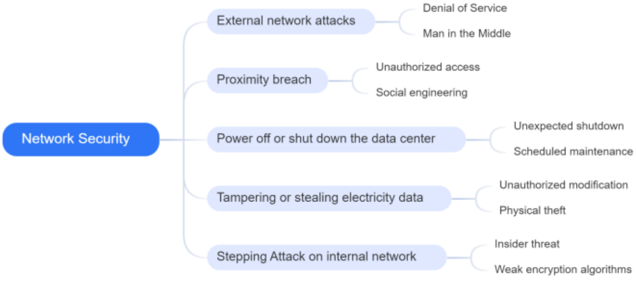

Fig. 4. Risks of network security

Table 2. Statistics on network security risks in some infrastructure in recent years

Event	*Date*	*Consequences*
Attackers use malicious emails to invade Ukrainian office computers. They attack Ukrainian power facilities repeatedly form these computers and shut down power supply equipment remotely.	2015&2016 (Q4)	Widespread and prolonged power outages.
China discovered 19 high-risk vulnerabilities in Treck TCP/IP Stack, involving various infrastructure devices.	2020 (Q2)	State-owned Assets Supervision and Administration Commission of the State Council ask major enterprises to conduct comprehensive safety inspections.
China's monitoring department found three high-risk vulnerabilities in the uninterruptible power supply (UPS) equipment from the American Power Conversion Corporation (APC).	2022(Q1)	Attackers can exploit this vulnerability to remotely take over UPS devices, carry out attacks and bring about damage to the device.

The data centers' equipment should use localized produced operating systems. Network security and privacy protection should be considered during production. For example, using bidirectional certificate authentication, using secondary challenge identity authentication, restricting remote high-risk interfaces, using security function libraries to prevent command injection, and using intrusion detection based on situational awareness.

Table 3. The main network security risks in infrastructure and countermeasures

	Main risk	*Details*	*Countermeasures*
1	External network attacks	Implement network attacks on network management, UPS, air conditioning, and other devices through external networks by violent cracking, DDoS attacks, vulnerability exploitation, etc.	Least port Least privilege Security deployment and reinforcement (software authentication and permission isolation) Challenge authentication Intrusion detection Integrity verification Componentized/service-oriented Minimize the system
2	Proximity breach	Malicious operations, such as control and parameter modification, are carried out through the device web and LUI.	Least port Least privilege Security log Access authentication High-risk operation white list control Security configuration check
3	Power off or shut down the data center	Intrusion management system and shut down equipments, bringing damage to data center equipment operation.	High-risk operation white list control Intrusion detection Minimize the system 24-hour security situational awareness Proximity access control authority management
4	Tampering or stealing electricity data	Stealing electricity data and analyzing customer operations to harm business interests.	Sensitive data encryption Data integrity protection Redundant backup of critical configuration data
6	Stepping Attack on the internal network	Attacking customer internal networks through management systems/power supply/cooling equipment.	Security deployment and reinforcement Network Isolation Component-based/service-oriented independent deployment

2.3 Supply Security

Faced with the complex international political situation today, the trend of hard decoupling has become apparent. Supply security is becoming increasingly important.

With the outbreak of the Russo-Ukrainian War in February 2022, Russia's supply chain has been completely blocked by the Western camp. Vulnerabilities and strategies of supply security are shown in Figure 5.

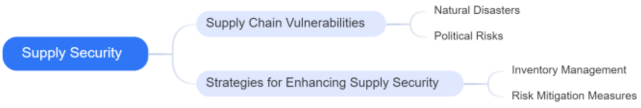

Fig. 5. Vulnerabilities and strategies of supply security

The Western camp isolated Russia by interrupting networks, commodities, after-sale services, certificates, realm names, public opinions, and international standard cooperation. Microsoft, IBM, Google, and Oracle stop their software and services such as backbone Internet transmission, issuing SSL certificates, realm names resolution, and international transmission network. Equipment supplier refuses to provide equipment and after-sales services, which makes current network operating equipment face the risk of inability to maintain. At the same time, Facebook and Twitter prohibit Russia from speaking out and occupy the battlefield of public opinion. Due to the lack of an independent and controllable industrial chain, these measures make Russian’s online activities near paralysis and pose serious threat to Russia's national security.

Equipment suppliers should be estimated in the process of data center construction to ensure the supply safety of equipment and after-sales services. At the same time, localization not only means produced by domestic manufacturers, but also means the localization of core components. Domestic manufacturers should deepen into the product design and control algorithm design. A diversified and autonomous supply chain system is the foundation for the supply security of data center infrastructure.

3 Conclusion

Data center infrastructure security is a systems engineering. It is an important component of data center security and the foundation for the safe operation of the entire data center. In order to protect the security of data center infrastructure, efforts need to be made in various aspects such as equipment manufacturing, physical and architectural design, operation and maintenance, etc. Comprehensive protective measures and continuous security management are necessary to ensure the safe and stable operation of data centers and protect user data assets and business continuity.

References

1. Manyika, J., Lund, S., Bughin, J., Woetzel, J., Stamenov, K., & Dhingra, D. (2016). Digital globalization: The new era of global flows. Retrieved from. https: //www.mckinsey.com/business-functions/mckinsey-digital/our-insights/digital-globalization-the-new-era-of-global-flows.
2. Cong Wang, Cuirong Wang, Xingwei Wang, Dingde Jiang. “Network Architecture Design for Data Centers Towards Cloud Computing,” Journal of Computer Research and Development, 2012, 49(2), pp. 286-293.

3. J. Marx Gómez, M. Mora, M. S. Raisinghani, W. Nebel, R. V. O'Connor (Eds.). "Engineering and Management of Data Centers: An IT Service Management Approach," Springer International Publishing, Cham 2017, pp. 73-89.
4. Postema, B. F., & Haverkort, B. R. "Evaluation of Advanced Data Centre Power Management Strategies," Electronic Notes in Theoretical Computer Science, 2018, 337, pp. 173-191.
5. Dan Li, Guihai Chen, Fengyuan Ren, Changlin Jiang, Mingwei Xu. "Data Center Network Research Progress and Trends," Chinese Journal of Computers, 2014, 37(2), pp. 259-274.
6. Hongbo Qin. "Research and Practice on Standard System Construction of Shanghai Green and Low—Carbon Data Center," SHANGHAI ENERGY SAVING, 2022, (7), pp. 779-784.
7. ingjing Wang. "Research on the Construction of Smart Data Center in City," Value Engineering, 2023, 42(2), pp. 136-138.
8. R. S. Coles, R. Moulton. "Operationalizing IT Risk Management," Computers & Security, 2003, 22 (6), pp. 487-493,
9. Ye Wang, Qiang Tu, Chengshu Cao. "Discussion about Basic Requirements for the Power Supply for Data Centers," Building Electricity, 2009, 28(11), pp. 23-27.
10. Xiao Liao, Jingsong Wu. "Discussion on Application of Row-based Cooling Used in High Power-density Data Center," Southern Energy Construction, 2015, 2(B12), pp. 172-177.
11. Yan Li, Peng Lv, Long Li. "Construction and Research on the Virtuahzation System of High Performance Data Center in Institutions of Higher Learning——Taking South Central University for Nationalities and Its library as Example," Library Theory And Practice, 2016, 0(2), pp. 74-79.
12. Barış Özkan, Mehmet Erdem, Eren Özceylan. "Evaluation of Asian Countries using Data Center Security Index: A Spherical Fuzzy AHP-based EDAS Approach," Computers & Security, 2022, Volume 122, pp. 102900.
13. J. Zhou, A. Raza, H. Sui. "Infrastructure investment and economic growth quality: empirical analysis of China's regional development," Applied Economics, 2021, 53 (23), pp. 2615-2630.
14. Jinzhi Jiang. "Discussion on Data Center Physical Environment Security," China Science & Technology Overview, 2023(22), pp. 64-66.
15. Wenxu Shen, Mingliang Cui. "Research on Network Security Operation and Maintenance Strategy of Data Center Network," China Computer Communication, 2023, 035(004), pp. 242-244.
16. K. Zhang, Y. Zhang, J. Liu, X. Niu. "Recent advancements on thermal management and evaluation for data centers," Applied Thermal Engineering, 2018, 142, pp. 215-231.