Research on Data Center Network Security Hardening Based on Media Convergence (Post-print)

Authors: Wu Honghui

Date: 2023-10-08T00:00:00+00:00

Abstract

Currently, the strategic decisions promulgated and implemented by China have effectively facilitated Internet development, gradually integrating Internet thinking into both daily life and production. Furthermore, the gradual convergence of traditional and new media has become a cornerstone for national strategy implementation. Under the synergistic influence of multiple factors, the quality of people' s production and living standards has been substantially enhanced. As cybersecurity is intimately linked to social stability and the smooth operation of the nation, and network data centers contain usage data and confidential files of target groups while simultaneously providing data transmission and exchange services for multiple users, the cybersecurity construction of data centers assumes paramount importance and requires urgent resolution within the broader media environment. Only by safeguarding data center cybersecurity can a secure national environment be fostered and the production and daily life of the people be effectively protected. This paper, based on the significance of strengthening data center cybersecurity construction under current media convergence, proposes strategies for cybersecurity reinforcement and designs a framework for cybersecurity solutions, with the aim of providing references for future research.

Full Text

Research on Data Center Network Security Reinforcement Construction Based on Media Convergence

Author: Wu Honghui (Nanjing Gaochun District Radio and Television Station, Nanjing, Jiangsu 211300)

Abstract: China' s current strategic policies have effectively promoted internet development and integrated internet thinking into daily life and production.

The gradual convergence of traditional and new media has become the foundation for implementing national strategies, significantly improving people' s quality of life under the combined influence of multiple factors. Since network security is closely linked to social stability and national operations, and data centers contain user data and confidential files while providing data transmission and exchange services for multiple users, data center network security construction becomes particularly critical and urgently needs to be addressed in the media convergence environment. Only by ensuring data center network security can we create a secure national environment and effectively protect people' s production and daily life. Based on the significance of strengthening data center network security construction under current media convergence, this paper proposes strategies for reinforcing network security and designs a framework for network security solutions, aiming to provide references for future research.

Keywords: data center; security protection measures; network security construction; framework design; security design

---

With the transformation of the internet information industry, an information age characterized by mobile internet technologies such as self-media and short-form new media videos has arrived. The integration of various information technologies has transformed bounded networks into borderless networks, gradually replacing the former limited boundaries of full-station networks. This increased openness presents severe security challenges and prominent safety issues. In the context of media convergence, we must vigorously strengthen network security efforts, ensure network security quality, and protect data center security to maintain a stable foothold for future development.

1. Overview of Data Centers

Data center construction has undergone decades of development alongside rapid information technology advancement. The prototype emerged in the 1940s with ENIAC (Electronic Numerical Integrator And Computer), developed in 1946 for the U.S. Ballistic Research Laboratory to store firing tables. In that era, only this computer could meet the requirements, featuring 17,468 vacuum tubes, 7,200 crystal diodes, 1,500 relays, 70,000 resistors, 10,000 capacitors, 1,500 relays, and over 6,000 switches. With its massive component count, it could perform 5,000 additions or 400 multiplications per second—1,000 times faster than relay computers and 200,000 times faster than manual calculations. In the 1950s, data center virtualization technology became commercialized with the emergence of transistor computers like TRADIC. The 1960s saw virtualization concepts gradually enter public consciousness. The 1980s introduced modular data centers, which deployed conventional data center equipment inside shipping containers (hence also called containerized data centers), transportable anywhere in the world. Though lacking the grandeur of traditional data centers, these offered extremely low construction costs (approximately 1% of traditional

data centers) and provided flexible mobility with shorter deployment cycles. In modern times, data centers have evolved into cloud data centers.

Data centers are core to supporting company operations and future development, encompassing "integrated servers, application platforms, centralized backup and storage models, unified platform management systems, customer-centered operational management organizations, and streaming media." This has gradually transformed data center operations from single to multiple business models with expanding scale. Information technology plays an increasingly important role in enterprises, and data centers are transitioning from pure consumption models to investment and revenue models.

2.1 Data Center Network Security as the Cornerstone of Governance in the Information Age

Today, people routinely discuss and use self-media and new media in their daily lives, from sixty- or seventy-year-old seniors to five- or six-year-old children, all proficient in using network media. However, China' s current network information platforms suffer from information redundancy and various risks and hidden dangers, making security issues critically important. In essence, maintaining data center and network security means protecting China' s political and cultural security.

With characteristics of high mass communication and broad interpersonal dissemination, the internet plays a vital role in building a harmonious society. As the IT industry rapidly develops, China' s policy interpretation methods have gradually shifted from traditional media to emerging media. Applying more new technologies widely disseminates the latest policies, guidelines, and strategies. Compared with traditional models, this approach offers lower costs, higher efficiency, and greater public acceptance. The government can also use internet technology to innovate management models and systems, expanding the role of electronic channels in daily office work and business operations. In pandemic environments, people can supervise work through network platforms, while the government can convey and interpret national policies to the public, enabling timely information reception. Government personnel communicating with citizens through network platforms ensures both safety and work efficiency.

2.2 Data Center Network Security as the Foundation for Building China into a Cyber Power

With the continuous development of internet information technology, informatization and network security have become important strategic issues for China' s national security and development, closely related to the lives and work of its vast population. We must grasp the overall situation and gradually build China into a cyber power through multi-party coordination. The most fundamental and critical step is completing infrastructure construction and improving various developing technologies to possess strong intrusion resistance capabilities.

We must prioritize media convergence-based data center network security in achieving the strategic goal of becoming a cyber power, firmly occupying advantageous positions in political and cultural domains of the superstructure in future competition, and making the country stronger through network technology.

3. Strategies for Reinforcing Data Center Network Security

3.1 Strictly Adhering to Data Center Network Security Construction Principles

Various operations on data—such as access, use, destruction, and modification—demonstrate that data is the top priority in data center network security maintenance. From the perspective of network data centers, networks are the fundamental platform for secure data center operation, serving data transmission functions. Therefore, the following principles must be observed in data center network security construction:

First, network security zones should be reasonably divided during construction, with clear hierarchical permissions between different zones. This ensures customers receive accurate authorization through identity authentication during use, preventing illegal intrusion and malicious data theft or damage. Second, a highly reliable network platform should be built, improving security levels to ensure safe and accurate data transmission, preventing data from being tampered with or read during transmission, and providing security protection for the network support platform itself to ensure stable and efficient operation. In summary, we must maintain an overall perspective in data center network security construction, avoiding reliance on a single method or preventive measure. We should adopt diverse measures, diversify system security protection measures, and employ multiple safeguards to ensure security. Construction should follow principles of simple operation and easy management, using the latest security technologies to achieve automated management procedures and reduce management burdens.

3.2 Firmly Controlling Public Opinion Orientation

The integrated development of traditional and emerging media has transformed the overall landscape of the media industry, shifting the main battlefield of public opinion struggle from traditional media to the internet. This represents a policy decision by our party and state to promote national soft culture and enhance cultural soft power. To firmly control public opinion orientation, we must be supported by advanced technology. In the context of media convergence, gaining initiative through public opinion orientation requires technological advantages to remain competitive in the fierce market. To achieve this, we must expedite infrastructure improvement. Although China holds advantageous positions in certain internet information technology fields, its infrastructure still lags behind many developed countries. We must break the situation of being

constrained by core technologies and equipment as soon as possible, which is detrimental to controlling public opinion orientation. Therefore, in the current media convergence process, we must vigorously improve various infrastructure components through multi-party coordination to better master public opinion autonomy.

Simultaneously, we must establish a network public opinion response mechanism for uncontrollable public opinion phenomena. With today' s highly developed networks, users can upload their observations to network platforms at any time, which can ferment and reach a climax within hours as user forwarding increases and various opinions converge. If we cannot control this situation well and instead avoid occurrences without providing positive guidance, this will undoubtedly increase negative impacts and hinder our ability to guide public opinion. Only by improving network public opinion monitoring systems and response mechanisms, regularly reporting and guiding online public opinion positively, responding directly to sensitive issues, and addressing social and public concerns can we maintain network security and keep the initiative in public opinion.

3.3 Innovating Courageously in Network Security Management Systems

Effective and scientific media management must be implemented to promote rapid integration of media with data center network platforms under the party' s correct leadership, and to manage different industry forms and ideologies online and offline efficiently, scientifically, and reasonably. We should transform management concepts, as only when ideological depth is achieved can management system innovation reach certain heights. Under the background of traditional and new media integration, previous traditional management models are no longer acceptable to the public and may not be 100% effective for media convergence. Management methods must progress alongside media convergence trends, with the two complementing each other to reach higher levels. In the internet information age, we must pay greater attention to the impact of online behaviors, making users responsible for their actions, controlling their own network speech, and supervising others. Responsible persons such as group administrators, forum moderators, and site owners have obligations to manage "internal" personnel.

We should also vigorously promote the Chief Information Security Officer (CISO) system. This system is crucial for maintaining network information security, with the CISO responsible for customizing information security strategies for the organization, predicting potential risk events, reporting to senior leadership, and proposing feasible solutions. Currently, this approach has been widely applied in some foreign countries, and China should introduce it, adapt it to our existing environment, and refine the process of maintaining network security to better contribute to data center network security reinforcement construction.

4. Framework Design for Network Security Solutions

This design addresses future development of the converged media platform, proposing requirements for security services, computing capabilities, and resource services. By introducing mature and advanced technologies, it adjusts and improves the overall framework of data center construction, using cloud computing as the core to achieve a service-centered construction approach based on converged media centers.

This design requires adopting the security framework shown in the figure, which must address boundary security, whole-network security visibility, data security, and more. Boundary security includes security domain isolation capabilities, network optimization capabilities, and user management capabilities. Security domain isolation primarily refers to the ability to segment network areas, thereby restricting traffic between zones and precisely controlling network flow to avoid large-scale security risks. Network optimization capabilities require providing flexible traffic management for user applications to ensure network bandwidth for critical users and applications and guarantee data transmission quality. User management capabilities mainly involve controlling user behavior on the access network, including controlling network access behavior, restricting access resources, and identity authentication.

4.2.1 Boundary Security

With internet development, information security issues have become increasingly severe. China has proposed strengthening all-round, all-weather perception of network security situations and continuously strengthening network security management. Whole-network security perception platforms typically consist of security perception systems and threat detection probes, offering high service response capabilities and deep analysis, which improves network data security processing performance to a certain extent. Security perception systems based on big data can perform traffic monitoring and data analysis, enabling comprehensive detection of massive data analysis.

To protect boundary security, we must first understand which network boundaries need protection, often determined through security zoning design. This design includes many boundaries: security management boundaries, internal office network boundaries, converged media platform boundaries, public cloud/dedicated cloud boundaries, provincial platform boundaries, and overall network exit boundaries.

4.2.2 Data Center Cloud Security

This design establishes a north-south security protection system for cloud platform tenants/tenant boundaries based on a virtualized architecture equal protection integrated machine security platform. The equal protection integrated machine architecture utilizes software virtualization, information security technology, service chain management, and Overlay technology to achieve an adap-

tive security technology architecture. Due to its open nature, the equal protection integrated machine can support third-party security component integration and provide users with a fully functional cloud security service market.

4.2.3 Host Security

Server endpoint security primarily consists of a control center and virtual endpoint agents. Endpoint agents must be installable on all hosts, including all physical hosts, cloud hosts, and virtual machines. The management platform should be deployed locally. After completing basic data collection, endpoint agents send useful data information to the control center, which then performs global aggregation and security analysis through the management platform.

4.2.4 Whole-Network Situational Awareness

First, Asset and Business Management. Based on functionality, internal network devices can be divided into two aspects: assets and business. The asset configuration details display module can identify transmission protocols, open ports, operating systems, and IP addresses of internal server assets. The business-asset relationship display module can constitute specific business groups according to asset IP addresses/address ranges.

Second, Monitoring and Identification Knowledge Base. The monitoring and identification knowledge base can identify massive amounts of data information with strong recognition capabilities.

Third, Visualization Platform. The whole-network attack detection visualization platform supports security situation awareness, enabling map-based and visual display of whole-network security events and attacks. The visualization platform can support whole-network business visualization, presenting access relationships of whole-network business objects and graphical display of invaded businesses. It also supports user-defined visualization of business asset management.

Fourth, Risk Visualization. According to equal protection requirements, it can visually display high-risk user violations, non-compliant behaviors, attack behaviors, and risky operations.

Fifth, Big Data Analysis Engine. The big data analysis engine is primarily responsible for implementing big data correlation analysis capabilities and various detection capabilities. This engine mainly consists of data preprocessing, model fusion, model construction, data fusion, and analysis result generation modules, which can greatly enhance data center network security capabilities.

Conclusion

Maintaining data center network security in the context of media convergence is a strategic choice in the information age and an inevitable trend in internet

information technology development. As China' s great rejuvenation continues, many challenges remain to be overcome. We must fully recognize existing problems and attach sufficient importance to them, base our efforts on China' s national conditions, adhere to the parallel development of progress and security, and build a cyber power through the joint efforts of all people and workers.

References: [1] Cai Gaowei. Research on Data Center Network Security Reinforcement Construction Based on Media Convergence [J]. Radio and Television Network, 2020, 364(04): 74-76. [2] Wang Yunbo. Thoughts on Network Security in the Context of Media Convergence [J]. Media Forum, 2019, 45(21): 94-94. [3] Zhao Peng. Research on Network Security Issues in the Context of Media Convergence [J]. Science and Technology Communication, 2016, 8(1): 198-200. [4] Xu Jian. Key Considerations in the Design of All-Media News Convergence Production and Release Platforms [J]. Television Engineering, 2015(003): 49-53. [5] Wang Fei. Media Convergence: Media Convergence Theory in the Digital New Media Era [M]. Guangzhou: Southern Daily Press, 2007. [6] Sun Yuan. How to Ensure Information Security in the Environment of Converged Media Construction [J]. Western Radio and Television, 2018, 439(23): 46-47.

Author Biography: Wu Honghui (1971-), male, from Nanjing, Jiangsu, engineer, research direction: radio and television technology. (Executive Editor: Hu Yang)

Note: Figure translations are in progress. See original paper for figures.