Research on Security Construction of Radio and Television Information Systems Postprint

Authors: Li Ping

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

Abstract

The development of the Internet has transformed operational models across various industries. In the process of continuous advancement within the broadcast television sector, there is extensive reliance on information technology. Currently, information system construction in the broadcast television domain has achieved relative maturity; however, information system security issues continue to emerge incessantly. Information security plays a vital role in safeguarding national security and promoting harmonious social development. Therefore, to fully leverage the capabilities of information systems and drive efficient development of the broadcast television industry, it is imperative to analyze existing system security issues and implement optimization measures. This paper presents an analysis of security construction for broadcast television information systems for reference.

Full Text

ChinaXiv Collaborative Journal

Research on Security Construction of Broadcasting and Television Information Systems

Li Ping (Beijing Radio and Television Station, Beijing 100022)

Abstract: The development of the Internet has transformed operational models across all industries. As the broadcasting and television sector continues to advance, it has become increasingly reliant on information technology. While information system construction in this field has reached a relatively mature stage, security issues have emerged incessantly. Information security plays a crucial role in safeguarding national security and promoting harmonious social development. Therefore, to fully leverage the functions of information systems and drive efficient development in the broadcasting and television industry, it is essential to analyze and optimize existing system security issues. This paper

examines the security construction of broadcasting and television information systems for reference.

Keywords: Internet; Broadcasting and Television; Information Systems; Security Construction

Classification Code: TP391
Document Code: A
Article ID: 1671-0134(2021)12-158-03
DOI: 10.19483/j.cnki.11-4653/n.2021.12.051

Citation Format: Li Ping. Research on Security Construction of Broadcasting and Television Information Systems [J]. China Media Technology, 2021(12): 158-160.

1. Characteristics of Broadcasting and Television Information System Security Construction

At present, China's broadcasting and television sector attaches great importance to information system security construction, viewing it as the guarantee for the normal operation of broadcasting and television network systems. In this construction process, informatization and digitalization technologies serve as key components. Overall, information system security construction exhibits three major characteristics [1].

First, operability. Information system security construction demonstrates strong operability, requiring that internal system functions satisfy integrated design principles, which provides substantial convenience for subsequent operations. Second, transmission capability. This characteristic means the system employs multi-channel load design with strong scalability and linear growth in speed. Third, security. This represents the most critical aspect of information system security construction. The very purpose of security design in the broadcasting and television industry is to provide safeguards for information system security, making security the natural core of the construction process. During implementation, the system integrates new antivirus software and employs multiple security strategy combinations to ensure information system security remains uncompromised.

2. Specific Structure of Broadcasting and Television Information System Security Architecture

The security architecture of broadcasting and television information systems primarily consists of three layers: management, operation, and technology [2]. The management layer encompasses information security-related legal knowledge, policies, management mechanisms, and organizational structures, representing the highest level of the entire system and providing policy guarantees.

The operation layer serves as the intermediate level, mainly providing material support for television information systems, including specifications for equipment production, application, installation, and maintenance. The technology layer primarily offers technical support for the system. Although its internal content is less extensive than the management and operation layers, its role remains significant, mainly comprising information reception technology, source technology, and communication technology. These three layers each play distinct roles within the system; the absence of any one layer would compromise information system security. Through their close integration, system operation becomes more orderly and standardized, with security issues handled systematically. The three layers mutually constrain yet complement one another.

3. Specific Manifestations of Security Issues in Broadcasting and Television Information System Construction

To address the various existing security issues, effective strategies must be implemented to improve system security and ensure high-quality development of the broadcasting and television industry.

3.1 Virus Intrusion

Virus intrusion represents one of the most common security issues in broadcasting and television information systems. Viruses refer to instructions or codes inserted into system programs that can destroy system functions or corrupt data. As technology advances, virus forms have gradually diversified, making information systems vulnerable to attacks. Viruses evolve according to their creators' intentions and exhibit proactive characteristics. In recent years, the variety of information system viruses has continued to increase and remains under development. Viruses differ in their attack purposes and natures. While broadcasting and television information systems have established preventive measures against traditional viruses, their preparedness for new viruses remains inadequate, leaving system security in a precarious state.

3.2 Hacker Attacks

Broadcasting and television play an important role in China's harmonious social development as a crucial medium for news dissemination. However, recent observations of broadcasting and television information systems reveal that hacker attacks occur frequently, becoming a major factor affecting normal system operation and a significant cause of information security vulnerabilities [3]. Hacker attacks vary in severity. Minor attacks may result in partial data theft and brief system malfunctions, while severe attacks can lead to direct network occupation and system destruction. Some hackers even attempt to spread rumors through broadcasting and television platforms, creating obstacles to secure system operation.

3.3 Operating System Vulnerabilities

Operating systems occupy a critical position in information systems as the primary platform for hardware resources. Software functions cannot be successfully realized without relying on operating systems, which serve as the connection between hardware and software. Their main functions include memory allocation, resource supply-demand sequencing, input-output device control, and network file system operation. However, during operation, operating systems may sometimes be exploited by other programs, causing normally functioning systems to suddenly malfunction and posing risks to information systems. As a key component of information systems, any security compromise to the operating system will directly affect the normal operation of other components.

3.4 Security Risks in Network Structure and Equipment

Information systems in China' s broadcasting and television industry generally employ hybrid topology structures. Network nodes such as switches or hubs inherently contain security risks, yet these vulnerabilities are not identified before deployment, becoming increasingly apparent during subsequent application. The most obvious security vulnerability lies in the physical addresses of hardware interfaces, which are highly susceptible to network attacks and represent a difficult point in security prevention for China' s broadcasting and television information systems.

3.5 Uneven Hardware Configuration

Hardware configuration in broadcasting and television information systems exhibits inconsistency, with most configurations meeting only current demands and lacking long-term vision. This results in hardware becoming obsolete after a period of use due to its inability to meet application requirements, necessitating replacement. When hardware configuration lacks scientific planning, the system' s risk prevention and resistance capabilities become weak. Furthermore, some equipment continues operating beyond its service life. Aging hardware devices not only fail to improve work quality but instead reduce overall system efficiency, which is detrimental to the development of the broadcasting and television industry [4].

3.6 Non-standardized Management

Non-standardized management of broadcasting and television information systems manifests primarily in several aspects. First, the lack of a security management center prevents effective management of security components, hardware, and software within the system, resulting in deficiencies in software distribution, hardware configuration, virus prevention, and security control. The security management center' s primary function involves analyzing, locating, and resolving various security issues within the system. Without such a center, system security cannot be enhanced, allowing security issues to gradually proliferate.

Second, system security maintenance remains in its preliminary stages, lacking extensive experience. The maintenance methods employed are relatively simple, and the absence of professional talent support leads to low levels of system security maintenance. Third, although China' s broadcasting and television industry has established network security management departments and defined their responsibilities, practical implementation is constrained by internal and external conditions, resulting in imperfect mechanisms for supervision, detection, and response to system security issues. Without robust mechanism support, system information security cannot be effectively guaranteed. Fourth, during network information security management, some administrators lack security awareness and fail to recognize the importance and necessity of security management. Moreover, users also lack strong security awareness when using the system, often exhibiting improper usage habits that create significant hidden dangers for system information security.

3.7 Insufficient Security Assessment and Testing

Broadcasting and television information systems face numerous factors causing security issues. Beyond the aforementioned manifestations, insufficient security assessment and testing work can also directly trigger security problems. China's broadcasting and television field has limited exposure to information system security assessment and testing, representing a significant gap in this area. When broadcasting and television organizations conduct assessment and testing work, they are also constrained by objective factors such as capability, technology, and equipment, with municipal-level broadcasting and television systems facing even greater difficulties in implementation. Security assessment and testing typically rely on network security inspection, yet the specific testing process involves narrow scope and simplistic methods, capable only of identifying simple or obvious security issues while failing to conduct in-depth system detection. This results in potential hidden security problems remaining undiscovered until they gradually emerge during later operation, by which time repair becomes more difficult and costly.

4. Effective Approaches for Broadcasting and Television Information System Security Construction

4.1 Application of Virus Protection Technology

To fundamentally prevent virus intrusion, virus protection technology must be applied to provide comprehensive protection for information systems. Viruses enter information systems through networks, indicating that network access is a prerequisite for virus infiltration into broadcasting and television information systems. Based on this understanding, broadcasting and television information systems must implement comprehensive network security strategies, utilizing antivirus software to scan all incoming information and block anything harmful to the system [5]. Additionally, firewall deployment can be enhanced as

the first line of defense against external intrusion. Firewalls can effectively prevent virus attacks on information systems. During operation, firewalls detect relevant permission verification objects and provide prompts based on the current operational status of the information system, allowing users to select permissions for installation. Firewalls can also automatically detect permissions, shielding those detrimental to the system and thereby reducing system risks. Furthermore, firewalls can issue warnings for erroneous instructions and immediately filter out harmful information, ensuring that incoming information poses no threat. During firewall installation, cloud computing technology can be employed to upgrade the system and establish automatic update functionality, enabling firewalls to upgrade automatically once the system issues an update command, significantly improving system operational reliability.

4.2 Application of Encryption and Access Control Technologies

Encryption technology serves as the cornerstone of broadcasting and television information system security, substantially enhancing information security through data encryption. Broadcasting and television operations involve numerous important information pieces requiring storage. Data information can be encrypted using encryption keys and functions to transform it into meaningless ciphertext, which recipients must decrypt to plaintext before viewing. This encryption method is well-suited for broadcasting and television information systems, ensuring that important data cannot be accessed illegally. Access control technology represents an effective strategy for preventing hacker intrusion, primarily deployed on devices such as routers or switches to control network access permissions. Applying this technology in broadcasting and television information systems enables control over system visitor permissions, allowing access only under secure conditions. In practical application, configuring access control lists in routers can create a robust firewall that screens IP data entering and exiting devices, isolating potentially intrusive access permissions and preventing illegal hacker intrusion.

4.3 Construction of Structural Protection Framework

During the security construction of broadcasting and television information systems, structural protection frameworks should also be established to prevent various security issues. The focus of broadcasting and television system construction should partially shift to framework building, ensuring specific construction work proceeds under structured protection concepts. This approach enables comprehensive network edge coverage of information systems, placing the entire information system within network protection scope. Regarding the definition of information system access paths, all interface parameters and related security protocols should remain robust. To ensure effective object access, internet access application path processing should also be properly handled, thereby effectively protecting the core of the broadcasting and television information system framework and enhancing overall system security [6].

4.4 Strengthening Software and Hardware Prevention

Both software and hardware occupy core positions in broadcasting and television information systems. If a terminal device becomes infected, the probability of servers or other terminal devices being affected increases accordingly. During hardware security prevention, user behavior can be managed through the establishment of operational norms to constrain user actions. Unnecessary service ports on hardware devices should be promptly closed, and arbitrary installation of system software should be prohibited. When managing broadcasting and television information system accounts, diversified settings should be adopted for authentication, authorization, and passwords. Regarding aging hardware equipment, the broadcasting and television field must replace it promptly and must not take chances [7]. Broadcasting and television information system software primarily includes operating systems and databases. To prevent software security failures, reliable software with inherent security development guarantees should be selected. Upon initial software application, broadcasting and television platform software security specifications should be promptly issued. Vulnerability information released by software vendors must be tracked immediately, with scientific and reasonable remediation plans formulated based on actual vulnerability conditions to improve software application stability.

4.5 Improving System Management Regulations

Security construction of broadcasting and television information systems cannot succeed without robust management regulations, which provide strong support for the entire construction process. The information system operating environment should be strengthened, with internet terminal application usage supervised to prevent improper operations from affecting system security. Important information data should be backed up, and reward-punishment mechanisms should be clearly defined. Employees performing well in management work should receive material or spiritual rewards, while managers who repeatedly make mistakes without correction should face corresponding penalties, ensuring that reward-punishment mechanisms exert their deterrent effect and guaranteeing the effective implementation of information system security management. Additionally, to enhance practical applicability, existing emergency plans can be improved by establishing an integrated support system using internet and computer technologies that combines equipment operation monitoring, emergency command, safe broadcasting, and early warning release functions, comprehensively improving broadcasting and television information system security levels.

4.6 Strengthening Security Assessment and Testing

Security assessment and testing permeates the entire lifecycle of broadcasting and television information systems. Without such testing, system security cannot be determined. The depth of system security assessment and testing must be enhanced, with detection scope expanded and diversified evaluation methods employed to ensure potential security issues can be identified, providing

guarantees for subsequent efficient operation [8]. During actual assessment and testing, comprehensive detection should be conducted on system equipment operation, user behavior, and network edge data behavior. When anomalies are discovered, they must be promptly reported without concealment, with serious consequences of concealment attributed to responsible individuals. User behavior should also be audited and evaluated, including login activities, core business operations, and configuration modifications. During assessment and testing, corresponding records should be maintained, clearly documenting specific testing objects, times, locations, events, and types to provide supporting evidence when necessary [9].

References

[1] Gao Xiaoqing. Network Security Risks and Strategies for Broadcasting and Television Information Systems [J]. Communication World, 2019(11): 51-52.
[2] Meng Lianrong. Security and Confidentiality Design of a Broadcasting and Television Information System [J]. Radio & Television Information, 2016(S1): 102-103.
[3] Qiu Furu. Application Research on Information Security Systems Based on Broadcasting and Television Network Convergence Terminals [J]. Wireless Internet Technology, 2020(16): 15-16.
[4] Fang Minye. Maintenance of Broadcasting and Television Information Transmission System Security [J]. West China Broadcasting & TV, 2016(17): 232.
[5] Chen Le. Analysis of Broadcasting and Television Information Platform Construction and Application in the Cloud Technology Era [J]. Information Weekly, 2019(41): 1.
[6] Zhang Li. Discussion on Current Status and Countermeasures of Broadcasting and Television Control Technology Safety Management [J]. Digital Users, 2019(4): 59.
[7] Xu Cheng. Research on Network Information and Data Security of Television Broadcasting Systems [J]. West China Broadcasting & TV, 2019(19): 255-256.
[8] Ren Xiaowei. Research on Network Security Hardening Methods for Broadcasting and Television Information Systems [J]. Broadcasting & Television Technology, 2019(2): 8-12.
[9] Peng Jie. Methods for Maintaining the Security of Broadcasting and Television Information Transmission Systems [J]. China Media Technology, 2014(6): 129.

Author Biography: Li Ping (1978-), female, from Xining, Qinghai, holds a master' s degree and is a senior engineer. Her research focuses on broadcasting and television information system construction and operation maintenance.

Responsible Editor: Zhang Xiaojing

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