Practice and Reflections on the Implementation of Multi-Level Protection Scheme for Cybersecurity in Press Groups: Post-Print

Authors: Zhang Yafeng

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

Abstract

The article is grounded in the key considerations for constructing network system security level protection evaluation frameworks, elaborates on the importance of such evaluations, and provides a detailed analysis of both the essential elements in building network security architectures and routine operational issues, thereby offering reference material for technical personnel at newspaper groups engaged in security level evaluation and construction.

Full Text

Preamble

Title: Cybersecurity Level Protection Construction: Practice and Reflections for Newspaper Groups

Abstract: This article focuses on the key aspects of cybersecurity level assessment and construction, elaborates on the importance of such assessment, and provides a detailed analysis of the critical elements in cybersecurity system construction and common daily issues, offering reference material for technical personnel in newspaper groups engaged in level protection assessment and construction.

Keywords: Information security system construction; Network system security level assessment

CLC Number: TP393

Document Code: A

Article ID: 1671-0134(2019)11-126-03

DOI: 10.19483/j.cnki.11-4653/n.2019.11.034

Author: Zhang Yafeng

1. Defining Assessment Objects

The primary business systems in newspaper groups currently include news editing systems, new media production and publishing systems, reporting command systems, media asset systems, business management systems, office automation systems, internet mail, and "central kitchen" information systems. These are all internet-based application systems facing major threats such as unauthorized data access, information leakage, illegal access, viruses, Trojans, APT attacks, insufficient security control enforcement, policy failures, and business vulnerabilities that can easily trigger cybersecurity risks.

The level protection classification for information systems must be planned from the initial construction stage. During the organization' s overall information planning process, boundary isolation should be implemented for interconnected areas, while shared components must meet the highest level protection requirements. Generally, a provincial newspaper group has approximately ten Level 3 systems requiring assessment. Given significant financial pressures in recent years and the high cost of cybersecurity hardware, how can newspaper groups save money while ensuring comprehensive security? Some groups choose to assess only critical information infrastructure while leaving other systems unassessed, with some even selecting just a single system for evaluation. Other groups treat all systems as one integrated system for assessment purposes, describing different functions as subsystems within the overall functional description. This approach requires clearly defining boundaries between subsystems but can save substantial assessment costs.

2. Information Security System Construction

As media convergence deepens, new media businesses within newspaper groups continue to expand, and application systems have gradually transformed from traditional editorial and publishing systems to omnimedia publishing systems, shifting from internal network systems to external network systems. In recent years, as news websites have gained increasing weight in major search engines, they have become prime targets for hacker attacks. Overseas gambling operations have besieged news websites through various means, and most domestic news websites have experienced intrusions, creating a severe cybersecurity situation. How can network system security be ensured? Cybersecurity level protection can comprehensively guarantee the safe and stable operation of network systems.

During level protection implementation, security management system construction is fundamental to protecting network systems. Whether a comprehensive security management system can be established is the key focus of level protec-

tion implementation. A complete security management system includes security management organizations, technical management, and security operations management, which are detailed below.

The security management organization is the highest leadership authority for managing network systems. The top leader is generally the unit' s executive leader or an authorized representative, establishing a security management committee or leading group as appropriate. The security management organization should appoint a director and dedicated security administrators, implementing three-role management for personnel configuration, with key positions managed jointly by multiple personnel. Approval matters and processes must be clearly defined, including important items such as system changes, critical operations, physical access, system integration, and major activities. A hierarchical approval system and regular review and approval system should be established. Routine operational matters such as daily operations, system vulnerabilities, and data backup should be documented in standardized forms. Comprehensive inspection items should be established, including consistency checks for policies and configurations, effectiveness checks for security measures, and major issues should be summarized in written reports.

Regarding security personnel management, background checks and skills assessments must be conducted, confidentiality agreements signed, and key position personnel agreements established. Upon personnel departure, permissions should be promptly terminated and departure confidentiality agreements required. Active personnel require security awareness education and position-specific skills training, with notification of security responsibilities and disciplinary measures. Different training plans should be developed for different positions, and regular skills assessments conducted for various positions. When external personnel access controlled areas, they must submit written applications, obtain authorization, be accompanied by designated personnel throughout their visit, and register for record-keeping. Access to controlled networks requires written applications, guest account creation with assigned permissions, and registration; permissions must be promptly cleared after departure. Confidentiality agreements must be signed with authorized external personnel, prohibiting the copying or disclosure of sensitive information. External personnel are generally prohibited from accessing core critical areas and applications.

System security construction includes selecting security measures based on the filed protection level, adjusting preventive measures according to risks, conducting overall security planning and scheme design for network systems with supporting documentation, completing reviews of the overall security planning and supporting documents, and commencing implementation. During the implementation phase, cybersecurity products compliant with national regulations and cryptographic products conforming to relevant cryptographic authority provisions must be selected. Products for critical components should undergo specialized testing before selection. For proprietary software, development and actual environments must be separated, with standardized code writing, com-

plete development process documentation, strict authorization for modifications, updates, and releases to program resource libraries, strict version control, and controlled development activities with malicious code detection. For externally procured software, malicious code detection must be performed, and complete documentation and user guides must be provided. During engineering implementation, designated personnel must manage the implementation process and develop engineering implementation plans. Qualified newspaper groups should implement third-party supervision. During system acceptance, acceptance plans, acceptance reports, and pre-launch security testing reports must be provided, including cryptographic application security testing. During system delivery, delivery lists, personnel training, construction process documentation, and operations and maintenance documentation must be provided.

System security operations management includes computer room environment management, asset management, operation monitoring, data backup, and security measure implementation, requiring dedicated personnel for computer room security management. Computer room environment management includes: computer room access and operations management, computer room security management systems (including prohibition of casually placing media and documents containing sensitive information), authorization of access personnel by security level, and real-time monitoring of critical areas. Asset management includes asset inventories, asset identification management, and asset management personnel. Media management includes secure storage, dedicated personnel management of specialized media, regular inventory checks, and controlled media circulation with records. Vulnerability and risk management includes: inspections, timely patching or post-assessment patching, risk assessment with report generation, and implementation of countermeasures. Important equipment configuration and operation manuals must be developed, operations and maintenance logs maintained, and logs and monitoring data analyzed. Logs must be retained during operations, with configuration libraries updated synchronously. Operations and maintenance tools must be used strictly with logs retained and sensitive information promptly deleted. Malicious code prevention management includes virus scanning of external connections, specification of malicious code prevention requirements, virus database upgrade checks, analysis of captured samples, and regular verification of anti-virus technical measure effectiveness. Backup and recovery management includes identification of critical business information, system data, and software requiring backup, specification of backup methods, media, and frequency, and development of backup strategies, recovery strategies, and procedures. Security incident handling includes timely security incident reporting, development of security incident reporting and handling management systems, cause analysis, lesson summarization, different handling procedures and reporting processes for major service interruptions and information leakage incidents, establishment of joint protection and emergency response mechanisms, and handling of cross-organizational security incidents.

3. Daily Management Issues and Considerations

The information security system provides comprehensive specifications from three aspects: information security management, information security technology, and information security operations. Through construction in these three areas, a complete information security system is formed that fully complies with all level protection assessment indicators when properly implemented. However, in practice, many newspaper groups' security systems often become mere formalities with inadequate implementation, existing only for level protection assessment purposes. This situation primarily arises from insufficient awareness of network system security protection, inadequate budget allocation, and insufficient staffing, leading to poor execution of security policies and rendering security systems nominal. Although some may pass cybersecurity level assessment, their network systems still harbor significant security risks. Only by strictly following established requirements for daily management can assessed network systems be ensured to operate securely.

References

[1] Lin Ningsi, Lai Jianhua. Research on Security Protection System for E-Government Website Clusters[J]. Fujian Computer, 2011-08-25.

[2] Xu Chengliang. Security Risk Analysis and Countermeasures for Electronic Bidding Systems[J]. Bidding and Procurement Management, 2017-10-25.

(Author' s Affiliation: Hebei Daily Newspaper Group)

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