 DOI: https://doi.org/10.12349/iser.v6i4.5296

Design of network security and information security under the new situation

Li Tan

Shizhu Tujia Autonomous County Rongmedia Center, Chongqing, 409199, China

Abstract

With the rapid development of information technology, the role of financial media center in the field of information communication is increasingly prominent, but the subsequent problems of network security and information security are becoming increasingly serious. This paper first analyzes the challenges faced by the financial media center in network security and information security, and then puts forward the solution to build an integrated architecture. Through in-depth research, this paper constructs a set of network security and information security integrated architecture for the financial media center, aiming to provide a strong guarantee for the safe operation of the financial media center. The research results show that this structure can effectively improve the network security protection capability of the financial media center, and provide strong support for the development of China's financial media industry.

Keywords

financial media center under the new situation; network security; information security; integrated architecture

新形势下融媒体中心网络安全及信息安全一体化架构设计

谭丽

石柱土家族自治县融媒体中心，中国 · 重庆 409199

摘　要

随着信息技术的高速发展，融媒体中心在信息传播领域的作用日益凸显，但随之而来的网络安全和信息安全问题也日益严峻。本文首先分析了融媒体中心在网络安全及信息安全方面所面临的挑战，随后提出了构建一体化架构的解决方案。通过深入研究，本文构建了一套针对融媒体中心的网络安全及信息安全一体化架构，旨在为融媒体中心的安全运行提供有力保障。研究结果表明，该架构能够有效提升融媒体中心的网络安全防护能力，为我国融媒体事业的发展提供有力支持。

关键词

新形势下融媒体中心；网络安全；信息安全；一体化架构

1 引言

随着互联网、大数据、云计算等新一代信息技术的迅猛发展，融媒体中心作为信息传播的重要平台，其作用日益凸显。然而，在信息传播速度和广度不断扩大的同时，网络安全和信息安全问题也日益严峻。融媒体中心面临着来自网络攻击、数据泄露、恶意软件等多方面的安全威胁，这对融媒体中心的正常运营和信息安全构成了严重挑战。因此，研究新形势下融媒体中心网络安全及信息安全一体化架构设计，对于保障融媒体中心的安全稳定运行具有重要意义。本文探讨了融媒体中心网络安全及信息安全一体化架构的设计思路。

【作者简介】谭丽（1981–），女，土家族，中国重庆人，本科，工程师，从事电子信息技术研究。

2 新形势下融媒体中心网络安全及信息安全一体化架构的需求分析

2.1 业务需求分析

融媒体平台需保障不同媒体形式的信息资源能够实现互通，包含文本、图形、声音和视频等多种媒介形式。提供个性化的内容与服务推荐，迎合用户独特的需求，提升用户的使用体验。信息可在多个渠道广泛传播，涉及手机、电脑、电视等设备，保证过渡的顺畅。融媒体团队借助网络平台实现远距离协作，提高作业执行速度。对用户行为和内容资料进行深入挖掘与分析，提供决策支持。

2.2 安全需求分析

融媒体中心的内部数据、用户信息及业务资料必须得到妥善防护，避免其被泄露、篡改或遭受损害。防止恶意攻击、病毒感染、系统漏洞等对融媒体中心系统造成不利后果。保障融媒体中心网络环境的内外安全，防御网络攻击、诈骗网站等风险。保障用户身份验证的合法性和有效性，禁止未

授权的入侵行为。确立紧急预案，解决网络安全相关事宜，减少损失。

2.3 性能需求分析

该平台系统必须拥有卓越的高并发处理能力，满足大量用户对于并行访问的期望。系统对用户请求的响应必须快速，保障用户满意程度。系统始终保持稳定的运行状态，降低故障的频率。系统理应具备卓越的扩展性能，符合业务增长的需求。该系统需兼容多种操作系统与浏览器，满足不同用户需求。

3 融媒体中心网络安全及信息安全一体化架构的设计

3.1 网络安全架构设计

3.1.1 边界防护

边界防护是网络安全架构中的第一道防线，旨在确保内外网之间的安全隔离，防止恶意攻击和非法访问。在内外网之间部署高性能防火墙，对进出网络的数据进行过滤、识别和阻止，实现对网络流量的精细化控制 [1]。在内外网边界部署入侵检测与防御系统，实时监控网络流量，识别异常行为，及时响应和处理安全事件。对于需要远程访问内网的用户或设备，采用 VPN 技术建立加密通道，确保数据传输的安全性。

3.1.2 入侵检测与防御

入侵检测与防御是网络安全架构中的核心组成部分，主要目的是实时监测网络中的恶意攻击行为，及时采取措施进行防御。对网络流量进行实时监控，分析异常行为，发现潜在威胁，及时报警。在 IDS 的基础上，对检测到的恶意行为进行实时阻断，防止攻击者进一步破坏网络。将来自不同安全设备的报警信息进行整合，实现统一监控和管理，提高应对安全事件的效率。

3.1.3 安全审计

安全审计是网络安全架构中的重要环节，通过对网络行为的记录和分析，发现潜在的安全隐患，为安全管理和决策提供依据 [2]。日志审计对网络设备、服务器、应用系统等产生的日志进行收集、存储和分析，及时发现异常行为。行为审计对用户在网络中的操作行为进行监控，识别违规操作，确保网络安全。安全合规性审计对网络安全政策、标准、规范进行审查，确保网络安全管理符合国家法律法规和行业标准。

3.2 信息安全架构设计

3.2.1 数据加密

采用先进的加密手段，包括 AES 和 RSA 在内的，在传输和存储数据过程中执行加密措施，确保数据传输过程中的安全性及完整性。将易受损的数据进行分类，根据不同的敏感度等级，采取适当的加密手段，涵盖高级加密及中等加密强度。对加密密钥执行严格的监管，通过密钥管理器进行密钥的生成、存储、分发与回收处理，确保密钥的保密不被泄露。

3.2.2 身份认证与授权

实施全面的认证策略，包括密码、指纹和面部识别在内的生物识别技术，提升认证的安全性。建立一个综合性的用户身份验证体系，统一管理用户身份信息，确保用户身份的唯一性与真实性 [3]。根据用户的身份和权限，实施严格的访问权限控制，确保用户只能查看获授权的信息。定期对用户的身份和权限进行核实，快速诊断并处理异常问题。

3.2.3 安全管理

建立完善的安全管理机制，明确划分各岗位与部门的安全职责，确保安全管理措施得到切实执行。持续进行安全风险评估，制定应对潜在安全威胁的策略。实施安全事件监控，持续监测异常举动，快速发现并处理安全事故。增强安全意识培训，提升员工对安全的警觉度及操作技能。定期举办安全演练，检验应急方案的执行效果，提升应对突发状况的能力。提升与外部安全机构的合作水平，快速获取安全信息，共同应对网络安全难题 [4]。采用先进的安全技术和产品，涵盖了防火墙、入侵检测系统以及漏洞扫描等工具，提升网络安全防护能力。定期维护并更新网络安全设备，确保其性能和安全性。

4 融媒体中心网络安全及信息安全一体化架构的实现

4.1 技术选型

应优先考虑采用具有超群安全特性的技术，确保融媒体中心网络及信息的安全防护。该系统采用 Linux 作为操作平台，该机子拥有出色的安全保障、稳定性和兼容性。挑选 MySQL 或 Oracle 作为数据库管理系统，具备出色的性能、稳固的可靠性和便捷的操作性。挑选一款功能强大的防火墙，Check Point 或 Fortinet，保障全面的安全性。运用入侵检测及防御技术，例如 Snort 或 Suricata，对网络中的异常行为进行不间断的监督。运用漏洞扫描及修复工具，包括 Nessus 和 OpenVAS 等，快速发现并修复系统漏洞。实施一种统一的安全管理模式，IBM 的 QRadar 安全解决方案与阿里云的安全管理平台，实现一致的安全管理标准。

4.2 系统部署

根据业务需求，对系统进行分区域管理，涵盖内部网络、外部网络及安全区域等。对系统实施分层次的处理，涵盖物理层、网络层、应用层等不同层次，提升系统的稳固性。对关键设备进行备份和冗余配置，确保系统在发生故障后能快速恢复正常运作。制定严格的安全防护措施，涵盖权限控制、数据加密手段及日志审核等方面。本层包括服务器、网络和存储等硬件设备。网络层由交换机、路由器以及防火墙等网络设备组成。应用层由业务系统、安全管理平台及数据库等要素构成。

4.3 测试与优化

核实各功能是否符合既定的设计标准。系统面对高并发与大量数据处理的性能表现。通过安全测试来确认安全策略的实效性，发现并修复潜在的安全漏洞。稳定性测试系统在长时间运行中的表现，确保系统始终保持稳定运行。根据测试获得的数据，对系统进行优化升级，提升系统的功能与安全保障 [5]。处于测试与优化环节，采用自动化测试工具，增强测试效率。重现高流量及大量数据的环境，对系统运行效率进行评价。模拟黑客攻击行为，对安全防护效能的评估系统。实施持续集成与持续交付（CI/CD）流程，提高系统运维效率。

5 融媒体中心网络安全及信息安全一体化架构的运行与管理

5.1 安全策略制定与执行

5.1.1 安全策略制定

融媒体中心网络安全及信息安全一体化架构的安全策略制定，应遵循国家网络安全法律法规、行业标准以及相关政策要求。确保融媒体中心信息系统安全稳定运行，保障信息资源安全，维护国家利益、公共利益和个人合法权益。遵循最小权限原则、完整性原则、可用性原则、保密性原则等，确保信息系统安全。针对融媒体中心信息系统，从物理安全、网络安全、主机安全、应用安全、数据安全等方面，制定具体的安全策略。

5.1.2 安全策略执行

按照安全策略要求，对融媒体中心信息系统进行安全配置、安全加固、安全监控等工作。建立健全安全事件应急响应机制，对发生的安全事件进行及时、有效的处理。定期对安全策略执行情况进行审计和评估，确保安全策略得到有效执行。根据安全形势变化、信息系统更新换代等因素，对安全策略进行调整和优化。为安全策略执行提供必要的技术支持，确保安全策略得到有效落实。对违反安全策略的行为，依法依规追究相关责任。

5.2 安全培训与教育

融媒体中心网络安全及信息安全一体化架构的运行与管理中，安全培训与教育是至关重要的环节。应提升全员网络安全意识，增强网络安全防范能力；培养专业网络安全人才，提高融媒体中心整体网络安全水平；加强信息安全教育，确保融媒体中心信息安全稳定运行。网络安全基础知识培训中，讲解网络安全基本概念、安全威胁类型、常见网络安全漏洞等；信息安全法律法规培训中，解读《中华人民共和国网络安全法》《中华人民共和国数据安全法》等相关法律法规；安全技术与管理培训中，介绍网络安全防护技术、信息安全管理规范、应急预案等； 实战演练培训中，通过案例分析、应急演练等形式，提高员工应对网络安全事件的能力；信息安全意识养成培训中，培养员工在日常工作中的安全操作习惯，降低安全风险。

5.3 应急响应与处置

融媒体中心应建立完善的网络安全及信息安全应急响应机制，明确应急响应的组织架构、职责分工、响应流程等，确保在发生网络安全事件时能够迅速、有效地进行处置。针对可能出现的网络安全事件，融媒体中心应制定详细的应急预案，包括事件分级、处置流程、资源调配、信息通报等内容，确保在突发事件发生时能够有序应对。应急响应队伍应密切关注网络安全状况，及时发现和处理网络安全事件，包括但不限于恶意攻击、数据泄露、系统瘫痪等。在发生网络安全事件时，融媒体中心应立即启动信息通报机制，向相关部门、上级单位、用户等通报事件情况，确保信息畅通。在事件处置过程中，应急响应队伍应进行全面调查和分析，查找事件原因，评估事件影响，为后续的防范措施提供依据。在事件得到有效控制后，融媒体中心应组织力量进行系统恢复和重建，确保业务正常运行。针对应急响应过程中的不足，融媒体中心应不断优化应急响应机制，提高应急处置能力，确保网络安全及信息安全一体化架构的稳定运行。

6 结论

融媒体中心网络安全及信息安全面临诸多挑战，包括网络攻击、数据泄露、恶意软件等。网络安全及信息安全一体化架构是解决融媒体中心安全问题的有效途径。融媒体中心网络安全及信息安全一体化架构应具备全面性、协同性、动态性、适应性等特点。通过构建一体化架构，可以有效提升融媒体中心的网络安全及信息安全水平，保障融媒体中心的正常运营。本文的研究成果为融媒体中心网络安全及信息安全一体化架构的设计提供了理论依据和实践指导，有助于推动融媒体中心安全稳定发展。

参考文献

[1] 魏伟.融媒体建设中的网络信息安全研究[J].电声技术,2022,46(08):39-41.

[2] 陈绍华.如何做好融媒体中心网络安全防护工作[J].西部广播电视,2022,43(06):238-240.

[3] 陈维华.浅谈县级融媒体平台的信息安全建设[J].新闻传播,2021(20):117-118.

[4] 陈维华.融媒体建设中网络信息安全规范实务[J].西部广播电视,2021,42(14):232-234.

[5] 马爽.融媒体中心共享安全体系规划设计[J].广播电视网络,2021,28(02):64-68.