广播电视行业网络安全现状与安全防范研究

郑海亮
阿克苏地区融媒体中心　新疆　阿克苏　843000

摘　要：广播电视行业作为信息传播的重要载体，其网络安全现状备受关注。随着信息技术飞速发展，广播电视行业面临日益复杂的网络威胁，包括黑客攻击、数据泄露、恶意软件传播等。本文深入分析当前广播电视行业的网络安全现状，并探讨有效的安全防范技术和管理体系构建策略。通过加强网络安全管理制度建设、提升技术防护能力、强化人员安全意识等措施，旨在提高广播电视行业的网络安全防护水平，确保信息传播的安全与稳定。

关键词：广播电视行业；网络安全；安全防范

1 广播电视行业网络安全概述

广播电视行业作为信息传播的重要渠道，其网络安全问题日益受到关注。随着电信、互联网、广播电视行业的深度融合以及手机客户端的飞速发展，新一代信息传输面临着新的风险和挑战。广播电视行业网络安全不仅关乎信息的正常传输和储存，更直接关系到国家安全、社会稳定以及广大用户的切身利益，其在网络安全方面主要面临以下几类风险：一是内部风险，由于人员操作失误或错误使用，可能导致系统存在安全漏洞；二是互动风险，随着信息技术的发展，广播电视节目通过手机客户端等渠道与观众的互动日益增多，这种交互如果缺少安全防范，可能使外界恶意代码进入系统；三是软件风险，当前网络黑客技术多样化，如果广播电视系统安全防护软件不能及时升级，将增大安全风险；四是身份验证风险，黑客可能通过破解密码或利用其他手段获取未授权访问权限；五是数据泄露风险，广播电视传输业中产生的大量数据可能包含用户个人信息和商业机密等敏感数据，一旦泄露将造成严重后果；六是内容侵权风险，未经授权的内容复制和传播可能侵犯版权持有者的权益。为了应对这些风险，广播电视行业采取了多项措施[1]。首先，成立广电网络和信息安全管理机构，对广播电视网络的工作进行正确规划，制定统一的标准，明确分工，推动行业内自我纠正。其次，加强身份验证措施，除了传统的用户名和密码组合外，引入双因素身份验证等技术。另外，采用加密技术对数据进行保护，限制访问权限，并建立严格的数据审计机制。同时，可采用数字水印技术对内容进行标记，以便追踪和验证，防止内容侵权。在技术手段上，积极采用先进的网络安全技术，如人工智能、深度学习等，提升系统安全防护能力。此外，应加强对技术人员的安全意识和技能培训，确保能够及时应对各种网络安全威胁。

2 当前广播电视行业网络安全存在的主要问题

2.1 技术层面的挑战

在广播电视网络中，部分设备厂商设计和生产设备时，未能充分考虑网络安全性能。这些设备可能存在硬件漏洞、软件后门或弱口令等安全隐患，易受恶意攻击和入侵。一旦设备被攻破，攻击者可以获取广播电视网络的控制权，进而实施数据窃取、篡改节目内容等恶意行为。广播电视行业使用的软件种类繁多，包括操作系统、应用软件、驱动程序等。这些软件在开发过程中可能存在编码错误、逻辑漏洞等问题，为攻击者提供了可乘之机。攻击者可以利用漏洞执行恶意代码、提升权限或绕过安全控制，对广播电视网络正常运行构成严重威胁。随着算力不断提升，传统加密技术面临着被破解风险。如果广播电视行业未能及时采用先进的加密技术，传输的数据和存储的信息可能面临泄露风险，加密算法的实现错误或配置不当也可能导致安全漏洞。随着5G、物联网、人工智能等新技术在广播电视行业的应用，新的安全风险也随之产生。

2.2 管理层面的不足

一是从业人员在信息安全意识上存在差距，对于网络安全的重要性认识不足。可能缺乏基本的网络安全知识和技能，无法有效识别和防范网络威胁。这种安全意识的缺乏导致安全策略执行不力，甚至成为网络攻击目标。二是在网络安全策略制定和执行上存在不足，缺乏全面安全管理体系，未能根据业务需求和风险评估结果制定相应安全策略。这导致安全控制措施的实施缺乏针对性和有效性，无法有效抵御各种网络攻击[2]。三是安全播出监控系统可能存在不完善或运行不正常情况，可能无法准确、及时地发现和应对各种安全事件和威胁。四是面对网络攻击或安全事件时，可能缺乏有效的应急响应机制。这包括缺失应急响应计划、应急响应团队不足

以及流程不明确等问题。这些不足可能导致安全事件无法得到及时有效地处理，进而引发更大的损失和影响。

3 广播电视行业网络安全防范技术研究

3.1 传统网络安全技术在广播电视行业的应用

在广播电视行业的网络安全防范中，传统技术发挥着举足轻重的作用。防火墙技术作为第一道防线，被广泛部署在广播电视网络的关键节点，通过设定访问控制策略，有效阻挡了来自外部网络的非法入侵和恶意攻击。防火墙监控和过滤进出网络数据包，确保数据经过授权才能通行，从而保护内部资源和数据安全。除了防火墙，入侵检测与防御系统（IDS/IPS）也是常用网络安全技术。它能够实时监测网络中的异常行为和可疑活动，发现潜在威胁立即告警并采取相应防御措施。IDS/IPS系统通过深入分析网络流量和数据包，能识别出如DDoS攻击、SQL注入、恶意软件传播等多种类型的攻击，为广播电视网络提供威胁检测和防御。通过对敏感数据加密处理也是广播电视行业保障数据安全的重要手段，广播电视行业通常采用的加密技术包括对称加密和非对称加密，在适当的时候，还可以采用国密算法，提升数据安全性，这些技术能够确保数据的机密性和完整性，有效防止数据泄露和篡改风险。身份认证与访问控制技术也是被广泛应用的网络安全技术。通过要求用户提供如用户名和密码、数字证书等有效的身份凭证，系统能够验证用户身份并确保仅合法用户能访问特定资源和数据。这种技术有效防止了未经授权的访问和滥用，保护了广播电视系统的安全性和稳定性。

3.2 新兴网络安全技术在广播电视行业的探索

随着网络技术不断发展，广播电视行业也开始探索和广泛应用新兴网络安全技术。人工智能与机器学习技术通过训练模型来识别和预测网络攻击行为，为广播电视行业提供了更加智能和高效的威胁检测和防御手段。区块链技术也在广播电视行业的网络安全防范中展现了巨大潜力，通过利用区块链的不可篡改性和透明性特点，可以构建更加安全和可信的数据传输和存储机制[3]，确保广播电视行业的数据完整性和真实性，防止数据被篡改或伪造，提高数据安全性和可靠性。零信任网络技术，代表了新一代网络安全防护理念，打破了传统网络边界概念，认为网络内部和外部都存在潜在安全威胁，要求对所有访问请求进行严格的身份验证和授权检查，确保只有合法用户才能访问特定资源和数据。这种技术能有效防止内部泄露和横向移动攻击风险，为广播电视行业提供更全面和细致的安全防护。另外，应用网络安全态势感知系统也能提前预警，有效预防网络攻击，降低系统风险。

3.3 安全防范技术的融合与创新

在广播电视行业的网络安全防范中，单一技术手段往往难以应对复杂多变的网络威胁。安全防范技术的融合与创新成为了必然趋势。通过将传统网络安全技术与新兴网络安全技术结合，可以构建全面、智能和高效的安全防护体系。例如，将防火墙、IDS/IPS等传统技术与网络安全态势感知、人工智能、机器学习等新兴技术相融合，实现智能化威胁检测和防御。通过训练模型识别和预测网络攻击行为，并结合传统访问控制策略，更准确地阻挡和应对各种攻击。同时还可以利用区块链技术进一步提高数据的安全性。另外，还可以积极探索应用基于行为的身份验证技术、量子加密技术等新的安全防范技术和方法。新技术独特的安全特性和优势，可以为广播电视行业提供更加先进和可靠的安全防护手段，通过安全防范技术的融合和与创新，不断提升自身的网络安全水平，确保广播电视节目安全传输和播出。

4 广播电视行业网络安全管理体系构建

4.1 网络安全管理制度与标准建设

为了确保广播电视网络安全稳定运行，必须有一套完善、可行的网络安全管理制度。这些制度应涵盖网络访问控制、数据保护、设备管理、系统维护、用户行为规范等方面。通过明确各项安全要求和操作流程，有效地规范网络使用行为，降低安全风险。伴随新媒体产业的兴起和深度融合，国家制定了一系列关于融媒体中心建设的标准体系，根据《推进地市级媒体加快深度融合发展实施方案》(中宣发〔2022〕14号）的安排部署，中央宣传部和国家广播电视总局组织编制了《市级融媒体中心总体技术规范》《市级融媒体中心数据规范》《市级融媒体中心接口规范》《市级融媒体中心网络安全防护基本要求》《市级融媒体中心技术系统合规性评估方法》5项技术标准规范，并于2023年2月1日发布。广播电视行业为应对变革也积极参与融媒体中心建设，为应对风险，应积极参与国家和行业网络安全标准的制定工作，结合行业特点和实际需求，推动适用于广播电视行业的网络安全标准体系进一步完善。这些标准包括网络安全技术标准、管理标准、评估标准等，为广播电视行业的网络安全工作提供有力的支撑和指导。通过遵循这些标准，可以确保广播电视网络的合规性，提高网络安全防护水平。在具体实施过程中，广播电视机构应根据相关国家标准，建立健全网络安全管理制度执行机制。通过定期审查、更新和完善制度，确保与时俱进适应网络安全发展的新形势。还应加强对制度执行情况的监督

检查，确保各项制度得到有效落实。对于违反制度的行为，应依法依规进行严肃处理，维护网络安全的严肃性和权威性。

4.2 网络安全组织架构与职责划分

广播电视机构应设立专门的网络安全管理部门或岗位，负责网络安全管理工作。这个部门或岗位应具备相应的权力和资源，能够协调各方力量，共同应对网络安全威胁。在组织架构中，应明确各级网络安全管理人员的职责和权限。从高层管理者到一线员工，每个人都应清楚自己在网络安全工作中的角色和责任。高层管理者应负责制定网络安全战略和规划，为网络安全工作提供足够的支持和资源。网络安全管理部门或岗位则负责制定具体的网络安全政策和措施，组织实施网络安全培训和演练，监督网络安全制度的执行情况等。一线员工则应遵守网络安全制度，规范自己的网络使用行为，积极参与网络安全工作。广播电视机构还应建立跨部门、跨地区的网络安全协作机制，通过加强与相关部门和机构的沟通与合作，共同应对网络安全威胁和挑战。这种协作机制可以促进信息共享、资源互补和优势互补，提高网络安全工作的整体效能。

4.3 网络安全培训与意识提升

广播电视机构应定期组织网络安全培训，邀请专家学者或业内人士为员工讲解网络安全知识、技能和实践经验。通过培训，使员工了解网络安全重要性，掌握基本的网络安全防护技能和方法。同时广播电视机构还应注重培养员工网络安全意识。通过宣传教育、案例分析等方式，使员工深刻认识网络安全威胁的严重性和危害性，增强自我保护意识和能力。员工应自觉遵守网络安全制度，规范使用网络，不泄露敏感信息，不随意下载和安装未知来源的软件或插件等[4]。广播电视机构还应鼓励员工积极参与网络安全演练和实践，通过模拟真实的网络安全事件和场景，让员工亲身体验和应对网络安全威胁。这些实践活动可以提高员工的应急响应能力和实际操作技能，为应对真实网络安全事件做好充分准备。

4.4 网络安全应急响应与恢复机制

在广播电视行业，网络安全事件时有发生，因此建立健全网络安全应急响应与恢复机制至关重要。广播电视机构应制定详细的网络安全应急预案，明确应急响应流程、步骤和责任人。预案应包括网络安全事件的发现、报告、分析、处置和恢复等各环节，确保在发生网络安全事件时能迅速、有效地应对。广播电视机构还应建立网络安全应急响应团队或专家库，这个团队或专家库应具备相应专业知识和技能，能迅速响应和处理网络安全事件。在发生网络安全事件时，应立即启动应急预案，组织相关人员进行现场处置和调查分析，及时控制事态发展并消除安全隐患。此外还应注重网络安全事件的恢复工作，在网络安全事件得到控制后，应及时对受损系统和设备进行修复和恢复，确保广播电视网络正常运行。最后对网络安全事件进行总结和分析，找出问题根源和教训，为今后的网络安全工作提供借鉴和参考。

结束语

广播电视行业网络安全是一个持续演进的过程，需要不断适应新技术、新威胁的挑战。通过本文的研究，期望能够为广播电视行业提供一套全面、可行的网络安全防范方案。未来，随着技术的不断进步和管理的不断完善，相信广播电视行业将能够构建起更加坚固的网络安全防线，为信息传播的安全与稳定提供有力保障。

参考文献

[1]郭沛宇.广播电视行业商用密码应用实践[J].中国信息安全，2021，（08）：54-56.

[2]马玉红.广播电视与视听新媒体行业网络安全监管探讨[J].传媒论坛，2021，4（13）：10-11.

[3]蔡岛.广播音频制播网络系统的技术安全维护探析[J].视界观,2021,000(002):P.1-1.

[4]余德骏.广播电视台网络数据的安全传输研究[J].网络安全技术与应用,2022,(03):102-103.