广播电视台播出系统网络安全建设方案设计

韩国庆
内蒙古自治区广播电视传输发射中心乌兰浩特825台　内蒙古　乌兰浩特　137400

摘　要：随着数字化浪潮推进，广播电视台播出系统网络安全面临诸多挑战。本文聚焦广播电视台播出系统网络安全建设，阐述其重要性，包括保障节目安全播出、保护数据安全及维护行业声誉。分析系统面临的外部攻击、内部管理漏洞、技术更新快、合规性要求提高及应急响应能力不足等挑战。基于此，提出构建多层次防御体系、加强内部安全管理、定期更新安全技术、建立合规性管理体系及提升应急响应能力等网络安全建设方案，旨在为广播电视台播出系统网络安全提供有效策略，确保其稳定、安全运行。

关键词：广播电视台；播出系统；网络安全；建设方案

引言：在数字化浪潮席卷下，广播电视台播出系统高度依赖网络技术，实现节目制作、传输与播出的高效运作。然而，网络环境复杂多变，播出系统面临诸多安全威胁。一旦遭受攻击，不仅会导致节目播出中断，影响观众收看体验，还可能造成数据泄露，损害广播电视台的核心利益与行业声誉。同时，随着法规政策不断完善，对播出系统网络安全合规性要求日益严格。因此，加强广播电视台播出系统网络安全建设迫在眉睫，是保障业务正常开展、提升行业竞争力的关键所在。

1 广播电视台播出系统网络安全的重要性

1.1 保障节目安全播出

广播电视台的节目播出是核心业务，网络安全是节目稳定播出的基石。播出系统一旦遭受网络攻击，如恶意软件入侵、DDoS攻击等，可能导致信号中断、画面失真、声音异常等问题，严重影响节目正常播出。这不仅会让观众收看体验大打折扣，还可能造成重大播出事故。尤其是在重要时段、重大活动的直播中，播出中断会引发广泛关注和不良影响。所以，确保播出系统网络安全，能有效抵御各类攻击，保障节目按时、准确、高质量播出，满足观众的收视需求。

1.2 保护数据安全

广播电视台播出系统存储着大量重要数据，包括节目素材、编排信息、用户数据等。这些数据具有极高的价值，一旦泄露或被篡改，将带来严重后果。节目素材泄露可能被竞争对手利用，造成版权纠纷和经济损失；编排信息泄露会打乱播出计划，影响节目正常流程；用户数据泄露则侵犯了观众隐私，引发信任危机。通过加强网络安全建设，采用数据加密、访问控制等技术手段，能有效保护数据不被非法获取、篡改或破坏，确保数据的完整性、保密性和可用性[1]。

1.3 维护行业声誉

广播电视台作为重要的文化传播机构，其行业声誉至关重要。播出系统的网络安全状况直接影响着公众对广播电视台的信任和评价。若频繁出现网络安全问题，如播出事故、数据泄露等，会让观众对广播电视台的技术能力和管理水平产生质疑，降低其在观众心中的形象和地位。相反，拥有健全的网络安全体系，能够稳定、安全地播出节目，保护好数据和用户权益，会赢得观众的信赖和好评，提升行业声誉，增强在市场中的竞争力，为广播电视台的长期发展奠定坚实基础。

2 广播电视台播出系统网络安全面临的挑战

2.1 外部攻击威胁

广播电视台播出系统在网络环境中暴露，成为众多外部攻击者的目标。黑客可能利用系统漏洞发起恶意攻击，如DDoS攻击，通过大量请求使系统服务器瘫痪，导致节目播出中断。恶意软件也常伺机而动，像病毒、木马等，一旦入侵系统，可窃取或篡改节目数据、编排信息等关键内容。此外，网络诈骗手段不断翻新，攻击者可能伪装成合法用户或合作伙伴，骗取系统访问权限。而且，随着网络技术的发展，攻击手段日益复杂和隐蔽，传统的防御机制难以有效应对，使得播出系统时刻面临外部攻击的严峻威胁，安全形势愈发严峻。

2.2 内部管理漏洞

广播电视台内部人员众多，管理环节复杂，易出现安全漏洞。部分员工安全意识淡薄，随意在不可信的网络环境中操作，或使用弱密码，增加了系统被攻击的风险。权限管理不善也是一大问题，一些员工可能拥有超出其工作范围的过高权限，一旦其账号被盗用或恶意利用，将对系统造成严重破坏。同时，内部数据流转缺乏有效监管，数据在传输和存储过程中可能被泄露或篡

改。此外，内部安全管理制度执行不到位，对违规行为的处罚力度不够，难以形成有效的约束机制，给播出系统网络安全带来潜在隐患。

2.3 技术更新迭代快

网络技术发展日新月异，新的安全威胁和攻击手段不断涌现。广播电视台播出系统所依赖的硬件设备和软件系统需要紧跟技术发展步伐进行更新升级。然而，新技术的引入往往伴随着新的安全风险，例如新的操作系统、应用软件可能存在未知漏洞，给攻击者可乘之机。而且，技术更新速度快，安全防护技术难以迅速跟上，导致系统在一段时间内处于安全防护的薄弱期。此外，不同设备和软件之间的兼容性问题也可能引发安全漏洞，使得播出系统在技术快速迭代的环境下，面临着日益复杂和严峻的网络安全挑战。

2.4 合规性要求提高

广播电视台播出系统网络安全正面临合规性要求提高的严峻挑战。随着行业对播出安全重视程度的不断加深，一系列涵盖播出流程各环节的严格安全准则应运而生。从节目素材的存储加密，到播出信号的稳定传输，再到应急响应机制的完备性，都有细致规范。播出系统需全面适配这些要求，进行软硬件升级与流程优化。然而，行业安全标准处于动态变化中，持续更新迭代，若不能及时跟进调整，系统易出现安全短板，给播出安全带来极大隐患[2]。

2.5 应急响应能力不足

当广播电视台播出系统遭遇网络安全事件时，快速有效的应急响应至关重要。但目前很多广播电视台在这方面存在明显不足。一方面，缺乏完善的应急预案，对于不同类型的网络安全事件，没有明确的应对流程和责任分工，导致事件发生时各部门之间协调困难，响应效率低下。另一方面，应急响应团队的专业能力有待提升，缺乏应对复杂网络安全事件的经验和技能，难以迅速准确地判断事件性质和影响范围，并采取有效的处置措施。

3 广播电视台播出系统网络安全建设方案设计

3.1 构建多层次防御体系

广播电视台播出系统构建多层次防御体系，需从多方面协同推进，以全方位保障网络安全。(1)强化网络边界防护。在网络进出口位置部署专业的防火墙设备，依据精细设定的规则，严格筛选进出流量，阻挡外部非法访问与恶意攻击，为播出系统构建起坚实的第一道屏障。同时，搭配入侵检测与防御系统，实时监测网络中的异常行为，对潜在威胁迅速做出反应，实现动态防护。(2)注重内部网络隔离。依据业务功能和安全需求，将内部网络划分为多个逻辑区域，通过访问控制技术，限制不同区域间的随意访问，防止攻击者在内部网络中横向扩散，降低安全风险。对关键业务区域，采用更严格的隔离措施，确保核心数据和业务的安全。(3)提升主机安全防护水平。为播出系统的各类主机设备安装可靠的杀毒软件和主机安全防护软件，定期进行病毒查杀和系统漏洞修复，及时消除安全隐患。同时，实施严格的身份认证和访问管理机制，采用多因素认证方式，确保只有授权人员能够访问主机资源，保障主机系统的安全稳定运行。

3.2 加强内部安全管理

广播电视台播出系统要实现稳固的网络安全，加强内部安全管理至关重要，可从以下方面着手。(1)提升员工安全意识。定期组织网络安全培训活动，内容涵盖常见网络攻击手段、数据保护要点以及安全操作规范等。通过培训，让员工深刻认识到网络安全的重要性，使其在日常工作中自觉遵守安全规定，不随意点击不明链接、不使用弱密码，从源头上减少因人为疏忽引发的安全风险。(2)优化权限管理机制。对播出系统内的各类账号权限进行细致梳理，依据员工的工作职责和实际需求，精准分配访问权限。避免出现权限过度分配的情况，防止员工因误操作或恶意行为对系统造成破坏。同时，建立权限审批流程，任何权限的变更都需经过严格审核，确保权限管理的规范性和严肃性。(3)强化内部监督审计。部署专业的审计系统，对播出系统的操作行为进行实时记录和审计。定期对审计日志进行分析，及时发现异常操作和潜在的安全隐患。一旦发现问题，迅速启动调查程序，追究相关人员责任，以此形成有效的威慑力，促使员工严格遵守内部安全管理制度，保障播出系统的安全运行。

3.3 定期更新安全技术

广播电视台播出系统所处网络环境复杂多变，定期更新安全技术是维持系统安全性的必要举措，具体可从以下方面开展。(1)及时更新安全防护软件。杀毒软件、防火墙等是抵御外部攻击的基础防线，其病毒库和防护规则需紧跟安全形势变化。定期升级这些软件，能让它们识别和拦截最新出现的病毒、恶意软件及网络攻击手段，有效阻挡外部威胁入侵播出系统，保障系统的基础安全。(2)跟进系统与设备固件更新。播出系统依赖的操作系统、服务器固件等若存在漏洞，易被攻击者利用。厂商会不断发布更新补丁来修复这些漏洞，定期为系统和设备安装更新，可填补安全漏洞，增强系统自身的安

全性和稳定性，降低被攻击的风险。(3)引入新兴安全技术。随着网络安全领域不断发展，如人工智能安全检测、零信任架构等新兴技术不断涌现。定期评估这些新技术对播出系统的适用性，适时引入并整合到现有安全体系中，能够提升系统对新型攻击的防范能力，构建更先进、全面的安全防护网，确保播出系统在复杂网络环境中安全运行[3]。

3.4 建立合规性管理体系

广播电视台播出系统建立合规性管理体系，对保障系统安全稳定运行、提升整体管理水平意义重大，可从以下方面着手构建。(1)明确合规标准与要求。组织专业人员对播出系统涉及的业务流程、技术环节进行全面梳理，结合行业最佳实践和自身安全需求，制定一套涵盖数据管理、访问控制、系统运维等多方面的内部合规标准。这些标准要详细且具有可操作性，为后续的合规管理工作提供清晰指引。(2)开展定期合规评估。成立专门的合规评估小组，按照既定的标准和流程，定期对播出系统进行全面评估。评估内容包括系统安全配置、数据存储与传输、用户权限管理等方面。通过评估及时发现系统存在的合规风险和安全隐患，形成详细的评估报告，为后续的整改工作提供依据。(3)强化合规整改与持续改进。针对评估中发现的问题，制定切实可行的整改计划，明确整改责任人和整改期限，确保问题得到及时有效解决。同时，建立合规性管理的持续改进机制，根据业务发展、技术更新等情况，不断优化内部合规标准和管理流程，使合规性管理体系始终适应播出系统的安全需求。

3.5 提升应急响应能力

广播电视台播出系统面临诸多不可预见的网络安全威胁，提升应急响应能力是保障系统稳定运行、降低损失的关键，可从以下方面着手。(1)制定全面应急预案。组织专业团队，结合播出系统的特点和可能面临的安全风险，制定涵盖网络攻击、设备故障、数据丢失等多种场景的应急预案。预案要详细规划应急处置流程、明确各部门和人员的职责分工，确保在突发事件发生时，能够迅速、有序地开展应对工作，避免出现混乱和延误。(2)组建专业应急团队。选拔具备网络安全、系统运维、数据分析等多方面知识和技能的人员，组成专门的应急响应团队。定期为团队成员开展培训和演练活动，提升他们对各类安全事件的识别、分析和处置能力，使其熟悉应急预案流程，能够在实战中快速、准确地采取应对措施。(3)完善应急资源保障。储备必要的应急物资和设备，如备用服务器、网络设备、数据备份介质等，确保在紧急情况下能够及时替换受损设备，恢复系统运行。同时，建立与外部技术支持机构的合作机制，在遇到复杂安全事件时，能够迅速获得专业的技术支持和援助，提升应急响应的效率和效果[4]。

结束语

广播电视台播出系统网络安全建设是一项长期且艰巨的任务，关乎节目安全播出、数据安全保护以及行业声誉维护。通过构建多层次防御体系，能筑牢外部攻击的防线；加强内部安全管理，可杜绝人为因素引发的安全隐患；定期更新安全技术，能紧跟安全形势变化；建立合规性管理体系，确保系统运行符合安全规范；提升应急响应能力，能在突发安全事件时快速止损。只有将这些措施有机融合、协同推进，形成全方位、多层次的网络安全防护网，才能有效应对各类网络安全挑战，保障广播电视台播出系统安全、稳定、可靠运行。

参考文献

[1]郭华.广播电视台网络安全技术的应用研究[J].西部广播电视,2022(23):233-234.

[2]周飞,王亮.试论广播电视网络安全防护技术与实践[J].电视技术,2021,43(19):77-78.

[3]康宇.浅谈广播电视台融媒体网络安全建设[J].中国新通信,2022,21(18):140.

[4]杨卫中.广播电视台综合网络的安全防范措施[J].西部广播电视,2022(05):255.