

广播电视网络安全防护技术

丽娜·吾兰

阿勒泰地区融媒体中心 新疆阿勒泰市 836599

【摘要】当前阶段，诸多行业都在与互联网技术紧密融合，网络安全治理乃是数字化转型的关键支撑部分，在广播电视领域当中，信息传输的稳定程度与可靠程度和网络安全构建有着密切关联，而且主流媒体的信誉以及公众信任度相互关联，通过完善网络安全防护技术，构建周密的网络安全防护体系，能够有效提高广播电视系统的安全防护水准和风险防御能力。

【关键词】广播电视；网络安全；防护技术

Broadcasting network security protection technology

Lina Wu Lan

Altay Regional Media Fusion Center Altay City, Xinjiang 836599

【Abstract】In the current stage, many industries are closely integrating with Internet technology.Cybersecurity governance is a critical component of digital transformation.In the broadcasting and television sector, the stability and reliability of information transmission are closely linked to the construction of cybersecurity systems.This is also related to the credibility of mainstream media and public trust.By enhancing cybersecurity protection technologies and establishing a comprehensive cybersecurity framework, the security protection level and risk defense capabilities of the broadcasting and television system can be significantly improved.

【Key words】radio and television; network security; protection technology

伴随着互联网技术在各领域的普遍运用，广播电视行业正经历一场深刻的数字化蜕变，在这一进程里，网络安全已成为维持行业稳定发展的重要支柱，倘若网络安全问题产生，不仅会让广播电视系统的数据安全面临威胁，还将降低它在公众心里的可信度，极大破坏行业的社会形象及长远规划，网络安全防护体系充当广播电视行业抵御风险的核心屏障，其技术水平直接关系到安全防护的实际绩效，只有不断提升防护技术水平，改进安全防护体系，才能真正保证广播电视系统顺利运行，促进该行业达成高质量发展。

一、广播电视行业网络安全现状

我国广播电视行业网络安全建设进程显得相对缓慢，在防护体系范畴存在明显短板。早期建设中，行业普遍采用如物理隔离这样的传统安全策略，系统架构也多以封闭技术体系为基础进行改造，不能适应互联网环境下复杂多样的安全需求。随着业务的拓展，各单位借助局域网实现了彼此联通，但网络边界防护措施显得松散，安全设备的配备欠缺，埋下安全隐患。设备老化和软件维护跟不上也是突出问题，部分专用设备长时间使用后出现性能降低，应用软件更新滞后，造成系统漏洞不断冒出等问题。行业内普遍存在专业人才短

缺、管理制度有缺陷的现象，一些从事该行业的人员安全意识薄弱，在系统建设期间往往更聚焦功能实现，忽略安全保障工作，造成重要节点安全责任的区分不明确，网络安全等级保护制度流于形式，部分部门评估区域网络安全风险的水平有限，在指导监督工作里欠缺统筹规划及协同推进，这些因素共同制约了广播电视行业网络安全防护能力的提升。

二、广播电视网络安全的重要性

当前数字化融合的浪潮快速兴起且发展态势强劲，广播电视网络作为信息基础设施的关键构成部分，承载着大量民众的个人资料以及企业的关键数据，它的稳定性对于我国数字主权以及社会经济稳定基础有着直接影响，一旦这些核心资料借助非法途径被窃取或泄露，将会导致个人隐私遭受极大损失，企业资产出现重大流失，并且发生信任危机的风险也会比较高，引发数字经济产业链以及公众舆论生态的一系列连锁反应。

伴随 5G 网络切片技术与物联网泛在接入能力深度结合，广播电视网络正快速向“云网端”一体化架构迈进，此种异构网络的融合趋势在增强业务创新效率的同时，也明显扩大了攻击的暴露范围，若广播电视网络安全防护体系未实

现同步升级,对其基础设施的攻击或许借助横向移动效应影响到电力、交通、金融等关键领域,形成跨行业风险传导链路,此类复合型安全威胁不仅会干扰数字经济运行的正常秩序,更大概率引发社会的恐慌情形,对国家治理能力现代化进程形成实质性阻碍,构建契合全媒体传播格局的新型广播电视网络安全体系,已成为国家网络安全战略的核心命题。

三、广播电视网络安全防护技术具体使用情况

(一) 网络安全防护技术

网络安全体系的搭建涉及网络结构、网络设备及安全设备三个核心部分,其中网络结构充当网络安全的基石,其设计质量直接决定着整体安全防护的水平。对网络结构进行科学规划可从多维度展开,第一,应按照层次化设计原则,构造严密的防护体系格局,实现内部网络与外部网络的有效分离。以广播电视单位为例,需把播出系统、整备系统等核心业务系统与外部网络做物理分离,采用有线传输方式组建内部专用网络,避开无线组网形成的安全风险,在开展与外部的业务交互时,譬如跟听众互动或者接入融媒体中心期间,要进一步强化网络边界防护,一并采用防火墙、网闸等安全设备筑起防护屏障,保障业务开展进程里的网络安全。第二,网络设备性能配置也是网络结构设计的关键要点,为了让业务高峰期系统实现稳定运行,网络设备选型要把峰值业务需求作为基准,保证其拥有充沛的业务承载能力,避免因设备性能不足导致服务中断,就核心交换机、汇聚交换机等关键系统设备而言,需创建完备的冗余备份机制。处于广播电视业务场景当中,建议铺设双通信链路,进而对核心网络设备采取热备份举措,从而在设备故障出现时达成无缝切换,保障业务流程不停歇运转。第三,从安全管理的层面看,应增强对网络设备用户权限的管理工作,依靠身份验证机制提升访问的安全水平,同时把设备日志审计功能开启,对系统运行数据进行完整记录存储,杜绝数据产生丢失现象,针对登录失败、超时等异常情形,制定相应的处理举措,及时截断潜在的安全威胁,全面增强网络结构的安全防护水平。

(二) 边界安全防护技术

边界安全的核心是借助有效的网络隔离保障内部系统的安全,其工作的重点主要有维护边界完整度、防御外部入侵以及阻止恶意代码蔓延等方面,在涉及边界完整性维护的范畴内,需着重对未获授权的设备接入及违规外联情况加以监测,此类安全检测一般称作非法内外联监控。实施进程里可借助合理配置网络协议参数,进而部署专业的管理系统以实现有效管控,针对外部网络的攻击举动,建议采用多层面的防御体系,涵盖设置防火墙和入侵检测系统等相关安全设备,在恶意代码防护方面,要部署专业的防病毒网关,同时

应留意区分网络级和主机级恶意代码防护产品功能的差异,采购过程中必须选择具备正规资质的供应商来保障产品质量。当前边界防护需要重点关注动态隔离技术的应用,通过软件定义网络实现安全域的动态划分,同时加强网络准入控制体系的建设,对各类接入设备实施严格的身份认证和权限管理。在防护策略上应当采用分层防御机制,结合流量监测和行为分析技术,构建覆盖网络边界全环节的立体防护体系。特别需要强化对新型网络攻击特征的识别能力,建立适应融媒体业务特点的边界访问控制模型。

(三) 服务端安全防护技术

执行服务端安全防护措施时,服务器以及数据库的安全保障是重点,实施安全防护策略、身份验证和访问控制等核心技术相当关键,探索身份验证及权限控制的安全领域,服务器和网络端在安全需求方面一致性较为明显,双方需要在登录管理、权限设定、日志审查等多个层面构建完善的安全防线。对于光驱、USB等外部设备的使用权限要执行严格规范管理,禁止接入所有未经批准的外部设备,执行主机系统的安全维护流程,涉及播出和整备的核心业务环节,构建一套规范的系统更新步骤很关键,在系统维护阶段或者版本升级期间,对模拟环境进行全面审查,开展风险预分析,降低系统更新可能引发的风险点,鉴于主机与网络环境面临的恶意软件挑战,要采用多层次的防护方法。综合运用不同产品的功能优势,形成综合性安全防护模式,提高整体防护能力,执行资源访问控制步骤,对用户登录实施严格管理程序,明确划分登录设备权限和访问权限界限,执行严格权限管理方案,对登录环节进行细致监督,保证服务端资源没有安全风险。服务端防护应当建立纵深防御体系,从硬件安全、虚拟化防护、操作系统加固到应用安全实现多层次保护。重点加强系统漏洞的闭环管理机制,完善补丁更新和配置加固流程。对于关键业务系统,需要实施最小权限原则和职责分离机制,同时加强服务间通信的安全管控,建立完善的审计追踪体系。要特别关注容器化部署环境下的安全隔离需求,防范潜在的逃逸风险。

(四) 终端安全与应用安全防护技术

在网络安全架构范畴当中,终端安全所处位置并非核心,然而却关联着众多应用场景以及潜在的安全问题,其所蕴含的风险不可轻视,为了可有效地抵御这些风险,可以依靠部署有集中管控能力的安全防护软件,搭建起覆盖终端设备的防护体系,达成对终端安全状况的统一监控以及风险处理,保证终端设备在复杂的网络环境里安全运行。应用安全防护主要聚焦于系统内软件应用的安全维护,除了常规的登录验证、用户权限分配等基础防护举措之外,在与外部系统进行交互的时候,特别需要强化数据保密性和完整性的维护,对于包含敏感信息的文本内容,应当构建过滤机制,达

成实时屏蔽,对应用程序源代码采取加密存储等安全措施,防止代码出现泄露的情况。终端防护需要构建统一的终端安全管理平台,实现安全策略的集中管控和终端状态的实时监控。重点加强移动终端的安全管理,建立设备认证、数据加密和远程擦除等保护机制。应用安全方面应当完善安全开发生命周期管理,加强第三方组件的安全评估,实施严格的代码审计和安全测试。同时要建立应用行为基线,通过运行时保护技术防范内存攻击等新型威胁。

(五) 数据安全与数据备份防护技术

处在网络安全防护体系架构里面,数据在核心位置上极为关键,其安全防护工作主要围绕数据安全以及数据备份这两大关键维度进行,数据安全意在保证信息具备较高的保密性与完整性,通过在数据传输阶段采用加密技术手段,可有力抵御数据泄露、恶意篡改等一系列严峻安全威胁,进而搭建起坚如磐石的数据安全保护屏障。数据备份机制堪称维系业务连续性的核心保障手段,其核心价值在于最大限度降低因数据丢失、毁坏所造成业务中断的潜在风险,在实际工作中,必须精准辨认并针对关键数据节点开展重点备份任务,同时构建起高效的数据恢复体系,以此保证在遭遇数据异常情形时,可以迅速使业务恢复正常开展。数据备份与恢复工作要形成一套严格规范、标准相同的流程体系,并深度整合进应急预案里面,成为其中必不可少的关键要素,为进一步夯实数据备份的可靠性,建议采用异地数据备份策略,以此避开因内网遭到攻击、发生故障等意外情形,引发备份数据同步出现损害的风险,进而构建起覆盖多层面、具备高冗余特性的数据安全防护体系,全方位保证数据的安全可靠。数据安全防护需要建立分类分级保护体系,针对不同敏感级别的数据实施差异化的加密和访问控制策略。重点加强数据流转过程中的安全管控,完善数据脱敏和水印技术的应用。备份系统应当具备防篡改和完整性验证能力,建立备份数据的全生命周期管理机制。同时要定期开展备份恢复演练,验证备份策略的有效性,确保在应急情况下能够快速恢复业务。

(六) 安全管理中心防控技术

安全管理中心在网络安全防护体系里起着核心枢纽的作用,有着全面、综合性的安全管理本领,为网络系统各环

节筑牢可靠的安全防护线,其主要职责有对网络运行状态进行实时监测以及对数据库安全加以严格监管,借助对系统运行数据的实时采集来进行深度分析,可以灵敏识别潜在的安全风险源。该中心肩负着对异常安全事件如实记录并及时预警的重大责任,对审计日志、补丁更新等关键安全要素开展全生命周期的精准管控,作为网络信息系统安全态势直观化呈现的窗口,安全管理中心为安全管理人员给予了关键的数据支撑和科学的决策凭据。凭借对系统运行数据的深度挖掘和智能研判,安全人员得以准确锁定安全问题,进而制定针对性十分显著的防护策略,在构建网络安全防护体系期间,切实发挥安全管理中心的核心作用十分关键,这不仅对提升网络安全防护的整体性与协同度有好处,更可达成对网络安全风险的动态监测及高效管控,由此为网络系统的平稳、可靠运转提供有力支撑。安全管理中心建设应当注重多源安全数据的融合分析,构建统一的安全事件关联分析引擎。重点提升威胁检测的准确性和及时性,建立标准化的安全事件响应流程。同时要加强对安全态势的预测预警能力,通过机器学习等技术手段识别潜在风险。安全管理中心还需与各安全防护系统建立协同联动机制,实现安全策略的统一部署和动态调整。

四、结束语

广播电视网络安全防护为一项系统性工程,其防护体系的搭建需融合多元技术手段,覆盖全流程里的各环节,采用多维度协同机制实现整体防护功用,随着数字技术的迭代升级,网络安全防护的标准与要求不断上扬,这给从业人员的专业素养造成了更高的挑战。处在这样的背景形势里,专业技术人员须持续强化技术学习力度,创新防护办法,主动借助前沿安全技术打造动态防御架构,通过改进网络安全防护体系,不仅可以成功抵御网络安全的威胁,保证广播电视业务稳定开展,还可推动行业核心竞争力的上扬,为广播电视行业的持续发展筑牢安全根基。

参考文献

- [1]达嘎.5G网络环境下广播电视网络安全风险分析[J].广播电视网络, 2025, 32(03): 70-72.
- [2]郑鹭平.广播电视播出系统网络安全高风险项的判定与补偿[J].广播电视信息, 2025, 32(03): 100-102.
- [3]郑修明.广播电视传输网络中的安全防护技术研究[J].电子元器件与信息技术, 2025, 9(01): 163-165+169.
- [4]孔德会.广播电视组播网络分层式安全防护技术研究[J].数字通信世界, 2024, (04): 43-45+66.
- [5]刘洁.广电系统网络安全防护的研究[J].中国有线电视, 2021, (12): 1220-1222.