广电行业信息化进程中关键信息基础设施保护

张　莉
中国广电新疆网络股份有限公司乌鲁木齐市分公司　新疆　乌鲁木齐　830000

摘　要：广电行业信息化进程中，关键信息基础设施保护至关重要。随着技术的不断进步和业务的快速发展，广电行业面临着日益复杂的网络安全威胁。本文探讨了广电行业在信息化进程中关键信息基础设施保护的现状、挑战及策略建议。通过强化技术防护、完善管理体系、提升应急响应能力和推动行业自律与合作等措施，旨在构建全方位、多层次的安全防护体系，确保广电行业关键信息基础设施的安全稳定运行，为行业的可持续发展提供有力保障。

关键词：广电行业；信息化进程；关键信息；设施保护

引言：随着信息技术的迅猛发展，广电行业正加速推进信息化进程，关键信息基础设施作为支撑行业运行的核心要素，其安全性直接关系到广电业务的连续性和用户数据的保护。在信息化进程中，广电行业关键信息基础设施面临着来自内外部的多种安全威胁，保护这些基础设施的安全成为行业亟待解决的问题。本文将从多个角度探讨广电行业关键信息基础设施的保护策略与建议。

1 广电行业关键信息基础设施概述

1.1 关键信息基础设施的定义

关键信息基础设施（Critical Information Infrastructure，CII）是指那些对于国家安全、经济运行、社会稳定以及公众健康至关重要的信息系统和物理设施。这些设施若遭到破坏、丧失功能或数据泄露，可能会对国家安全、社会秩序、公共利益或经济稳定造成重大损害。它们通常涉及能源、交通、水利、金融、通信、教育、医疗、广播电视等多个关键领域，是保障国家和社会正常运转的重要基石。

1.2 广电行业关键信息基础设施的特点

广电行业关键信息基础设施具有几个显著特点：第一、高度集成性：广电行业的信息基础设施往往集成了多种技术和系统，包括信号传输、节目制作、内容分发、用户管理等多个环节，形成了一个复杂而庞大的系统。第二、实时性要求高：广播电视节目的播出具有很强的时效性，要求信息基础设施能够实时、准确地传输和处理数据，确保节目信号的连续性和稳定性。第三、安全性至关重要：广电行业涉及大量敏感信息和公众舆论，因此其信息基础设施的安全性至关重要。必须采取有效的安全措施，防止数据泄露、篡改和攻击[1]。第四、覆盖范围广：广电行业的信息基础设施通常覆盖全国甚至全球范围，需要具备良好的网络覆盖能力和传输效率。

1.3 在广电行业中的重要性

关键信息基础设施在广电行业中扮演着举足轻重的角色，其重要性主要体现在几个方面：（1）保障节目播出质量。关键信息基础设施的稳定运行是确保广播电视节目正常播出的基础，直接关系到观众的收视体验和满意度。（2）促进产业升级转型。随着数字化、网络化、智能化技术的发展，广电行业正在经历深刻的变革。关键信息基础设施的建设和升级成为推动产业升级转型的重要力量。（3）提升行业竞争力。通过构建高效、安全、智能的信息基础设施，广电企业能够提升服务质量、降低成本、增强创新能力，从而在激烈的市场竞争中脱颖而出。（4）维护国家安全和社会稳定。广电行业作为重要的信息传播渠道，其关键信息基础设施的安全直接关系到国家安全和社会稳定。加强广电行业关键信息基础设施的安全防护是维护国家利益和社会稳定的必然要求。

2 广电行业信息化进程中关键信息基础设施面临的风险

2.1 外部风险

广电行业信息化进程中，关键信息基础设施面临的外部风险主要包括自然灾害和人为攻击两个方面。自然灾害如雷电、火灾、地震等可能对网络设施造成直接破坏，导致系统瘫痪或数据丢失。而人为攻击则更加复杂多变，包括黑客入侵、病毒传播、恶意代码注入等，这些攻击可能来自境内外敌对势力、不法分子或竞争对手，旨在窃取敏感信息、破坏系统正常运行或制造社会混乱。随着广电行业网络规模的扩大，系统之间的节点互联互通，一旦某个关键节点受到攻击，可能会迅速扩散至整个网络系统，造成重大损失。

2.2 内部风险

内部风险主要源于广电行业内部的管理和操作失误。一方面，由于人员安全意识不足、操作不规范或误操作，可能导致系统出现安全漏洞，为外部攻击者提供可乘之机。例如，员工可能因疏忽大意而泄露系统登录密码、使用弱口令或复用口令，这些行为都可能成为黑客攻击的突破口。另一方面，广电行业内部可能存在安全管理不到位的问题，如缺乏完善的安全管理制度、应急预案和监控机制，导致安全事件发生时无法及时响应和处理。内部员工的不当行为或恶意破坏也可能对关键信息基础设施构成威胁。

2.3 新技术应用带来的风险

随着云计算、大数据、物联网等新技术的广泛应用，广电行业关键信息基础设施面临的风险也在不断增加。云计算技术的引入虽然降低了硬件设施部署成本，提升了用户体验，但也带来了数据控制权减弱、安全措施依赖云服务商、数据泄漏风险增加等问题[2]。大数据技术的应用使得广电行业能够更高效地处理和分析用户数据，但同时也面临着数据隐私泄露和滥用的风险。物联网技术的普及则使得广电系统的边界更加模糊，外部攻击者可能通过物联网设备入侵系统，造成更大的安全威胁。新技术的发展还带来了更多的未知风险和挑战，需要广电行业不断探索和完善安全防护措施。

3 广电行业关键信息基础设施保护存在的问题

3.1 技术防护短板

在广电行业关键信息基础设施的保护中，技术防护短板是一个不容忽视的问题。随着信息技术的飞速发展，黑客攻击手段日益复杂多变，而广电行业的技术防护体系却往往滞后于这些威胁的发展。一方面，部分广电企业的网络安全设备和技术更新不够及时，仍在使用过时或低效的防护手段，难以有效抵御新型网络攻击。例如，防火墙、入侵检测系统等传统安全设备在面对高级持续性威胁（APT）、零日漏洞攻击等新型攻击方式时，往往力不从心。另一方面，随着云计算、大数据等新技术的广泛应用，广电行业的数据量和复杂度大幅增加，但相应的数据加密、访问控制、审计追踪等技术措施却未能跟上，导致数据泄露和滥用风险增加。广电行业在物联网设备的安全防护上也存在明显短板，物联网设备的广泛应用使得系统暴露面扩大，而设备本身的安全防护能力往往较弱，容易被黑客利用作为入侵系统的跳板。

3.2 管理体系缺陷

管理体系缺陷是广电行业关键信息基础设施保护中的另一个关键问题。首先，部分广电企业缺乏完善的网络安全管理制度和流程，导致安全管理存在盲区。其次，广电行业在网络安全人才培养和引进方面也存在不足，导致安全管理人员的技术水平和应急处理能力参差不齐。部分安全管理人员缺乏必要的网络安全知识和实践经验，难以有效应对复杂多变的网络安全威胁。另外，广电行业在跨部门协作和信息共享方面也存在障碍，导致在应对网络安全事件时缺乏统一的指挥和协调机制，影响了应急响应的效率和效果。

3.3 应急响应不足

应急响应不足是广电行业关键信息基础设施保护中的另一个亟待解决的问题。一方面，部分广电企业缺乏完善的应急预案和演练机制，导致在网络安全事件发生时无法迅速、有效地进行应对。应急预案的制定往往缺乏针对性和可操作性，难以适应不同场景下的应急需求；演练机制的缺失则使得安全管理人员缺乏实战经验和应对能力，难以在紧急情况下做出正确的决策和行动。另一方面，广电行业在应急响应资源和技术支持方面也存在不足。部分广电企业在面对大规模网络安全攻击时，缺乏足够的应急响应团队和技术手段进行快速响应和恢复。由于跨部门协作和信息共享机制的缺失，导致在应急响应过程中缺乏统一的指挥和协调，影响了应急响应的效率和效果。这些问题不仅可能导致系统瘫痪和数据丢失等严重后果，还可能对广电行业的声誉和用户体验造成不可估量的损害[3]。

4 广电行业关键信息基础设施保护策略与建议

4.1 强化技术防护体系建设

在广电行业关键信息基础设施保护中，强化技术防护体系建设是首要任务。这要求广电企业紧跟技术发展步伐，不断更新和完善网络安全防护手段，确保系统能够抵御各类网络攻击。广电企业应加大对网络安全技术和设备的投入，引入先进的防火墙、入侵检测系统、数据加密技术等，构建多层次、立体化的安全防护体系。这些技术设备能够有效识别和拦截恶意流量，保护系统免受攻击。广电企业应加强对物联网设备的安全管理，物联网设备的广泛应用使得系统暴露面扩大，因此，必须加强对这些设备的安全认证、访问控制和数据加密等措施，防止黑客利用物联网设备作为入侵系统的跳板。广电企业还应积极采用新技术，如人工智能、机器学习等，提升安全防护的智能化水平。这些新技术能够自动识别和分析网络流量中的异常行为，及时发现并处置潜在的安全威胁。广电企业应建立定期的安全评估和漏洞扫描机制，及时发现并修复系统漏洞，确保系统的安全性和稳定性。还应加强对新技术和新应用的安全评估，

确保在引入新技术和新应用时不会引入新的安全风险。

4.2 完善安全管理体系

完善安全管理体系是保障广电行业关键信息基础设施安全的重要基础。这要求广电企业建立健全的网络安全管理制度和流程，确保安全管理工作有章可循、有据可查。首先，广电企业应制定明确的数据分类和分级保护制度，对不同类型的数据采取不同的保护措施，确保敏感数据得到重点保护。还应建立数据访问控制和审计追踪机制，防止数据被非法访问和滥用。其次，广电企业应加强对网络安全管理人员的培训和教育，提升他们的安全意识和技能水平。通过定期的培训、考核和演练，使安全管理人员能够熟练掌握各种安全防护技术和应急响应流程，提高应对网络安全事件的能力。另外，广电企业还应建立跨部门协作和信息共享机制，加强与其他部门、企业和机构的沟通和合作，共同应对网络安全威胁。通过信息共享和协作，可以及时发现并处置网络安全事件，降低安全风险。最后，广电企业应建立网络安全责任制，明确各级管理人员和员工的网络安全职责和义务。通过责任制的落实，可以确保安全管理工作得到有效执行，提高安全管理水平。

4.3 提升应急响应能力

提升应急响应能力是保障广电行业关键信息基础设施安全的重要手段。这要求广电企业建立完善的应急预案和演练机制，确保在网络安全事件发生时能够迅速、有效地进行应对。广电企业应制定详细的应急预案，明确应急响应的流程、措施和责任分工。预案应涵盖不同类型的网络安全事件，包括黑客攻击、病毒传播、数据泄露等，确保在事件发生时能够迅速启动应急响应流程。广电企业应定期组织应急演练，提高安全管理人员和员工的应急响应能力。通过演练，可以检验应急预案的可行性和有效性，发现存在的问题和不足，及时进行完善和改进。广电企业还应建立应急响应团队和技术支持体系，确保在网络安全事件发生时能够迅速调动资源和技术力量进行处置。应急响应团队应由专业的安全管理人员和技术人员组成，具备快速响应和处置能力[4]。广电企业应加强与相关部门的沟通和协作，建立快速响应和处置机制。在网络安全事件发生时，能够迅速与相关部门取得联系，获取支持和帮助，共同应对网络安全威胁。

4.4 推动行业自律与合作

推动行业自律与合作是保障广电行业关键信息基础设施安全的重要途径。这要求广电企业加强行业内的沟通和协作，共同制定行业标准和规范，提高整个行业的安全防护水平。广电企业应积极参与行业标准和规范的制定工作，推动建立统一的网络安全标准和规范体系。通过标准和规范的制定，可以明确安全防护的要求和措施，提高整个行业的安全防护水平。广电企业应加强与行业内其他企业的沟通和协作，共同应对网络安全威胁。通过信息共享、技术交流和合作研发等方式，可以共同提升安全防护能力，降低安全风险。广电企业还应积极参与行业自律组织的工作，推动建立行业自律机制。通过自律机制的建立，可以规范行业内企业的行为，提高行业的整体形象和信誉度。广电企业应加强与政府、科研机构和社会组织的合作，共同推动网络安全技术的发展和应用。通过合作，可以获取更多的技术支持和资源，提高安全防护的智能化和自动化水平。

结束语

在广电行业信息化快速发展的背景下，关键信息基础设施保护不仅是技术挑战，更是行业责任与使命。通过持续的技术创新、管理优化和应急能力提升，已构建起更加坚固的安全防线。未来，广电行业应继续加强合作，共享安全智慧，共同应对新兴威胁，确保关键信息基础设施的安全稳定运行。让我们携手共进，为广电行业的繁荣发展保驾护航，共创智慧、安全、高效的信息化新时代。

参考文献

[1]顾婷.关于广电行业会计信息化向智能化发展的探讨[J].中国总会计师,2020(10):106-107.DOI:10.3969/j.issn.1672-576X.2020.10.041.

[2]陈超.广电行业内部审计研究[J].财会学习,2023(13):129-131.DOI:10.3969/j.issn.1673-4734.2023.13.046.

[3]欧阳代义,肖子龙.信息化建设背景下广电网络工程项目建设管理机制的研究[J].广播电视网络,2022,29(5):114-116.

[4]张锣亮.浅析广电网络企业信息化建设[J].中国宽带,2020(11):111.