 DOI: https://doi.org/10.12349/iser.v6i5.5684

Analysis and prevention of network security of short wave broadcasting transmitter

Yajing Song

China Radio and Television Administration, 2024 Station, Jiamusi, Heilongjiang, 154025, China

Abstract

With the advent of the digital intelligence era and the advancement of information construction for shortwave broadcasting stations, network technology has been widely applied. While improving efficiency, cybersecurity management faces unprecedented security risks and challenges. This paper introduces the types of cybersecurity threats and preventive measures, as well as analyzes the main issues currently present in the cybersecurity of shortwave radio stations (such as diversified attack methods and insufficient protection capabilities). It combines technical and management strategies (such as firewalls, encryption technologies, and operation and maintenance systems) to explore comprehensive cybersecurity protection solutions under the empowerment of technology. The aim is to provide a reference for cybersecurity management for technical maintenance personnel.

Keywords

radio transmitter, network security, prevention methods, security threats, safety management

短波广播发射台网络安全的分析与防范的研究

宋雅静

国家广播电视总局二〇二四台，中国 · 黑龙江 佳木斯 154025

摘　要

随着数智化时代的到来，短波广播发射台信息化建设的推进，网络技术被大量应用，提升效率的同时，网络安全管理面临着前所未有的安全风险与挑战。本文通过介绍了网络安全威胁的种类和防范方法以及分析当前短波广播电台网络安全的存在的主要问题（如攻击手段多样化、防护能力不足等），结合技术与管理策略（如防火墙、加密技术、运维体系等），探讨技术赋能下的网络安全的综合防护方案，希望能够为技术维护工作者提供网络安全管理参考。

关键词

广播发射台；网络安全；防范方法；安全威胁；安全管理

1 引言

短波广播发射台作为广播传媒行业的重要组成部分，承担着重要的信息传播任务。在数智化时代，随着网络技术的快速发展和广泛应用，短波广播发射台的网络安全问题日益凸显。网络攻击、数据泄露、恶意软件等安全威胁不仅可能破坏广播发射设备的正常运行，还可能对国家信息安全和社会稳定构成严重威胁。因此，加强短波广播发射台的网络安全管理显得尤为重要。

2 短波广播发射台网络安全问题分析

2.1 网络安全威胁多样化

随着网络技术的不断进步，网络攻击手段亦呈现出持续更新和多样化的趋势。具体而言，攻击者利用病毒、木马、蠕虫等恶意软件进行攻击，以及通过网络钓鱼、拒绝服务攻击、中间人攻击等新型攻击手段。这些攻击手段不仅形式多样，而且隐蔽性极强，攻击目标明确，针对性强，一旦遭受网络攻击，可能导致数据泄露、系统瘫痪，对短波广播发射台的安全管理构成严重的威胁，我们只有系统化了解网络安全威胁才能及时采取安全防范措施。

2.1.1 计算机病毒和恶意软件

病毒和恶意软件是指病毒、蠕虫、木马、勒索软件、间谍软件等，在计算机网络系统中，这些是设计用来感染和破坏计算机系统的程序，可以通过电子邮件附件、下载文件或访问感染的网站传播。通过网络远程控制其他用户的计算机，窃取信息资料，或者用来进行其他有害行为。

2.1.2 网络钓鱼

网络钓鱼是一种以欺骗手段获取敏感个人信息（如口令等）的攻击方式，通过发送欺诈性电子邮件和构建仿冒网站实施诈骗行为。

【作者简介】宋雅静（1982–），女，中国吉林桦甸人，本科，工程师，从事广播发射台站节目传输及网络信息化研究。

2.1.3 拒绝服攻击

拒绝服务攻击（Denial of Service,DoS）拒绝服务攻击（Denial of Service, DoS）通常利用传输协议的脆弱性、系统漏洞以及服务漏洞，对目标系统发起大规模的攻击。该攻击通过发送超出目标处理能力的大量合法请求数据包，消耗可用的系统资源和带宽资源，导致程序缓冲区溢出错误，使得目标系统无法处理合法用户的请求，无法提供正常服务，最终导致网络服务瘫痪，甚至系统死机。

分布式拒绝服务攻击（DDoS）是在 Dos 基础上产生的，也是目前威力最大的 DoS 攻击方法。

2.1.4 中间人攻击

中间人攻击是涉及攻击者在通信双方之间建立独立的连接，并交换所截获的数据。此攻击手段使得通信双方误以为他们通过一个私密的连接直接与对方交流，而实际上，整个会话过程完全处于攻击者的控制之下。在中间人攻击的场景中，攻击者能够截获通信双方的对话内容，并可能插入或篡改新的信息。中间人攻击是一个（缺乏）相互认证的攻击。

2.2 网络安全防护能力不足

在数智化时代，短波发射电台对网络技术的依赖显著增强，网络技术、应用系统的使用提升了短波发射台的工作效率，减少了人力需求，解决了电台人力资源紧张的压力，但是部分台站由于网络设备投入了大量的资金，网络设备防御设备投入不足，普遍存在人防系统设备老化的问题。网络防御存在缺陷，整个网络环境存在不安全的因素，如：病毒入侵风险高，漏洞管理滞后，漏洞未能及时检测修补，数据传输加密不足等等，缺乏动态防御、行为分析等主动对抗能力，防御技术远远的低于攻击的技术，不能对目前发射台的网络的起到有效的防护。

部分短波发射台自行研发了技术软件或硬件，由于技术力量不足，软件或操作系统中存在未修补的安全漏洞，这些漏洞可能源自编程错误、设计缺陷或不当的系统配置，黑客可以利用这些漏洞入侵系统或获取敏感信息。同时也缺少专业的网络技术维护人才，多数都是兼职担任，缺少在网络安全领域具备深厚技术功底和丰富实践经验的专业人才。部分发射台站网络安全人才培养方面存在不足，导致部分发射台站网络安全维护滞后，这也造成了部分发射台站存在网络安全隐患。

2.3 管理机制存在漏洞

部分短波发射台缺乏统一的安全策略和流程，内部网络安全管理制度不完善，遇到问题，响应滞后，执行不力。在网络安全管理上权限管理松懈，管理设备密码策略上松散、重复使用弱密码的问题普遍存在。网络工作电脑未及时安全防病毒查杀软件，部分设备安装的网络防护设备软件也未能做到及时更新，缺乏对整个台站网络设备定期的安全审计和监控，无法及时发现和修复安全漏洞增加被攻击的风险。

2.4 人员安全意识淡薄

智能化网络设备给发射台的技术人员带来工作的便利，也带来了网络安全风险隐患。部分技术人员安全意识淡薄，对网络威胁认知不足，使用网络设备和网络时，缺乏基本安全防范意识，使用简单易猜或重复使用的密码使攻击者能够轻易地通过暴力破解或字典攻击获得访问权限。部分职工网络安全意识认识不足，内外网存储介质混用，在未确定内外网的情况下，随意将外网接入内网使用，接收邮件时，对于来路不明的链接、下载未知来源的文件随意点击，这些行为极易导致恶意软件的感染和敏感信息的泄露

3 短波广播发射台网络安全防范策略

在短波发射台站数智化转型中，网络安全问题日益复杂，需要我们从技术、管理、法规等多维度构建全面的防护体系。针对短波发射台站网络安全问题，我们应采用相应的防护策略，保障网络运行环境的安全。

3.1 多样化网络安全威胁应对策略

3.1.1 网络防火墙构建。

在短波发射台站的网络边界部署防火墙设备，配置防火墙的访问控制规则。允许或阻止特定的网络流量，仅允许特定 IP 地址或端口进行通信，以防范未授权访问与攻击行为。启用防火墙的日志记录与报警机制，确保能够及时识别并应对潜在的安全威胁。

3.1.2 访问控制与身份认证。

制定严格的访问控制策略，根据用户的角色和职责分配不同的访问权限，限制不同用户对短波发射台站系统和资源的访问权限。确保敏感数据和关键系统只能被授权用户访问。

3.1.3 入侵检测与防御。

在短波发射台站的网络中部署入侵检测系统，实时监测网络流量和系统日志，识别并报警潜在的入侵行为。IDS 可以帮助及时发现并响应安全事件，防止攻击者进一步渗透和利用系统漏洞。

3.1.4 数据加密与传输安全。

对短波发射台站中的敏感数据进行加密存储和传输，确保数据在传输过程中不被窃听或篡改。使用 TLS/SSL 协议加密 Web 通信。

3.2 构建网络安全防范体系

3.2.1 加大信息系统风险和安全漏洞管理。

安装并使用最新的防病毒软件，定期对短波发射台站的系统和设备进行漏洞扫描和风险评估，及时发现并修复安全漏洞。

3.2.2 网络隔离与分区，细化网络安全区域。

将短波发射台站的办公网与技术网进行物理或逻辑隔离，防止办公网中的安全风险传播到技术网。将短波发射台站的关键系统（如发射机控制系统、信号传输系统等）独立部署在一个或多个网络分区中，降低它们受到攻击的风险。

采取多因素身份认证，强化信息系统权限管理。在短波发射台站的关键系统中实施多因素身份认证机制，结合密码、生物识别（如指纹、面部识别）和动态验证码等多种因素进行身份验证，提高用户身份验证的准确性和安全性。对用户和系统角色进行职责权限划分，确保操作人员只能访问完成工作所需的最小权限范围内的资源和数据。

3.2.3 完善数据备份与恢复机制

网络在运行中会受到攻击或人为过失导致网络数据丢失和系统瘫痪，制定数据备份策略，定期备份重要数据，防数据丢失或篡改，将备份数据存储在安全的位置，确保其可恢复性。

3.3 建立网络安全防范意识

提升网络安全防范意识是确保短波发射台整个网络安全的重要一环。组织定期的网络安全培训课程，邀请网络安全专家或内部安全团队进行网络威胁、攻击手段、防范措施等，帮助员工了解网络安全的重要性和紧迫性。

制定详细的操作规范，明确员工在网络安全方面的职责和要求。教育员工持续保持警觉，警惕网络钓鱼邮件、恶意软件等网络威胁。避免点击来源不明的链接、下载未知来源的文件、泄露个人敏感信息等行为。

4 短波发射台网络安全防范的实际案例

以高寒地区某一短波发射台为例以下简称（某台），为了确保发射台网络安全和数据安全，某台采取一系列网络安全防范措施，取得了显著的成效。

某台在网络边界部署了高性能的防火墙设备，并对防火墙进行了安全策略配置，允许合法的流量进出，阻断不安全或恶意的流量进出。防火墙根据源、目的地址、端口等重要信息，精准管控流量的进出，对数据包的内容进行有效过滤。目前，某台大部分服务器都安放在数据中心，DDoS 攻击也是某台面临的主要网络安全威胁，防火墙的部署在抵御 DDoS 攻击中，发挥了巨大的作用，也为某台网络安全提供保障。在防火墙部署后，某台就有效地拦截了非法网址的攻击，如图 1 示意图所示。

在部署防火墙的基础上，某台又先后部署了入侵检测设备、漏洞扫描设备以及审计日志设备作为防火墙的必要补充，在不影响网络运行的情况下，对网络进行扫描和监测记录，发现安全隐患后，会切断网络连接并记录下异态的时间并报警提醒。

对于所有电脑终端，某台部署了 360 终端管理系统，对所有的终端安装杀毒软件，并对端口进行封堵，防止非法使用移动存储介质。360 终端管理系统可以远端对各终端软件进行监管。及时发现不安全行为，并进行隔离，某台 360 终端管理系统部署后，在运行中发现了某系统运行病毒，并进行了隔离，维护人员根据系统提示，查找问题所在，进行处理，解决网络威胁。

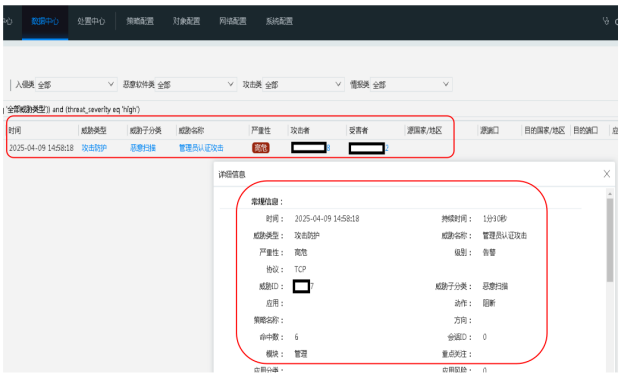

图 1 防火墙拦截恶意扫描

某台还制定了各项网络安全管理制度，明确了安全职责和使用规范，并邀请网络设备厂家对台站现有的网络技术人员培训，提升其网络维护水平，组织网络技术人员定期对台内所有职工进行网络安全培训，使网络安全意识入脑入心。

通过上述网络安全防范措施的实施，某台短波发射台成功抵御了多次网络攻击和威胁。员工的网络安全意识显著提高，能够及时发现并报告潜在的安全风险。近年来也未发生过网络安全事故，收到了良好的成效。

5 结论与展望

短波发射台在数智化转型过程中面临着诸多网络安全挑战。通过部署防火墙与入侵检测系统、实施访问控制与身份认证、数据加密与传输安全、安全培训与意识提升措施，有效提升短波发射台的网络安全防范能力。这些措施不仅保障了系统的正常运行和数据安全，也为短波发射台的数智化转型提供了有力支撑。网络安全已进入了“攻防对抗常态化”阶段，未来我们短波发射台要紧跟时代发展，融合技术创新、构建覆盖“技术 - 人才 - 政策”的全链条防护网络以应对数字化、智能化带来的安全挑战。

参考文献：

[1] 网络安全与攻防技术实训教程. 互联网文档资源（https://max.book118.），2023

[2] 最新《网络安全攻防技术》. 互联网文档资源（https://wenku.baidu.），2020

[3] 赵铖冲. 基于双向生成对抗神经网络的汽轮机网络入侵检测方法研究. 南京理工大学硕士论文, 2023