医院计算机网络安全管理工作的维护策略分析

马国鹏　强　皑*
宁夏医科大学总医院信息中心　宁夏　银川　750000

摘　要：随着智能化技术的深入应用，医院计算机网络安全面临诸多挑战，包括外部威胁、内部威胁及严格的合规性要求。在此背景下，本文分析了医院网络系统的特点及当前网络安全管理的难点，重点探讨了网络安全策略、基础设施安全、数据安全与加密、访问控制与权限管理等核心策略。此外，本文提出了日常维护与监控、漏洞扫描与补丁管理、应急响应计划等具体维护措施，以提升医院网络的整体安全性。通过多层次、全方位的安全管理，医院可有效应对网络安全威胁，保障患者隐私和医疗数据的安全。

关键词：医院计算机；网络安全管理；维护策略

引言

信息技术的迅猛发展，医院网络系统已成为现代医疗服务不可或缺的重要支撑。然而，医院网络系统在处理大量敏感患者信息的同时，也面临着日益严峻的网络安全挑战。外部威胁如网络攻击、数据泄露和DDoS攻击，以及内部威胁如勒索病毒和人为失误，都对医院网络安全构成了严重威胁。此外，严格的合规性要求也使得医院在数据保护和隐私管理方面面临更高的标准。因此，制定和实施有效的网络安全策略，包括加强基础设施安全、数据加密、访问控制与权限管理，以及建立应急响应计划，成为保障医院网络安全的关键。本文旨在分析当前医院计算机网络安全的现状，探讨有效的安全管理策略，并提出具体的维护措施，以期为医院网络安全管理提供参考和指导。

1 医院计算机网络安全现状分析

1.1 医院网络系统的特点

医院网络系统是现代医疗服务的重要支撑，具有以下几个显著特点：首先，医院网络系统的数据处理量大且复杂。医院涉及的各类信息包括患者个人信息、医疗数据、诊断报告、影像资料等，这些数据需要高效、安全地存储、传输和处理。其次，医院网络系统需要高度的安全性。由于涉及大量敏感的患者信息，系统必须具备强大的数据加密、防火墙、入侵检测等安全防护措施，以防止数据泄露和外部攻击。此外，医院网络系统要求高可用性和稳定性。医疗服务对时间和准确性的要求极高，因此网络系统必须保证24小时不间断服务，避免因故障或停机导致的医疗延误。最后，医院网络系统需要实现设备间的互联互通。各种医疗设备、诊断仪器、电子病历系统等需要通过网络进行实时数据交换和共享，以提供准确、及时的医疗服务[1]。

1.2 当前医院网络安全面临的挑战

1.2.1 外部威胁

当前医院网络安全面临的外部威胁日益严重，主要表现为以下几个方面：首先，网络攻击是医院面临的主要外部威胁之一。黑客可能通过勒索病毒、恶意软件等手段攻击医院网络，导致系统瘫痪、数据丢失或泄露，甚至通过勒索病毒要求支付赎金。其次，数据泄露也是一个严重问题。外部攻击者通过漏洞入侵医院网络，获取患者个人信息、诊疗记录等敏感数据，可能被用于非法交易或其他不法用途，给患者隐私安全带来极大风险。此外，分布式拒绝服务攻击（DDoS）也对医院网络构成威胁。攻击者通过大量虚假流量淹没医院网站或系统，造成网络服务中断，影响日常医疗操作和急诊处理。

1.2.2 内部威胁

当前，医院网络安全面临的外部威胁日益严峻，主要体现在以下几个方面：首先，勒索病毒攻击成为医院面临的重大安全挑战。黑客通过勒索病毒加密医院的数据文件，要求支付赎金才能恢复系统，导致医疗服务中断，严重影响患者的治疗。其次，数据泄露也是外部威胁之一。医院内部和外部网络的漏洞可能被攻击者利用，窃取大量敏感的患者信息，如病历、诊断报告等，这不仅危及患者隐私，还可能导致法律和声誉风险。

第一作者简介：名字：马国鹏(出生年月1987.11)，性别男，学历：本科，职称：初级，研究方向：计算机，通讯地址：宁夏银川市兴庆区胜利南街804号 宁夏医科大学总医院信息中心 电话：13469617851邮箱：234030435@qq.com

通讯作者：强皑1989年5月，性别男，学历：大学本科，职称中级，通讯地址：宁夏银川市兴庆区胜利南街804号 宁夏医科大学总医院信息中心，邮编750000

1.2.3 合规性要求

当前，医院网络安全面临的挑战不仅包括技术层面的防护，还涉及严格的**合规性要求**。医院在数据保护和隐私管理方面必须遵循多项法律法规，如《中华人民共和国网络安全法》以及《医疗信息安全管理规范》等，确保患者的敏感信息得到妥善保护。首先，医院需要符合数据隐私保护的合规性要求，确保患者的个人信息不被泄露、篡改或滥用。对于医疗数据的存储、传输和使用，必须实施加密、访问控制等技术手段，防止未经授权的访问。其次，随着电子健康记录（EHR）的普及，医院必须遵循相关法律法规对电子数据存储和交换的合规性要求，确保医疗信息的安全性和完整性。

2 医院计算机网络安全管理的主要策略

2.1 网络安全策略的制定与实施

医院计算机网络安全管理的主要策略包括加强安全防护、完善管理制度、进行定期安全评估和加强人员培训。随着信息技术在医疗行业的广泛应用，医院面临着数据泄露、病毒攻击、网络入侵等安全威胁，因此制定有效的网络安全策略显得尤为重要。首先，医院应加强网络基础设施的安全防护，采用防火墙、入侵监测系统（IDS）等技术手段，实时监控网络流量，及时发现和应对异常活动。同时，医院需要确保所有操作系统和软件的及时更新与漏洞修补，减少被攻击的风险。其次，医院要建立健全的信息安全管理制度，明确网络安全责任，确保每个部门、每位员工都能遵守信息安全规范。定期进行安全评估与风险分析，及时识别潜在的安全隐患，制定应急响应方案，确保能够在发生安全事件时迅速有效地处理。此外，加强对医院员工的网络安全培训至关重要。通过定期的安全培训，增强员工的安全意识，避免人为失误或恶意行为导致信息泄露或网络攻击[2]。

2.2 基础设施安全

医院计算机网络安全管理的基础设施安全是保障医院信息系统安全的核心。随着信息技术在医疗领域的广泛应用，医院的计算机网络面临着日益复杂的安全威胁，因此，建设健全的基础设施安全是保障网络安全的第一步。首先，医院需要部署防火墙、入侵检测系统（IDS）和入侵防御系统（IPS），这些技术能够有效监控网络流量，及时发现并阻止恶意攻击。防火墙作为网络安全的第一道屏障，应针对外部攻击进行有效隔离，确保医院内部网络的安全性。其次，医院要确保其网络设备和系统的定期维护与升级。通过及时修补漏洞和更新操作系统，避免潜在的安全风险。同时，应对网络设备进行物理安全管理，防止未经授权的人员访问医院的核心网络设备。

2.3 数据安全与加密

医院计算机网络安全管理中的数据安全与加密策略至关重要，尤其是在保护患者隐私和医疗数据方面。医疗信息的泄露不仅会危及患者的个人隐私，还可能导致医院面临法律责任和声誉损害。因此，实施有效的数据安全与加密措施是确保医院网络安全的核心内容之一。首先，医院应采用数据加密技术对敏感信息进行保护。无论是存储在数据库中的患者信息，还是在网络上传输的医疗数据，都应通过加密算法进行加密处理。常见的加密技术如对称加密、非对称加密和SSL/TLS加密协议，能够有效防止数据在传输过程中被窃取或篡改。其次，医院还应对敏感数据进行分类管理，对于不同级别的数据采取不同的安全保护措施。对于涉及个人隐私、医疗记录等重要信息，要采取更严格的加密措施，并限制访问权限，仅允许授权人员查看或修改。此外，医院应定期进行数据备份和恢复演练，确保在系统出现故障或遭受攻击时，能够快速恢复数据并保持服务连续性。同时，对数据访问权限进行严格管理，避免因人为操作失误或内部员工滥用权限而导致数据泄露。

2.4 访问控制与权限管理

医院计算机网络安全管理中的访问控制与权限管理是保护医疗数据和信息安全的重要策略。由于医院内涉及大量的敏感信息，如患者个人资料、诊疗记录等，严格的访问控制能够有效防止未经授权的人员访问或篡改数据。首先，医院应实施基于角色的访问控制（RBAC）策略，根据不同岗位的职责分配相应的访问权限。医疗人员、行政人员和技术支持人员的访问需求不同，因此，应当为每个角色定义清晰的权限范围，确保每位员工只能访问与其工作相关的资源。例如，医生可以查看患者的病历信息，而财务人员则只能访问与财务相关的数据。其次，权限管理需要与身份认证机制相结合。医院应采用多因素认证（MFA）等先进的身份验证方式，确保只有经过验证的人员才能登录系统并访问敏感数据。此外，应定期更新访问权限，及时调整离职员工的账户权限，防止因人员变动带来的安全漏洞。医院还应实施审计与监控机制，记录每一次访问和操作日志，确保在发生安全事件时能够追溯责任和源头。通过定期审查访问权限和操作记录，医院可以及时发现异常行为，增强网络的安全性[3]。

3 医院计算机网络安全管理的具体维护措施

3.1 日常维护与监控

医院计算机网络安全管理的日常维护与监控是确保

网络系统持续稳定运行、防止安全漏洞的关键措施。随着医疗信息化的推进，医院网络安全面临着越来越多的威胁，因此，日常维护与监控必须成为医院信息安全管理的重要组成部分。首先，医院应定期更新和打补丁，确保所有计算机系统和软件都处于最新状态。黑客常利用软件漏洞进行攻击，因此，及时安装操作系统、数据库和应用程序的安全补丁，能有效修补已知漏洞，降低被攻击的风险。其次，医院应加强对网络流量的实时监控，利用入侵检测系统（IDS）和入侵防御系统（IPS）监测异常活动。通过分析网络流量和日志记录，能够发现潜在的安全威胁，并在早期采取应对措施。尤其是在面对DDoS攻击或恶意软件时，及时发现和响应至关重要。此外，医院还需实施数据备份与灾难恢复策略。定期进行数据备份，确保在系统故障或遭遇攻击时能够快速恢复。同时，建立应急响应机制，定期进行安全演练，确保在发生网络安全事件时，相关人员能够迅速、有效地应对[4]。

3.2 漏洞扫描与补丁管理

医院计算机网络安全管理中的漏洞扫描与补丁管理是保障系统安全的重要手段。医院内使用的各种信息系统，如电子病历、药品管理系统等，承载着大量敏感数据，任何漏洞都可能成为黑客攻击的突破口，因此，及时发现并修复漏洞是防止网络安全事故的关键。首先，医院应定期进行漏洞扫描，采用专业的安全扫描工具对网络中的设备、操作系统和应用程序进行全面检查。漏洞扫描能够帮助发现系统中存在的安全漏洞、配置错误或未授权的应用，及时识别潜在的安全风险。扫描报告可以为安全管理员提供具体的漏洞详情，帮助其制定修复计划。其次，漏洞扫描发现问题后，医院应尽快部署补丁管理[5]。补丁管理包括及时获取操作系统、应用软件和网络设备的安全补丁，并确保所有设备都能按时安装更新。这些补丁通常修复了软件中的已知漏洞，是阻止恶意攻击和病毒传播的有效手段。

补丁管理不仅要定期进行，还要确保补丁的适用性和兼容性。医院在实施补丁时，必须考虑到临床系统的稳定性和兼容性，避免因为不当更新导致系统故障或服务中断。因此，医院应进行测试和验证，确保补丁安装后不会影响到日常医疗操作。综上所述，漏洞扫描与补丁管理是医院网络安全防护的基础措施，通过定期扫描和及时修复漏洞，医院能够有效减少被攻击的风险，确保患者数据和医疗服务的安全。

3.3 应急响应计划

医院计算机网络安全管理中心的应急响应计划是应对突发网络安全事件的关键保障。随着信息化建设的不断推进，医院的各类敏感数据和医疗服务面临着越来越多的网络攻击风险。因此，建立一个高效的应急响应计划至关重要。首先，医院应明确应急响应的组织结构，成立专门的安全应急响应小组，成员包括信息技术人员、安全专家、管理人员等，确保在发生安全事件时能够快速响应。其次，应急响应计划应包括详细的事件分类、应对流程及职责分工，确保每个环节有序进行。在出现数据泄露、病毒攻击等突发情况时，能够快速识别、隔离并控制事件，防止事态扩大[6]。此外，医院应定期进行应急演练，模拟不同类型的安全事件，检查应急响应流程的有效性。通过演练，提升员工的应急处理能力和团队协作效率。总之，完善的应急响应计划能帮助医院在面对网络安全事件时，迅速有效地应对，最大限度地减少损失，确保医疗系统的正常运行。

结语

医院计算机网络安全管理工作是确保医疗信息系统稳定运行、保护患者隐私的关键。通过加强网络安全防护、定期漏洞扫描与补丁管理、制定应急响应计划等措施，医院能够有效应对各类网络安全威胁。持续的安全管理和培训提升，将帮助医院构建更加稳固的安全防线，保障医疗服务的安全性和可靠性，促进信息化建设健康发展。

参考文献

[1]詹振坤.医院信息化建设中计算机网络安全管理与维护工作思考[J].无线互联科技,2021,18(10):25-26.

[2]刘毅.医院计算机网络安全管理工作的维护策略分析[J].中国现代医药杂志,2021,23(04):86-87.

[3]张婉.信息技术背景下医院计算机网络安全管理探究[J].信息与电脑(理论版),2020,32(17):182-184.

[4]陈益军.医院计算机网络安全管理工作的维护策略分析[J].信息记录材料,2020,21(08):221-222.

[5]王艺伟.医院信息化建设中计算机网络安全管理与维护[J].电脑知识与技术,2020,16(14):78-79.

[6]申军霞.关于医院计算机网络安全管理工作的维护策略研究[J].计算机产品与流通,2020,(05):56.