信息技术环境下医院网络安全管理分析与探究

王立娜

（北京市和平里医院，北京　100039）

摘　要：随着信息技术在医疗领域的广泛应用，医院网络安全管理变得至关重要。本文通过对医院网络安全管理的分析与探究，旨在提供有效的网络安全管理策略，以保护医院信息系统的安全性和隐私性。研究表明，医院网络面临着各种安全威胁和风险，包括数据泄露、恶意软件攻击和未经授权访问等。因此，建立完善的安全管理体系、加强员工培训和意识教育、实施严格的访问控制、定期进行安全审计和漏洞扫描等措施是确保医院网络安全的关键。

关键词：医院网络安全管理；信息技术；安全威胁；网络隐私

中图分类号：TP393.08　　**文献标志码：**A

Analysis and Exploration of Hospital Network Security Management in the Information Technology Environment

WANG Lina

（*Beijing Hepingli Hospital, Beijing* 100039, *China*）

Abstract：With the widespread application of information technology in the medical field, hospital network security management has become crucial. This article aims to provide effective network security management strategies to protect the security and privacy of hospital information systems through the analysis and exploration of hospital network security management. Research has shown that hospital networks face various security threats and risks, including data breaches, malware attacks, and unauthorized access. Therefore, establishing a sound security management system, strengthening employee training and awareness education, implementing strict access control, regularly conducting security audits and vulnerability scanning are key measures to ensure hospital network security.

Keywords：hospital network security management；information technology；Security threats；network privacy

随着科技的飞速发展和医疗信息化的推进，医院信息系统已成为医疗机构不可或缺的一部分。医院网络安全管理的重要性凸显出来，因为医院信息系统中存储了大量的患者敏感数据和医疗机密信息。如果不加以妥善保护，这些信息可能会被黑客攻击、泄露或滥用，给患者隐私和医疗机构的声誉带来严重损害。本文旨在通过分析和探究医院网络安全管理，提供有效的网络安全管理策略，以应对不断增长的网络安全威胁。首先，文章将回顾医院网络安全面临的主要威胁和风险，包括数据泄露、恶意软件攻击和未经授权访问。然后，将探讨如何建立完善的安全管理体系，包括制定安全政策、加强员工培训和意识教育，以及建立严格的访问控制措施。此外，还将讨论定期进行安全审计和漏洞扫描的重要性，以及如何响应安全事件和建立有效的紧急响应机制。

1　医院网络安全面临的主要威胁和风险

1.1　数据泄露和信息窃取

医疗机构存储着大量的患者敏感数据和医疗机密信息，如个人身份信息、病历记录和诊断结果等。这些数据一旦泄露或被窃取，将会对患者的隐私权和医疗机构的声誉造成严重损害。数据泄露和信息窃取的风险主要来自内部和外部的威胁。内部威胁可能源自员工的不当操作、疏忽大意或恶意行为，例如未经授权地访问患者数据或将数据复制到移动设备上。外部威胁包括黑客攻击、网络钓鱼和恶意软件感染等，这些攻击手段通过网络漏洞或社交工程等方式获取敏感数据。为了应对数据泄露和信息窃取的威胁，医院需要采取一系列的安全措施。首先，加密技术是保护数据安全的重要手段。通过对敏感数据进行加密，即使在数据泄露的情况下，攻击者也无法获得原始数据。医院可以使用现代的加密算法和安全协议来保护数据的机密性和完整性。其次，医院应建立严格的访问控制机制，

收稿日期：2024-01-04

作者简介：王立娜（1983.10-），女，汉族，北京人，职称：助理工程师，本科，研究方向：网络安全管理，信息系统项目管理。

限制员工只能访问与其工作职责相关的数据，并监控员工的访问行为。通过分配合适的权限和角色，可以确保只有授权人员能够访问敏感数据，并且记录和审计员工的访问活动，以便发现异常行为。定期进行安全审计和漏洞扫描也是防止数据泄露的重要手段。医院应该对网络系统和应用程序进行定期的安全审计，发现潜在的安全风险和漏洞，并及时采取措施修复这些漏洞。漏洞扫描工具和安全评估服务可以帮助医院识别系统中的弱点，并提供建议和解决方案[1]。此外，敏感数据的备份和灾难恢复计划也是重要的安全措施之一。医院应该定期备份关键数据，并确保备份数据的安全存储和可靠性。在发生数据泄露或系统故障时，可以通过灾难恢复计划迅速恢复数据和服务，减少损失。最后，持续的员工培训和安全意识教育是防止数据泄露的关键。医院应定期向员工提供网络安全培训，教导他们如何识别和应对安全威胁，以及正确操作网络系统和设备。员工应该了解数据保护的重要性，并知晓如何报告安全事件和疑似威胁。

1.2 恶意软件攻击

恶意软件包括病毒、木马和勒索软件等，它们通过电子邮件、恶意链接或感染的存储设备等途径进入医院网络系统。一旦恶意软件感染了医院的计算机或服务器，就可能导致敏感信息泄露、系统功能瘫痪或勒索医院赎金等问题。为了应对这种威胁，医院需要采取多层次的防御措施。首先，安装更新的杀毒软件和防火墙是基本的安全措施，可以检测和阻止恶意软件的传播。这些安全工具可以扫描系统和网络流量，及时发现和清除恶意软件。其次，医院应该加强员工的安全意识教育，教导他们如何辨别和避免恶意软件的攻击手段。员工应该学会不打开来自未知来源的附件或链接，以防止恶意软件通过社交工程手段侵入系统。此外，医院还应定期更新系统和应用程序，并安装最新的安全补丁，以修复已知的安全漏洞。这样可以减少黑客利用已知漏洞进行攻击的可能性。另外，限制用户的权限也是一种有效的安全措施。每个用户应该只拥有访问其工作所需的最低权限，这样可以减少潜在的风险，即使账户被攻击或被恶意软件利用，也能限制其对系统的影响。

1.3 未经授权访问和滥用

未经授权访问和滥用是医院网络安全领域的另一个重要问题，对此，医院需要采取一系列措施来应对这一威胁。这些措施旨在防止未经授权的用户访问敏感数据、防止员工滥用权限以及限制未经授权设备接入网络，从而保护患者隐私和医疗机构的数据安全。首先，医院应建立一个完善的安全管理体系，并明确安全政策和规范。这些政策和规范应涵盖密码强度要求、访问控制规则、设备使用规定等方面，以确保系统和数据的安全。通过明确的安全政策，医院可以为员工提供明确的指导，使其了解哪些行为是被禁止的，从而减少安全漏洞的出现。其次，医院应定期对员工进行网络安全培训和意识教育，提高他们对网络安全的认识和理解。培训内容可以包括硬件设备的安全使用、网络安全知识以及个人密码管理等方面。通过增强员工的安全意识，可以减少因为疏忽或不当操作而引发的安全事件，提高整体的安全水平。医院还应采取有效的访问控制措施来限制对敏感数据和系统资源的访问。这可以包括使用强密码和多因素身份验证，为不同的用户配置适当的权限。医院应实施定期的权限审查和撤销措施，以确保只有合法且有需要的用户才能访问敏感数据和系统资源。此外，监控和记录用户的访问行为也是必要的，以便及时发现并应对任何未经授权的访问或滥用行为。另外，医院应采用网络防火墙、入侵检测系统和安全审计工具等技术手段来监控和保护网络安全。这些工具可以帮助医院及时发现和阻止未经授权的访问尝试，识别潜在的安全威胁，并提供安全事件的日志记录和分析功能，以便进行调查和取证。最后，医院应建立一个响应机制，以便在发生安全事件时能够迅速采取行动。这包括建立一个紧急响应团队，制定应急预案，并定期进行演练和测试，以确保团队成员熟悉应对程序并能够迅速应对安全事件。通过采取这些措施，医院可以有效地应对未经授权访问和滥用的威胁，保护敏感数据和系统资源的安全。然而，网络安全是一个持续的过程，医院需要不断关注和更新安全措施，以适应不断演变的安全威胁。只有通过综合的安全管理措施和持续的监测，医院才能确保网络系统的安全性和稳定性。

2 信息技术环境下医院网络安全管理措施

2.1 建立完善的安全管理体系

安全政策和规范应该是明确、具体且可执行的，以确保医院网络系统的安全性和合规性。在医院网络安全政策中，首先需要明确规定医院的网络安全目标和原则。这包括确保患者隐私和数据保护、防止未经授权访问、识别和应对安全威胁等。政策还应规定安全责任和权限，明确各级管理人员和员工在网络安全方面的职责和义务。安全规范应提供具体的操作指南和要求。例如，规定密码复杂度和更新频率、数据备份和恢复策略、网络设备和软件的安全配置要求等。规范还涵盖网络审计和监控、安全事件响应和报告等方面的流程和要求，以确保医院能够及时发现和应对安全事件。制定安全政策和规范的过程应由医院信息化领导小组成员共同参与。他们应该代表不同部门和职能，以确保政策和规范的全面性和适用性。在制定过程中，应该考虑法律法规、行业标准和最佳实践，以确保医院网络安全符合相关要求。政策和规范的制定后，需要进行定期的审查和更新。医院网络安全环境在不断变化，新的安全威胁和漏洞可能会出现。因此，政策和规范需要与时俱进，以适应新的挑战和技术环境。此外，为了确保政策和规范的有效执行，还需要进行员工培训和意识教育。医院应该定期向员工提供网络安全培训，教导他们如何识别和应对安全威胁，以及正确操作网络系统和设备。

2.2 强化访问控制措施

访问控制措施主要包括身份验证、权限管理和监控等方面的措施。首先，医院可以采用强身份验证机制，例如使用多因素身份验证（MFA）来确保只有经过授权的用

户访问敏感数据和系统资源。MFA 要求用户提供多个身份验证因素，如密码、指纹、短信验证码等，以增加访问的安全性。其次，医院应建立健全的权限管理机制，限制用户对系统资源的访问权限。每个用户应该被分配到适当的权限级别，并及时审查和更新权限。定期进行权限审查和撤销已离职或不需要的用户的权限，以防止未经授权的访问。监控包括实时监控、日志记录和报警系统等，以提高对网络安全威胁的感知能力。强化访问控制措施还包括对网络边界的保护。医院应该使用防火墙、入侵检测和预防系统（IDS/IPS）等技术，对网络流量进行筛查和监控，以阻止恶意攻击和未经授权的访问[3]。建立完善的安全管理体系需要制定明确的安全政策和规范，进行员工培训和意识教育，以及强化访问控制措施。这些措施相互配合，帮助医院提高网络安全防护能力，保护患者隐私和数据安全。同时，医院还应定期评估和改进安全管理体系，以适应不断变化的安全威胁和技术环境[4]。

2.3 定期进行安全审计和漏洞扫描

首先，进行漏洞优先级评估。根据漏洞的严重程度、易受攻击的潜力和可能的影响，对漏洞进行优先级评估。这有助于确定修复漏洞的优先顺序，并根据医院的具体情况和业务需求来制定相应的修复计划。其次，制定修复计划。根据漏洞的优先级，制定详细的修复计划。计划应包括修复措施、负责人、时间表和跟踪机制。确保每个漏洞都有明确的责任人负责修复，并设定合理的时间表来完成修复工作。跟踪机制有助于监督修复进度，并确保漏洞得到及时修复。接下来，执行修复工作。根据制定的修复计划，对漏洞进行修复工作。这可能涉及更新系统和应用程序的补丁、配置更改、强化访问控制等。确保修复工作得到适当的测试和验证，以确保修复措施有效并不会引入新的问题。完成修复后，进行定期的重新扫描。重新扫描的目的是验证漏洞是否已成功修复，并及时发现新的漏洞。这有助于确认修复措施的有效性，并保持医院网络系统的安全状态。同时，建立漏洞管理系统，对漏洞进行跟踪和记录。这可以帮助建立漏洞修复的持续过程，并确保所有漏洞得到妥善处理。记录漏洞修复的详细信息，包括修复日期、修复方法和验证结果等。这有助于监控漏洞修复的情况，并提供参考数据用于安全审计和合规要求。通过对漏洞扫描结果进行分析和处理，医院可以及时修复漏洞，减少系统受到攻击的风险，并确保网络系统的安全性和稳定性。定期的漏洞扫描和修复工作是医院网络安全管理的重要组成部分，需要持续关注和投入资源来确保网络系统的稳健防护[5]。

2.4 响应安全事件和建立紧急响应机制

安全事件是指可能对医院网络系统和数据造成威胁或损害的事件，包括非授权访问、恶意软件攻击、数据泄露和拒绝服务攻击（DDoS）。为了更好地管理和应对安全事件，医院可以采取以下步骤：首先，及时检测和识别安全事件的发生是至关重要的。通过安全监控系统和日志分析等手段，医院可以及早发现安全威胁并确认事件的性质和范围。其次，进行情报收集和分析。医院应收集有关安全事件的信息和数据，并对其进行分析，以评估威胁和影响。这有助于了解攻击者的行为模式、攻击手段以及潜在的漏洞。接下来，采取响应和遏制措施。医院应该快速采取行动，限制安全事件的扩散和影响。这可能包括隔离受影响的系统、停止恶意活动、阻止非授权访问等措施，以保护关键系统和数据。然后，进行恢复和修复工作。医院需要恢复受影响的系统和服务的正常运行，并采取必要的修复措施，如修复漏洞、清除恶意软件等。这有助于恢复业务连续性和保护系统免受进一步的攻击。最后，进行事后分析和报告。医院应对安全事件进行详细分析，确定事件的原因和漏洞，并撰写事件报告。报告中应提出改进措施和建议，以防止类似事件再次发生。这有助于从安全事件中吸取教训，并改进安全防护措施。通过有效的安全事件管理和应对措施，医院可以更好地保护网络系统和数据的安全性，降低安全风险，并确保医院网络的可靠性和合规性。这需要医院建立健全的安全策略和规范，并与时俱进地更新和改进这些措施，以适应不断变化的安全威胁和技术环境[7]。

3 结 语

综上所述，网络安全一直是医院信息化建设中不可忽视的重要环节，也已成为医院正常运行的重要部分。为保障数据安全，医院应建立完善的安全管理体系、明确安全政策和规范，定期进行漏洞扫描，及时发现修复漏洞防止潜在的安全威胁。此外应建立紧急响应机制，加强员工网络安全意识培训与教育并定期进行安全演练，以提高应对网络安全事件的能力。确保医院网络系统稳定和安全运行。

参考文献：

[1] 刘顺 . 智慧医疗视角下医院网络安全管理系统构建探析 [J]. 电脑知识与技术 ,2023,19(11):63-65.
[2] 彭宇 . 基于智慧医疗的医院网络安全管理研究 [J]. 中国设备工程 ,2022,(23):28-30.
[3] 裴晨思 . 基于区块链的医院网络信息安全管理探讨 [J]. 软件 ,2022,43(11):108-110.
[4] 刘翰腾 , 王毅 , 陈宗耿等 . 现代医院网络安全管理面临的挑战和对策 [J]. 中国信息安全 ,2022,(07):55-58.
[5] 谷敏 . 医院网络安全管理方案与措施探究 [J]. 网络安全技术与应用 ,2022,(06):115-117.
[6] 戚大军 . 二级医院网络安全管理研究 [D]. 青岛大学 ,2022.
[7] 刘朋 . 网络环境下医院计算机网络安全管理分析 [J]. 长江信息通信 ,2021,34(12):137-139.