医院计算机网络安全管理措施

张　翔*　张海涛
吴忠新区医院　宁夏　吴忠　751100

摘　要：医院计算机网络安全管理措施包括强化网络边界防御，如设置防火墙和入侵检测系统；实施访问控制与身份认证，限制用户权限；加强数据加密与备份，确保数据安全；防护恶意程序，安装并定期更新杀毒软件；注重硬件安全管理，保护中心机房与设备；严格管理软件与系统，修补漏洞并配置高性能服务器。这些措施共同保障医院信息系统稳定运行，有效防范网络威胁，保护患者隐私，维护医院安全与信誉。

关键词：医院计算机；网络安全；管理措施

引言：随着医疗信息化的发展，医院计算机网络安全已成为医院运营不可或缺的一部分。医疗数据的敏感性、患者隐私的保护以及医院业务的连续性，都要求医院必须高度重视计算机网络安全管理。本文旨在探讨医院计算机网络安全管理的各项措施，包括技术防范、管理制度建设等方面，以期为医院提供一个全面、可行的网络安全管理方案，确保医院信息系统稳定运行，保障患者权益，提升医疗服务质量和效率。

1 医院计算机网络安全概述

1.1 医院计算机网络安全定义

医院计算机网络安全是指通过一系列技术、管理和法律手段，保护医院计算机网络系统及其中的数据不受未经授权的访问、攻击、破坏或篡改，确保网络系统的机密性、完整性和可用性。这涵盖了医院内部所有使用计算机技术和网络通信的医疗信息系统，如医院信息系统（HIS）、影像归档和通信系统（PACS）等，以及与之相连的所有设备和数据。

1.2 医院计算机网络安全的重要性

在当今数字化时代，医院计算机网络已成为医院运营的核心组成部分。它不仅关系到医疗服务的连续性和质量，还直接涉及到患者的隐私保护和医疗数据的安全。医院计算机网络存储着大量的患者个人信息和医疗记录，这些信息对于医疗诊断、治疗和科研具有重要意义。一旦网络系统遭受攻击或数据泄露，将导致患者信息被滥用，可能引发医疗欺诈、身份盗窃等严重后果，同时也会给医院带来极大的法律风险和社会舆论压力。此外，医院计算机网络还承担着医疗资源的分配和管理任务。如果网络系统出现故障或瘫痪，将直接影响医院的正常运营，导致医疗服务中断，给患者带来不便和痛苦[1]。因此，确保医院计算机网络安全是维护医疗秩序、保障患者权益和提高医疗服务质量的必然要求。

1.3 医院计算机网络安全面临的主要威胁

医院计算机网络安全面临的主要威胁包括非法访问、数据泄露和恶意程序攻击等。（1）非法访问是指未经授权的用户通过破解密码、利用漏洞等方式进入医院网络系统，窃取或篡改敏感数据。（2）数据泄露则是指医院内部员工因疏忽或恶意行为，将患者信息泄露给外部人员或机构。（3）恶意程序攻击是指黑客利用病毒、木马等恶意软件，对医院网络系统进行攻击和破坏，导致系统瘫痪或数据丢失。这些威胁不仅来源于外部黑客的攻击，还可能来自医院内部员工的失误或恶意行为。因此，医院需要建立完善的网络安全管理体系，加强员工的安全意识培训和技术防范措施，确保医院计算机网络的安全稳定运行。

2 医院计算机网络安全管理现状分析

2.1 医院信息化建设的背景与现状

随着信息技术的不断进步和医疗需求的日益增长，医院信息化建设已经成为医疗行业转型升级的重要驱动力。在政策的引导和支持下，医院正逐步实现业务流程的数字化、智能化，以提升医疗服务质量和效率。医院信息系统（HIS）、电子病历系统（EMR）、医学影像系统（PACS）等关键系统的广泛应用，使得医疗数据的管理和使用更加高效便捷。同时，远程医疗、移动医疗等新兴业态的兴起，进一步推动了医院信息化建设的步伐。然而，随着医院信息化水平的不断提升，医院计算机网络的安全风险也日益凸显。医疗数据的敏感性和隐私性要求极高，一旦泄露或被篡改，将对患者权益、医院声誉以及医疗秩序造成严重影响。

2.2 计算机网络安全管理在医院的应用情况

近年来，医院对计算机网络安全管理的重视程度逐渐提高。许多医院已经建立了基本的网络安全防护体

通讯作者：张翔

系，包括防火墙、入侵检测系统、数据加密等措施，以防范外部攻击和数据泄露。同时，医院还加强了对内部员工的网络安全培训，提高了员工的安全意识和操作规范。此外，医院在信息化建设中还积极探索新技术的应用，如云计算、物联网等，以提升医疗服务的智能化水平。然而，这些新技术也带来了新的安全风险。例如，云计算环境下数据的存储和传输更加复杂，增加了数据泄露的风险；物联网设备的安全防护能力较弱，易受到攻击。因此，医院在应用新技术时，必须同步加强网络安全管理，确保技术的安全性和可控性。

2.3 医院计算机网络安全管理中存在的主要问题

尽管医院在计算机网络安全管理上取得了一定进展，但仍存在诸多问题：（1）重视程度不足。部分医院管理层对网络安全的认识不够深入，将网络安全视为IT部门的职责，缺乏全局性的战略规划和持续的投入。（2）资金投入有限。医院在信息化建设上的投入已经很大，但在网络安全方面的投入相对不足，难以购置先进的网络安全设备和软件。（3）缺乏专业技术团队。网络安全管理需要专业的技术支持，但部分医院缺乏专业的网络安全人才，导致网络安全管理水平和应对能力有限。（4）安全意识淡薄。部分医院员工对网络安全的认识不足，缺乏基本的安全意识和操作规范，容易成为网络攻击的突破口。（5）法规遵从性不高。随着网络安全法规的不断完善，医院在网络安全方面的法规遵从性要求越来越高。然而，部分医院在网络安全制度建设、数据保护等方面还存在不足，难以满足法规要求。

3 医院计算机网络安全管理措施

3.1 网络边界防御

（1）设置防火墙。防火墙是医院计算机网络的第一道防线，通过设定安全规则，对进出网络的数据包进行过滤和监控。防火墙能够有效阻止未经授权的访问和恶意软件的入侵，保护医院内部网络不受外部威胁。在设置防火墙时，应根据医院业务需求和网络安全策略，合理配置规则，确保既能有效防护又能保持网络畅通。（2）部署入侵检测系统。入侵检测系统（IDS）能够实时监控网络中的异常行为，及时发现并报告潜在的安全威胁。通过与防火墙的协同工作，入侵检测系统能够进一步提升医院网络的安全防护能力。医院应部署基于网络和主机的入侵检测系统，对关键业务和敏感数据进行实时监控和预警[2]。（3）控制外部网络访问。为了降低外部网络对医院内部网络的潜在威胁，医院应严格控制外部网络访问。这包括限制访问医院网络的外部IP地址范围、关闭不必要的网络端口和服务等。同时，对于必须开放的端口和服务，应设置严格的访问控制和认证机制，确保只有授权用户才能访问。

3.2 访问控制与身份认证

（1）对网络进行分段管理。医院网络应根据业务需求和安全策略进行分段管理，将不同部门和业务系统的网络隔离开来。这不仅可以降低安全风险，还能提高网络的可用性和可管理性。在网络分段时，应充分考虑数据的流动性和业务需求，确保网络分段的合理性和有效性。（2）限制不同用户的访问权限。医院应建立完善的用户权限管理机制，对不同用户进行角色划分，并根据其角色和职责赋予相应的访问权限。这有助于防止内部人员滥用职权或误操作导致的安全事件。同时，医院还应定期对用户权限进行审查和更新，确保权限的准确性和时效性。（3）采用密码、指纹或智能卡等方式进行身份认证。为了确保用户访问的合法性和安全性，医院应采用多种身份认证方式。除了传统的密码认证外，还可以考虑使用指纹、智能卡等生物特征或物理介质进行身份认证。这些认证方式具有更高的安全性和可靠性，能够有效防止未经授权的访问和攻击[3]。

3.3 数据加密与备份

（1）对重要数据进行加密存储和传输。为了保护医院敏感数据的安全性和隐私性，医院应采用数据加密技术对重要数据进行存储和传输。通过对数据进行加密处理，即使数据在传输过程中被截获或存储时被非法访问，也无法被直接读取和利用。医院应选择合适的加密算法和密钥管理方式，确保数据加密的有效性和安全性。（2）定期进行数据备份。数据备份是防止数据丢失和保障业务连续性的重要手段。医院应建立完善的数据备份机制，定期对关键数据和系统进行备份。备份数据应存放在安全可靠的位置，并定期进行恢复测试，以确保备份数据的可用性和可靠性。（3）灾难恢复计划制定与实施。为了应对可能发生的自然灾害、人为错误或恶意攻击等导致的网络瘫痪和数据丢失等灾难性事件，医院应制定详细的灾难恢复计划。该计划应包括数据备份策略、恢复流程、应急响应措施等关键内容。同时，医院还应定期组织演练和培训活动，提高员工对灾难恢复计划的理解和执行能力。

3.4 恶意程序防护

（1）安装杀毒软件。杀毒软件是防御恶意程序入侵的有效工具。医院应在所有终端设备和服务器上安装杀毒软件，并定期进行更新和升级。杀毒软件能够实时监测和清除恶意程序，保护医院网络免受病毒、木马等恶意软件的攻击。（2）实时监控和防护恶意程序。除了安

装杀毒软件外，医院还应实施实时监控和防护恶意程序的措施。这包括使用网络入侵防御系统（IPS）和终端安全管理软件，对网络流量和终端设备行为进行实时监控和分析。通过识别异常行为和潜在威胁，这些系统能够及时采取措施阻止恶意程序的传播和攻击。（3）定期更新升级杀毒软件。由于恶意程序不断演变和更新，杀毒软件也需要不断更新和升级以保持其防护能力。医院应建立定期更新杀毒软件的机制，确保软件能够及时识别和防御最新的恶意程序。同时，医院还应关注杀毒软件的更新通知和漏洞信息，及时修补可能存在的安全漏洞[4]。

3.5 硬件安全管理

（1）网络布线与设备选择。网络布线是医院计算机网络的基础设施之一，其质量和安全性直接影响网络性能和安全性。医院应选择符合标准和质量的网络布线材料和设备，并遵循规范的布线工艺和操作流程。同时，医院还应定期对网络布线进行检查和维护，确保线路的完整性和可靠性。在网络设备选择方面，医院应根据业务需求和安全要求选择性能稳定、安全性高的设备。这些设备应具备完善的安全功能和策略配置选项，能够支持防火墙、入侵检测、访问控制等安全防护措施的实施。同时，医院还应定期对网络设备进行维护和升级，确保其正常运行和安全性。（2）中心机房的安全防护。中心机房是医院计算机网络的核心区域，其安全性直接关系到整个网络系统的稳定和安全。医院应采取多种措施保护中心机房的安全，包括设置门禁系统、监控摄像头、烟雾报警器等物理安全设施；配置冗余电源、UPS不间断电源等供电保障设施；以及实施严格的防火、防水、防潮等环境控制措施。（3）硬件设备的监管与维护。医院应对所有网络硬件设备进行统一监管和维护。通过建立设备台账和管理制度，医院可以全面了解设备的配置、性能和使用情况。同时，医院还应定期对设备进行维护和检修，确保其正常运行和延长使用寿命。对于即将报废或更新的设备，医院应提前做好规划和准备工作，避免设备更新带来的安全风险。

3.6 软件与系统安全

（1）严格管理和控制系统登录账号与访问权限。医院应建立完善的管理机制，严格控制和管理系统登录账号与访问权限。通过为每个用户分配唯一的账号和密码，并设置合适的访问权限级别，医院可以确保只有授权用户才能访问和使用系统资源。同时，医院还应定期审查账号和权限配置情况，及时删除无效账号和回收不必要的权限。（2）修补系统漏洞，关闭不常用的网络端口。系统漏洞和不常用的网络端口是黑客攻击的常见目标。因此，医院应定期对系统进行漏洞扫描和风险评估，及时发现并修补可能存在的安全漏洞。同时，对于不常用的网络端口和服务，医院应及时关闭以减少潜在的安全风险。在操作过程中，医院应谨慎处理与业务相关的关键服务和端口，并采取相应的安全防护措施。（3）高配置的服务器与不间断电源配置。医院计算机网络系统的稳定运行离不开高性能的服务器设备。为了确保医疗业务的连续性和数据的安全性，医院应选择配置高、性能稳定的服务器，并定期进行性能测试和维护。在选择服务器时，医院应考虑其处理能力、存储容量、扩展性以及安全性等因素，以满足业务发展和安全需求。

结束语

综上所述，医院计算机网络安全管理措施是保障医疗服务连续性和患者数据安全的重要基石。通过综合运用多种技术手段和管理措施，医院可以有效提升网络安全防护能力，降低潜在风险。未来，随着技术的不断进步和医疗信息化的深入推进，医院应持续关注网络安全领域的新动态，不断完善和更新安全管理措施，以适应新的挑战和需求，确保医疗信息系统安全稳定运行，为患者提供更加优质的医疗服务。

参考文献

[1]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,(08):86-87.

[2]张亚西.医院计算机网络安全管理研究[J].网络安全技术与应用,2020,(03):29-30.

[3]张丹丹.试论医院计算机网络安全管理维护工作的途径[J].网络安全技术与应用,2019,(10):112-113.

[4]魏昭民,苏闪闪.医院计算机网络安全管理措施[J].数字通信世界,2019,(06):64-65.