医院计算机网络的安全管理

王 冰 魏 博
宁夏医科大学总医院 宁夏 银川 750000

摘 要：医院计算机网络系统作为医疗体系的关键部分，其安全性至关重要。当前医院网络安全管理面临重视程度不够、使用者众多且安全意识参差不齐等挑战。网络攻击、数据泄露、系统故障是主要威胁。为加强安全管理，医院需建立完善的安全管理制度，明确职责和权限；采用先进的安全技术，如防火墙、入侵检测系统、加密技术等；并加强人员培训，提高安全意识。同时，医院应实施安全评估、制定安全管理计划、落实安全管理措施，并建立应急响应机制。

关键词：医院计算机；网络安全；管理研究

引言：随着医疗信息化的深入发展，医院计算机网络系统已成为现代医疗体系的核心支撑。然而，网络系统的安全性和稳定性却面临着诸多挑战。网络攻击、数据泄露、系统故障等威胁日益严峻，给医疗服务的连续性和患者数据的安全性带来了极大风险。因此，加强医院计算机网络安全管理显得尤为重要。本文将从现状、威胁、策略和实施步骤等方面，深入探讨医院计算机网络安全管理，为医院提供全面的安全管理指南，确保医疗服务的安全稳定运行。

1 医院计算机网络安全管理的现状

医院计算机网络系统作为现代医疗体系的重要组成部分，其安全性和稳定性直接关系到医疗服务的连续性和患者数据的安全性。随着医疗信息化的不断深入，医院计算机网络系统日益庞大和复杂，涉及到多个部门和科室，设备众多，管理难度也随之增加。当前，虽然许多医院已经建立了相对完善的计算机网络系统，但在安全管理方面仍存在诸多挑战和不足。（1）部分医院对网络安全的重视程度不够，这是医院计算机网络安全管理中的一个显著问题。网络安全不仅仅是技术问题，更是管理问题。一些医院在构建网络系统时，过于注重功能的实现和便捷性，而忽视了安全性的设计和管理。缺乏完善的安全管理制度和有效的安全防护措施，使得网络系统容易受到外部攻击和内部滥用。例如，没有定期更新和升级网络安全设备，没有建立严格的访问控制机制，没有制定应急响应计划等，这些都为网络安全漏洞的发生埋下了隐患。（2）医院计算机网络的使用者众多，这也是网络安全管理中的一个难点。医护人员、管理人员、患者等不同群体都在使用医院计算机网络系统，他们的计算机操作水平和安全意识参差不齐。一些医护人员可能缺乏必要的网络安全知识，容易成为网络攻击的靶点；一些管理人员可能忽视网络安全规定，违规操作导致数据泄露；一些患者可能不了解网络安全的重要性，随意连接医院网络，增加病毒传播的风险。这种多样性和复杂性使得医院计算机网络安全管理更加困难。（3）针对上述问题，医院需要采取一系列措施来加强计算机网络安全管理。一方面，医院应提高对网络安全的重视程度，将网络安全纳入医院管理的重要议程。建立健全的安全管理制度，明确各部门的职责和分工，确保网络安全工作的有序进行。同时，加大投入，引进先进的安全技术和设备，提高网络系统的防护能力。另一方面，医院应加强网络安全教育和培训，提高医护人员和患者的网络安全意识。通过定期举办网络安全知识讲座、开展网络安全演练等方式，增强大家的网络安全防范能力。同时，建立严格的访问控制机制，对不同用户进行权限管理，确保网络系统的安全可控[1]。

2 医院计算机网络面临的主要威胁

2.1 网络攻击

（1）网络攻击是医院计算机网络面临的最直接、最严峻的威胁之一。黑客们利用各种先进的技术手段，如网络扫描、漏洞挖掘、恶意软件传播等，对医院的计算机网络系统进行持续不断的窥探和攻击。他们的目标很明确：窃取患者信息、医疗数据等敏感信息，或者破坏医院的网络设备和系统，使医院业务陷入瘫痪。（2）网络攻击的手段不断翻新，攻击方式也越来越隐蔽。例如，通过钓鱼邮件、恶意链接等方式，黑客可以轻易诱骗医护人员点击，从而植入木马或病毒，进而控制整个网络系统。一旦医院网络系统被黑客攻破，不仅患者的隐私将受到严重侵犯，医院的正常医疗秩序也将受到极大干扰，甚至可能危及患者的生命安全[2]。

2.2 数据泄露

数据泄露是医院计算机网络面临的另一个严重威胁。医院作为医疗服务提供者，存储了大量的患者个人信息、医疗记录等敏感数据。这些数据一旦泄露，将给患者的隐私和医院的声誉带来不可估量的损害。数据泄露的原因多种多样，可能是网络攻击导致的非法窃取，也可能是内部人员违规操作造成的意外泄露，还有可能是设备故障导致的意外丢失。无论哪种原因，数据泄露的后果都是严重的。因此，医院必须加强对数据的安全管理，确保数据的保密性、完整性和可用性。

2.3 系统故障

系统故障是医院计算机网络面临的另一个重要威胁。医院的计算机网络系统运行环境复杂，设备众多，任何一个环节出现问题都可能导致整个系统无法正常运行。硬件故障、软件故障、网络故障……这些故障一旦发生，将直接影响医院的正常业务开展。系统故障不仅会导致医疗服务的中断，还可能造成数据的丢失或损坏。因此，医院必须建立完善的系统故障应急响应机制，确保在故障发生时能够迅速定位问题、排除故障，恢复系统的正常运行。同时，医院还应加强对系统设备的维护和保养，延长设备的使用寿命，减少故障发生的可能性。

3 加强医院计算机网络安全管理的策略和措施

3.1 建立完善的安全管理制度

建立完善的安全管理制度是加强医院计算机网络安全管理的基础和前提。医院应充分认识到网络安全的重要性，将网络安全管理纳入医院管理的整体框架中，制定详细、全面的网络安全管理制度。（1）医院应明确网络安全管理的职责和权限，确保各个部门和岗位都清楚自己在网络安全管理中的责任和义务。通过设立专门的网络安全管理岗位，负责网络安全的日常监管和应急响应，确保网络安全工作的有序进行。（2）医院应规范网络设备的使用和维护流程，确保网络设备的配置、更新和维护都符合安全标准。对于关键的网络设备，应实行严格的访问控制，防止未经授权的访问和操作。（3）医院还应加强对网络用户的管理和培训。通过制定网络使用规定，明确网络用户的行为规范，防止因网络用户的不当行为而导致的安全问题。此外，医院还应定期对网络用户进行网络安全培训，提高他们的安全意识和防范能力。（4）建立健全的安全审计机制也是加强医院计算机网络安全管理的重要环节。医院应对网络安全事件进行及时的记录和分析，通过安全审计日志等手段，追踪安全事件的发生原因和过程，以便及时发现和解决安全问题。同时，医院还应定期对网络安全管理制度的执行情况进行检查和评估，确保制度的有效实施[3]。

3.2 采用先进的安全技术

采用先进的安全技术是加强医院计算机网络安全管理的重要手段。医院应紧跟技术发展的步伐，引进和应用先进的安全技术设备，提高网络的安全防护能力。（1）防火墙是医院计算机网络的第一道防线。医院应配置高性能的防火墙设备，对网络流量进行实时监控和过滤，阻止非法入侵和恶意攻击。同时，医院还应定期对防火墙规则进行更新和优化，确保防火墙的有效性和适应性。（2）入侵检测系统是医院计算机网络的第二道防线。通过部署入侵检测系统，医院可以实时监测网络中的异常行为和攻击行为，及时发现并响应安全事件。入侵检测系统还可以与防火墙等安全设备联动，形成立体的安全防护体系。（3）防病毒软件是医院计算机网络不可或缺的安全工具。医院应部署全面的防病毒软件，对网络中的病毒、木马等恶意软件进行实时检测和清除，确保网络环境的清洁和安全。（4）医院还应采用加密技术对患者信息、医疗数据等敏感信息进行加密处理。通过加密技术，可以确保数据在传输和存储过程中的安全性和保密性，防止数据泄露和非法访问。

3.3 加强人员培训

加强人员培训是加强医院计算机网络安全管理的关键。医院应注重对医护人员、管理人员等网络用户的培训和教育，提高他们的计算机操作水平和安全意识。（1）对于医护人员和管理人员，医院应定期组织网络安全培训课程，向他们普及网络安全知识和操作技能。通过培训，使他们能够正确使用网络设备和系统，遵守网络使用规定，避免因操作不当而导致的安全问题。同时，医院还应鼓励医护人员和管理人员积极参与网络安全管理工作，共同维护网络的安全和稳定。（2）对于网络管理人员，医院应加强对他们的专业培训和技能提升。网络管理人员是医院计算机网络安全管理的核心力量，他们的专业素质和技术水平直接影响到网络的安全防护能力。因此，医院应定期组织网络管理人员参加专业培训课程，学习最新的网络安全技术和管理理念，提高他们的网络安全管理能力和技术水平。

4 医院计算机网络安全管理的实施步骤

4.1 进行安全评估

（1）安全评估是医院计算机网络安全管理的第一步，也是至关重要的一步。它旨在通过对医院计算机网络系统的全面审查，精准识别系统中存在的安全漏洞和风险。这一过程中，需要采用专业的安全评估工具和技术，对网络架构、系统配置、应用安全、数据安全等多

个维度进行深入分析。具体来说，安全评估应包括对网络拓扑结构的审查，以识别潜在的网络瓶颈和单点故障；对系统配置的检查，以确保系统设置符合安全最佳实践；对应用安全性的评估，以发现可能存在的应用漏洞和后门；以及对数据安全的审查，以确保数据的加密、备份和恢复机制健全有效。（2）安全评估的结果将为后续的安全管理策略和措施提供重要依据。通过评估，医院可以明确哪些区域是安全管理的重点，哪些漏洞需要优先修复，从而有针对性地制定安全管理计划，提高安全管理的效率和效果。

4.2 制定安全管理计划

根据安全评估的结果，医院需要制定详细的安全管理计划。安全管理计划是医院计算机网络安全管理的行动指南，应明确安全管理的目标、策略、措施以及实施步骤。在制定计划时，医院应充分考虑自身的业务特点、网络规模、安全需求等因素，确保计划的针对性和可行性。安全管理目标应具体、可衡量，如减少安全事件的发生次数、提高系统的恢复能力等。安全策略应明确如何防范、检测和响应安全威胁，如采用防火墙、入侵检测系统、防病毒软件等安全设备。安全措施则应具体列出需要实施的安全技术手段和管理措施，如定期更新系统补丁、加强用户访问控制等。同时，安全管理计划还应明确安全管理的责任和分工，确保各项安全管理工作能够落实到具体部门和人员。通过明确责任分工，可以形成合力，共同推进医院计算机网络安全管理的实施[4]。

4.3 实施安全管理措施

按照安全管理计划的要求，医院应逐步实施各项安全管理措施。这些措施应涵盖技术和管理两个层面，构建全面的安全防护体系。（1）在技术层面，医院应安装和配置必要的安全设备，如防火墙、入侵检测系统、防病毒软件等，以实时监控和防御网络攻击。同时，应加强网络用户的管理，通过身份验证、访问控制等手段，确保只有授权用户才能访问网络资源。此外，还应定期进行数据备份和恢复演练，以确保在数据丢失或损坏时能够及时恢复。（2）在管理层面，医院应建立健全的安全管理制度和流程，如安全审计、漏洞管理、事件响应等。通过制度化管理，可以规范医院计算机网络的使用和维护行为，提高系统的安全性和稳定性。同时，医院还应定期对安全管理措施的实施效果进行评估和改进。通过评估，可以及时发现并解决存在的问题，确保安全管理措施的有效性和持续性。

4.4 建立应急响应机制

除了日常的安全管理措施外，医院还需要建立完善的应急响应机制。应急响应机制是应对网络安全事件的重要保障，能够确保在发生安全事件时能够迅速、有效地进行处理。（1）医院应制定详细的应急响应预案，明确应急响应的流程和责任分工。预案应包括事件报告、初步处置、调查分析、修复恢复、总结评估等各个环节。通过预案的制定和演练，可以提高相关人员的应急处理能力和协作效率。（2）在应急响应过程中，医院应确保信息的及时传递和共享。通过建立有效的沟通机制，可以确保相关部门和人员能够及时了解事件的情况和处理进展，从而协同作战，共同应对安全事件。

结束语

医院计算机网络安全管理是保障医疗服务连续性和患者数据安全的关键。通过安全评估、制定安全管理计划、实施安全管理措施以及建立应急响应机制，医院可以构建起全面的安全防护体系。在此过程中，医院应充分认识到网络安全的重要性，加强人员培训，提高安全意识，同时紧跟技术发展的步伐，采用先进的安全技术设备。只有不断完善网络安全管理制度，加强技术防护和应急响应能力，医院才能有效应对各种网络安全威胁，确保计算机网络系统的安全稳定运行，为医疗服务的顺利开展提供有力保障。

参考文献

[1] 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（8）：129-130.

[2] 程鹏.医院信息化建设中计算机网络安全管理和维护[J].国际公关,2020（8）：204-205.

[3]李振宇.计算机网络信息安全及防护策略研究[J].网络安全技术与应用,2023（03）：153-154.

[4]陈金木,陈峰,郑少朋.高校计算机网络信息安全问题及其防范措施研究[J].网络空间安全,2023,14（01）：85-90.