医院信息化建设中网络安全防护策略分析

钱耀宇

（厦门市海沧区妇幼保健院，福建　厦门　361021）

摘　要：在医院信息化建设过程中，加强和落实网络安全防护工作，对于提升医院工作质量和信息安全具有非常重要的意义。现如今，医院的网络安全防护工作还存在一些有待进一步解决和优化的问题，比如网络安全问题、系统安全问题等。本文以医院信息化建设中出现的各种网络安全问题为入手点，探究如何加强医院网络安全防护，旨在能够为医院信息化建设发展提供一些有用的建议。

关键词：医院　信息化建设　网络安全　防护策略

中图分类号：TP393.08；R197.324　　**文献标识码：**A　　**文章编号：**1003-9082（2023）05-0007-03

现阶段，在我国社会主义现代化建设事业不断前进的时代背景下，各领域都呈现出欣欣向荣的景象，医疗行业就是其中之一。为了能够更好、切实有效地提高医院的医疗水平，需要迎合时代发展，落实信息化建设工作。在此过程中，首要任务就是领域保证网络安全，也只有这样才能够保证医院信息化建设的稳定性和高效性。

一、医院网络安全的重要性

医院网络安全的重要性不容忽视。医院作为重要的医疗机构，涉及大量的患者敏感信息和医疗机密，因此必须确保网络系统的安全性。从以下五个方面说明医院网络安全的重要性。

1.保护患者隐私和机密性

医院存储着大量的患者敏感信息，包括病历、身份证号码、社会保险号码等。如果这些信息被黑客攻击或泄露，将造成患者个人隐私的泄露，给患者带来严重的损害。

2.防止网络攻击

医院的网络系统面临来自内部和外部的各种威胁，包括病毒、恶意软件、勒索软件等。这些攻击可能导致医院网络瘫痪、数据丢失、系统崩溃等，严重影响医疗服务和医院的正常运营。

3.维护医疗机构的声誉

网络安全事故不仅给患者带来负面影响，还会损害医院的声誉。一旦发生数据泄露或其他安全事件，患者和公众对医院的信任度将大幅下降，可能导致患者流失和业务受损[1]。

4.遵守法规和法律要求

许多国家和地区都制定了相关的法律和法规来规范医疗机构的数据安全与隐私保护。医院需要确保网络安全，以遵守法律要求，并承担相应的责任和罚款。

5.保障医疗服务的连续性

医院网络系统的安全性也与医疗服务的连续性息息相关。如果网络受到攻击或遭受系统故障，可能导致医院无法正常提供病患诊疗，造成严重后果。

二、医院信息化建设中网络安全防护过程中常见的问题

1.网络安全问题

在医院信息化建设中，网络安全问题是一个常见的挑战。以下是一些常见的网络安全问题：第一，病毒和恶意软件。病毒和恶意软件是常见的网络安全威胁，它们可以通过电子邮件、可移动介质或恶意链接传播。医院需要使用有效的防病毒软件和恶意软件检测工具来防止这些威胁。第二，身份验证问题。医院网络系统应该有强大的身份验证机制，以确保只有授权的用户能够访问敏感信息和系统。但是，弱密码、共享账号、未及时撤销权限等问题可能导致未授权人员访问敏感数据。第三，数据泄露风险。医院存储着大量的患者个人敏感信息，这些数据一旦泄露，会导致患者隐私受到损害。因此，医院需要加强数据加密技术、访问控制和审计等措施，以减少数据泄露风险。第四，远程访问安全。随着医疗技术的发展，越来越多的医生和患者需要通过远程访问医院网络系统。然而，远程访问可能会增加网络安全风险，医院需要实施安全的远程访问机制，如VPN（虚拟专用网络）等。第五，安全意识培训。员工的安全意识对于预防网络安全问题至关重要。医院应该定期进行网络安全培训，教育员工识别和防范网络威胁，以减少安全漏洞的风险。

2.系统安全问题

在医院信息化建设中，系统安全问题是一个常见的挑战。以下是一些常见的系统安全问题。

第一，密码安全。密码是系统安全的第一道防线，但

许多用户常常使用弱密码或在多个系统中重复使用相同密码。这使得黑客猜测、破解密码的工作更容易。医院应该鼓励用户使用强密码，并定期更换密码。

第二，身份验证问题。弱的身份验证机制会导致未经授权的人员访问系统。医院应该采用强大的身份验证措施，如多因素认证和生物识别技术，以确保只有授权人员可以访问系统。

第三，软件和系统更新。没有及时更新软件和系统是一个常见的系统安全漏洞。医院应该确保及时下载和安装软件和系统的安全补丁，以修复已知的漏洞和弱点。

第四，数据备份和灾难恢复。没有足够的数据备份和灾难恢复计划可能导致数据丢失和系统瘫痪。医院应该定期备份数据，并测试和更新灾难恢复计划，以确保在系统故障或安全事件发生时能够快速恢复。

第五，授权和权限管理。不正确的授权和权限管理可能导致未经授权的人员访问敏感数据和系统。医院应该确保只有需要访问特定数据和系统的人员获得适当的授权和权限。

第六，系统监控和日志记录。缺乏系统监控和日志记录使得医院无法及时发现和响应安全事件。医院应该建立有效的系统监控和日志记录机制，以便快速检测和应对潜在的安全威胁。

第七，员工培训和安全意识。员工是系统安全的重要环节，他们需要接受定期的安全培训，提高对网络安全威胁的认识，并了解如何正确处理系统和数据，以避免安全漏洞的产生。

三、医院信息化建设中网络安全防护的有效策略

1.定期做好网络杀毒工作

一是使用权威的杀毒软件：选择一款权威的杀毒软件，并保持其及时更新。这些软件通常能够检测和清除病毒、恶意软件和其他威胁。二是定期扫描和更新：定期进行全面的系统扫描，确保所有设备和文件都被杀毒软件检测[2]。此外，及时更新杀毒软件的病毒库和程序版本，以获取最新的病毒定义和安全补丁。三是安全文件下载和传输：在下载和传输文件时要保持警惕。只从可信的来源下载文件，并使用安全的协议和加密方式进行传输，以防止病毒和恶意软件的传播。四是防火墙设置：配置和使用防火墙来限制对网络的未经授权访问。防火墙可以对传入和传出的网络流量进行过滤和监控，以防止攻击和非法访问。五是员工培训和意识提高：加强员工的安全意识和培训，教育他们如何识别可疑的邮件附件、网站链接和文件。员工应该知道如何处理和报告潜在的网络安全威胁。定期做好网络杀毒工作有助于减少病毒和恶意软件的传播风险，提高医院网络的安全性。但要注意的是，网络杀毒只是网络安全的一方面，还需要综合其他安全措施来全面保护医院网络系统的安全。

2.加强网络安全管理工作

第一，制定网络安全政策：制定明确的网络安全政策，明确规定用户对网络和系统的使用规范，规定安全措施和责任。确保所有用户理解并遵守这些政策[3]。第二，强化访问控制：建立严格的访问控制机制，将用户和用户权限分级，只给予必要的权限，并定期审查和撤销权限。采用身份认证、多因素认证等强化身份验证措施。第三，加强网络监控：建立有效的网络监控系统，对网络流量、日志和事件进行实时监控和分析。及时发现和响应异常行为和安全威胁，并采取必要的措施进行阻止和处置。第四，进行定期的安全漏洞评估和渗透测试：定期对网络和系统进行安全漏洞评估和渗透测试，发现潜在的安全风险和漏洞，并及时修补。第五，建立紧急响应计划：制定紧急响应计划，明确网络安全事件的处理步骤和责任。设立专门的安全团队来快速应对网络安全事件，并及时通知和报告相关的部门和当局。第六，加强员工培训和提高安全意识：确保员工接受定期的网络安全培训，提高他们对网络安全的认识，了解最新的安全威胁和应对措施。培养员工的安全意识，教育他们如何正确处理敏感数据和电子邮件。通过加强网络安全管理工作，医院可以提升整体网络安全水平，减少潜在的风险和威胁，保护患者隐私和机密性，确保医院信息化建设的顺利进行。

3.做好深度防护工作

做好深度防护工作是医院信息化建设中网络安全防护的重要策略之一。深度防护是指采取多种安全措施来保护网络和系统的安全，以提高防护能力和应对能力。以下是一些有效的深度防护策略：一是周密的网络安全架构设计：构建合理可靠的网络安全架构，包括网络分段、DMZ设置、入侵检测和防御系统等，以隔离网络流量和防止恶意攻击。二是强化边界防御：部署防火墙、入侵检测和防御系统（IDS/IPS）等边界安全设备，限制对外部网络的可访问性，并监控和阻止潜在的攻击流量[4]。三是使用安全性高的通信协议和服务：使用安全性较高的通信协议，如HTTPS、SSH等，以保护数据传输的安全。同时，限制使用不安全的服务，避免被利用进行攻击。四是安全审计和日志管理：建立安全审计和日志管理机制，记录网络和系

统的安全事件、用户活动和异常行为。定期审查和分析日志，及时发现和响应潜在的安全威胁。五是定期漏洞扫描和风险评估：定期进行漏洞扫描，发现和修复系统和应用程序中的漏洞。同时，进行风险评估，评估网络和系统的安全风险，并采取相应的措施加以防范。六是员工和用户教育：加强员工和用户的网络安全意识和培训，教育他们如何防范网络攻击和潜在的威胁，如避免点击垃圾邮件和病毒链接，保护个人账号和密码等。

4.定期进行数据备份

数据备份是将重要的数据复制到另一个存储介质，以便在数据丢失、系统故障或安全事件发生时能够快速恢复。第一，确定备份频率：根据数据的重要性和更新频率，确定备份的频率。一般而言，关键数据应该进行每日备份，而其他数据可以较少频繁备份。第二，选择适当的备份媒介：根据数据量和复制速度要求选择合适的备份媒介，如硬盘、磁带、云存储等。同时，确保备份媒介的可靠性和安全性。第三，分层备份策略：采用分层备份策略，即根据数据的重要性和访问频率进行层级化备份。常见的分层备份包括完全备份、增量备份和差异备份。第四，定期检查和测试备份数据：定期检查备份数据的完整性和可恢复性，确保备份的数据正常并能够顺利恢复。同时，进行恢复测试，确保备份过程和恢复过程的有效性[5]。第五，存储备份数据的安全性：备份数据存储介质应该具有一定的安全性措施，如加密、访问控制和离线存储等，以防止备份数据的泄露和损坏。第六，制定灾难恢复计划：制定详细的灾难恢复计划，包括备份数据的存储位置、备份和恢复流程、责任分工等。在发生数据丢失或系统故障时，能够快速有效地恢复数据和系统。

5.制定网络安全事故应急预案

制定网络安全事故应急预案是医院信息化建设中网络安全防护的重要策略之一。应急预案是为了在网络安全事故发生时能够及时、有效地对抗和应对，以减少损失并尽快恢复正常运行。第一，确定责任和组织机构：明确网络安全事故应急预案的责任人和责任部门，并建立专门的应急响应团队。这个团队应由技术专家、管理人员和安全人员组成，能够快速、有效地应对紧急情况。第二，分析风险和威胁：定期进行网络风险评估和威胁分析，识别可能的网络安全威胁和攻击方式。根据风险评估结果，制定相应的安全策略和相应措施。第三，定义网络安全事件响应流程：明确网络安全事件的分类和级别，并制定相应的应急响应流程。在不同的网络安全事件发生时，根据事先设定的流程进行应急响应和阻止进一步的影响。第四，建立与外部合作伙伴的联系：与执法部门、网络安全公司和其他合作伙伴建立联系和合作机制。及时汇报网络安全事件和威胁，共享信息和资源，加强应对能力。第五，提供员工培训和意识提高：定期组织网络安全培训和演练，增强员工的安全意识和应急响应能力。教育员工如何识别网络安全威胁，如何正确处理和报告安全事件。第六，定期测试和修订：定期对网络安全事故应急预案进行测试和演练，在实际操作中检验预案的可行性和有效性。根据测试结果和实际经验，修订和完善应急预案。通过制定网络安全事故应急预案，医院能够在网络安全事件发生时迅速响应和处理，最大限度地减少损失，并保障患者隐私和数据的安全。应急预案的制定和实施需要定期评估和更新，以应对不断变化的网络安全威胁。

结语

综上所述，在网络信息时代下，医院信息化建设步伐也逐步加快，但是也出现了很多安全隐患，而这些安全隐患正是新时代限制医院实现全面信息化发展的重要因素，会在无形之中破坏医院内部管理体系，同时让医院中各项医疗信息泄露，会让医院的医疗研究成果被窃取，甚至非法利用。想要有效提升医院在日常运行期间的质量与效率，便需要加大力度开展医院的信息化建设工作，医院网络安全的重要性不仅关乎患者隐私和机密性的保护，更关乎医院的声誉、合法合规和医疗服务的连续性。医院应该加强网络安全的投入和建设，并且全方位地做好网络安全防护工作，确保医院在实践当中更加优质地完成每一项工作，为患者提供更加优质的医疗服务。

参考文献

[1]黄彪.探究医院信息化建设中的网络安全与防护策略[J].网络安全技术与应用,2022(12):104-106.

[2]孙佩.医院信息化建设中的网络安全与防护研究[J].电子元器件与信息技术,2022,6(09):204-207.

[3]徐大志.医院信息化建设中的网络安全分析与防护[J].长江信息通信,2022,35(03):185-187.

[4]沈志伟.医院信息化建设中网络安全管理与防护的探讨[J].无线互联科技,2021,18(22):33-34.

[5]刘小宇,李璐.医院信息化建设中网络安全及防护的探析[J].网络安全技术与应用,2021(10):131-132.