文章类型：论文 刊号（ISSN）：2972-3469(P) / 2972-3507(O)

简析医院信息系统管理中的网络安全威胁与维护策略

李浩然
DOI:10.12238/irmet.v3i1.16760

[摘　要] 医院信息系统管理是医学与信息工程技术交叉应用的重要体现。目前医院信息系统中主要有医院日常运营时产生的绝大部分数据资料(例如病患就诊资料、科研档案资料以及财务数据等)。医院信息系统的可靠安全运行,能够保障相关数据处理工作的顺利实施,并且可以在提升从业人员工作效率与医院管理效率的同时,加强不同科室、医生护士以及不同部门与单位之间的联系。但是医院信息系统运行过程中,涉及到计算机与网络安全等诸多技术,因此存在不同的网络安全风险,所以为了确保医院信息系统的可靠运营,避免相关资料泄漏与遗漏,以及提升医护工作效率与增加医院管理效益,必须结合医院信息系统的运行现状问题,提出加强医院信息系统中的软硬件设备管理、结合实际优化网络资源配置与服务器、防范病毒以及严格访问限制等安全维护措施,旨在发挥医院信息系统在医院管理中的价值。
[关键词] 医院信息系统；网络安全；威胁；维护；策略
中图分类号：TU246.1　文献标识码：A

A Brief Analysis of Network Security Threats and Maintenance Strategies in Hospital Information System Management

Haoran Li

[Abstract] Hospital information system management is an important manifestation of the cross application of medicine and information engineering technology. At present, the hospital information system mainly includes the vast majority of data generated during the daily operation of the hospital, such as patient visit information, scientific research archives, and financial data. The reliable and secure operation of hospital information systems can ensure the smooth implementation of relevant data processing work, and can strengthen the connection between different departments, doctors and nurses, as well as different departments and units, while improving the work efficiency of practitioners and hospital management efficiency. However, during the operation of the hospital information system, many technologies such as the Internet are involved, so there are different network security risks. Therefore, in order to ensure the reliable operation of the hospital information system, avoid the leakage and omission of relevant data, and improve the efficiency of medical care work and increase the efficiency of hospital management, we must combine the current problems of the operation of hospital information, propose security maintenance measures such as strengthening the management of software and hardware equipment in the hospital information system, optimizing the network resource allocation and servers, preventing viruses, and strict access restrictions, in order to give play to the value of the hospital information system in hospital management.
[Key words] hospital information system; Network security; Threat; maintain; strategy

数字化时代,医院正逐步迈向信息化、智能化,医院信息系统已深度融入到日常医疗的方方面面。它极大地便利了医护人员工作,让患者就医体验得以改善,比如线上预约挂号节省了排队时间,电子病历方便医生查阅历史诊疗情况等。并且医院信息系统的安全运行对于现代医院的正常运营有着重要价值,其能够对医院运营过程中产生的数据资料进行科学管理,有效提升了医生护士的工作效率和医院的数据资料管理效率。

1 医院信息系统与网络安全的概述

1.1医院信息系统的概述。(1)涵义。信息系统建设是促进现代医院建设管理发展的主要举措,其有利于提升医院的相关管理工作效率和促进医院发展。医院信息系统作为数字化管理系统,其主要是运用先进的现代化技术(网络技术、通信技术、大数据技术、计算机技术等),对医院经营活动产生的数据资料实施收集、整理、分析与应用等管理(包括医生护士的人事管理、

药品采购及其管理、病患就诊的医疗管理、医学科研资料以及医院基建等),简而言之就是对医院经营过程中的人、物、财等相关信息资料进行管理,从而提升医院管理工作开展的效率与效益。(2)构成。医院信息系统主要是由计算机硬件系统、软件系统与网络系统等构成,其可靠运行,能够对医院数据资料(主要包括医生护士、就诊病患以及医学科研等信息档案)开展科学管理,使医院的数据资源得到共享,并且加强了不同科室、不同部门和单位之间的联系,从而为医院在开展医疗诊治活动与医学研究等方面提供数据参考。但是医院信息系统在实际运用过程中,由于受到诸多因素的影响(比如制度、作业人员、设备、病毒以及网络等),有可能造成医院产生的数据资料信息丢失、不完整等现象,使其存在很多安全问题,同时给不法人员留下了窃取相关数据的安全漏洞,严重影响了医院数据安全及其社会经济效益,还制约了医疗诊治工作的有效实施,并且威胁到医学科研工作的进展。

1.2网络安全的概述。信息化技术的快速发展,促进了网络技术的不断进步,同时网络安全也变得日益重要。基于信息化时代的网络安全对于社会大众的正常生产生活影响非常大,甚至关系到国家安全与管理。所以新时代的民众都需要了解网络安全的内涵及其特征。网络安全是利用先进的科学技术和不同措施,对有关网络系统的数据资料安全实施保护,防止其丢失。现阶段危害网络安全的原因比较多,比如自然原因(比如水灾、地震等)、人为原因(比如人为失火造成的灾害、不法人员制造病毒和黑客攻击等),因此需要结合相关原因,采取有效措施开展安全维护。

2 医院信息系统网络安全面临的主要威胁

2.1外部恶意攻击威胁。随着互联网的普及运用,医院信息系统面临着来自外部的诸多恶意攻击威胁。黑客群体出于不同目的,常常将医院信息系统视为攻击目标。其中,黑客可能会发起分布式拒绝服务攻击(DDoS),通过控制大量僵尸网络向医院服务器发送海量请求,导致服务器资源被耗尽,系统无法正常响应,进而瘫痪,使医疗业务陷入停滞。另外,黑客还会运用高级持续威胁(APT)手段,长期潜伏、隐秘收集医院信息系统中的敏感数据,如患者隐私信息、医院内部的科研成果等,一旦得手,便会造成严重的信息泄露后果。

2.2内部潜在风险威胁。医院信息系统面临的网络安全威胁不仅来自外部,内部潜在风险同样不容忽视。一方面,内部工作人员可能存在因操作不规范而引发的安全问题,比如医护人员在使用信息系统时,由于安全意识不足,随意下载不明来源的软件,或者误操作删除重要的数据文件,这都可能破坏系统的正常运行,甚至造成关键数据丢失。另一方面,尽管是少数情况,但也存在部分内部人员出于私利等不良动机,故意违反信息系统使用规定,滥用权限去访问、篡改或泄露患者的隐私信息以及医院机密资料。

3 医院信息系统管理中的网络安全维护措施

3.1病毒防范的安全维护策略。病毒是黑客与域外势力侵袭医院信息系统网络安全的主要手段,其安全防范措施一般包括:第一,对医院信息系统的内网和外网进行分隔,同时应用相关系统对其实时检测与查杀,防止病毒侵袭问题;第二,制订相关防范制度,及时对医院产生的数据资料实施检测,运用先进设备和技术措施,提高防火墙运行速率,以保障系统运行安全;第三,依据相关要求,做好数据的加密工作,比如字段加密要求、动态管理密钥等,同时要结合实际状况完善加密形式,从而保证医院信息系统网络安全。

3.2软硬件设备管理的安全维护策略。结合医院信息系统的实际运行状态,依据医院资产管理的相关条例,结合设备的性能、经济性以及应用要求,做好老化设施的替换工作,确保软硬件设备运行时的网速与网络安全。(1)硬件安全维护管理。医院信息系统网络安全的硬件设施一般包括服务器、机房、网线等,其安全维护管理目的是保证其可靠运行以及防止其发生故障。安全问题的原因一般是设施老化以及自然灾害影响(水灾、雷电等),因此在安全维护管理时,需要结合不同原因,做好检测工作。同时结合相关设备的安全管理特点和实际状况,采取对应的技术措施,比如安装保险设备。如果是硬件设施老化现象,就有可能影响网络信号强度,因此需要对其进行替换,以达到信息系统网络安全运行目的。(2)软件维护管理。医院信息系统一般包含数据库、传输和操作系统等软件。医院信息系统软件是域外势力和黑客侵袭的重点,其被侵袭将严重威胁到医院产生的各种资料安全。实施软件维护管理工作,首先要运用最新的病毒检测系统,建立健全防火墙,并对其发现的病毒实施查杀,确保网络安全维护管理成效。同时需要及时升级修补软件系统,了解其可能存在的网络安全风险,做好医院数据资料的储存与处理工作,对医院的重要数据(比如医学科研档案资料等)实施高规格的加密手段,以确保医院信息系统安全。

3.3加强系统漏洞监测与修复。定期开展全面漏洞扫描,精准定位潜在风险。定期运用专业的漏洞扫描工具对医院信息系统的各个层面,包括操作系统、数据库、应用程序等进行全面扫描,有助于及时、精准地发现隐藏的安全漏洞,为后续修复工作提供可靠依据,从而有效预防外部攻击利用这些漏洞入侵系统。例如,每月安排固定时间,使用像Nessus这类功能强大的漏洞扫描工具对医院信息系统展开全面检测。首先,在不影响医院正常医疗业务运行的前提下,配置好扫描工具的参数,使其能深入到操作系统层面,检查Windows Server 或Linux系统是否存在未及时更新补丁导致的已知漏洞,比如是否存在可被远程利用的缓冲区溢出漏洞等。对于数据库方面,检测MySQL或Oracle数据库的版本及配置情况,查看是否存在弱口令、权限设置不合理等安全隐患。针对各类医疗应用程序,扫描其代码中是否有可被黑客利用的逻辑错误漏洞。扫描完成后,工具会生成详细的漏洞报告,清晰地列出发现的漏洞名称、所在位置、风险等级等信息,方便后续进行针对性修复。及时跟进漏洞修复,确保系统处于安全状态。在发现系统漏洞后,迅速组织专业技术人员依据漏洞的严重程度和相关特点制定修复方案,并及时实施修复操作,更新

软件版本、安装补丁等，保障医院信息系统能够持续稳定且安全地运行，避免因漏洞未修复而遭受网络攻击。例如，当通过漏洞扫描发现某医疗应用程序存在SQL注入漏洞（一种可被恶意利用来篡改或窃取数据库中数据的漏洞）后，技术人员会第一时间进行分析评估。确定其严重程度为中等级别后，马上查阅该应用程序官方发布的漏洞修复指南以及对应的补丁文件。接着，在医院信息系统的测试环境中先进行补丁安装测试，验证是否会影响应用程序的正常功能以及与其他系统组件的兼容性。经过反复测试确保无误后，选择在医院业务低谷时段，比如凌晨时段，对正式运行的该应用程序部署补丁，完成修复工作，并再次进行检测确认漏洞已被成功修复，以此保障系统的整体安全性，防止因这一漏洞被攻击者利用而引发数据泄露等安全事故。

3.4严格网络访问控制。利用访问控制列表（ACL）精准限制访问权限。访问控制列表（ACL）是强化网络访问控制的重要手段，通过它可以根据不同用户、部门以及业务需求，精准地限制对医院信息系统各资源的访问权限，避免非授权访问，保障系统安全。例如，在医院信息系统中，对于医疗影像存储系统，可利用ACL进行权限设置。首先，将医院内不同科室划分为不同的用户组，比如影像科为一组、临床科室为一组、行政科室为一组。影像科作为主要操作和管理影像数据的部门，赋予其对影像存储系统的读写权限，可上传、查看、修改影像资料等；临床科室则仅赋予读取权限，方便医生查看患者影像辅助诊断；而行政科室鉴于工作关联性不大，限制其访问该系统。这样能有效控制不同主体对关键系统资源的访问，防止因权限混乱造成的数据泄露或误操作风险，确保影像存储系统安全地服务于医疗工作。采用虚拟专用网络（VPN）保障远程访问安全。随着医院业务拓展，医护人员远程办公、远程会诊等需求增多，采用虚拟专用网络（VPN）技术能为远程访问医院信息系统构建安全通道，确保在公网环境下的数据传输安全，防止外部非法截获与入侵。例如，当医护人员因外出或在家需要远程访问医院内部的电子病历系统时，通过使用VPN进行连接。医护人员先在自己的终端设备（如电脑、手机）上安装医院授权的VPN客户端，输入个人专属的账号和密码进行登录认证。登录成功后，终端与医院信息系统之间建立起加密的虚拟专用网络通道，所有传输的数据都会经过加密处理，即使在公网传输过程中被截取，第三方也无法获取其中的内容。

4 结束语

综上所述，随着互联网技术在社会不同领域的普及应用，使得信息系统已然在现代医院得到充分运用。现代医院信息系统管理的从业人员都会采取不同技术措施开展网络安全防护，比如建立防火墙、采买安全软件、设置病毒检查与防范系统等，上述技术措施可以防控大部分的网络安全。然而基于信息技术的持续进步，使得威胁网络安全的方式方法越来越多且复杂多变。并且由于医院数据资料的重要程度，以及不法人员与域外势力长期威胁着医院信息安全等现状，所以医院信息系统面对的网络安全现状呈现非常严峻的态势，因此医院信息系统管理的从业人员需要结合其运行实际，采取相应的技术措施做好网络安全维护，从而保证医院正常运营。

[参考文献]

[1]侯均,王野平.试析医院信息系统的网络安全管理与维护措施[J].网络安全技术与应用,2020(12):156-157.

[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(08):204-205.

[3]容甘泉.医院信息系统的网络安全维护探讨[J].信息与电脑,2021(06):236-238.

[4]魏玮.医院信息系统的网络安全与维护[J].计算机与网络,2021(01):53.

[5]吴兵.医院信息网络安全管理与维护策略[J].电脑知识与技术,2021(11):51-53.

[6]许顺生.医院信息系统的管理与网络安全[J].科学与信息化,2023(6):159-161.

[7]周扬.医院信息系统的网络安全与威胁应对[J].电子乐园,2023(3):0034-0036.

[8]张敬国.医院信息系统的网络安全维护措施[J].集成电路应用,2023,40(2):156-157.

[9]时亚松.医院信息化建设中的网络安全管理与维护[J].中国信息界,2024(2):84-85.

[10]刘杰.医院信息系统中的网络安全管理思路研究[J].科学与信息化,2023(11):184-186.

[11]梁景翔.医院计算机网络信息系统的安全风险与控制研讨[J].电脑爱好者(普及版),2023(4):106-108.