◁信息管理▷

智慧医院建设背景下医院网络安全闭环管理模式研究

李宽省，李家栋，张栩，丁睿
（贵州医科大学附属医院，贵阳市 550000）

【摘要】 智慧医院建设背景下，医院在网络安全方面存在着诸多的风险点，一定程度上阻碍智慧医院的建设与发展。对此，笔者分析医院网络安全问题的成因及其困境，萃取关键的四个要素形成闭环管理策略的核心要素，并构建网络安全闭环管理架构，支撑网络安全闭环管理模式及对策措施的探讨，以期为解决智慧医院建设中面临的网络安全问题提供一些借鉴。

【关键词】 智慧医院；网络安全；闭环管理
【中图分类号】 R197　【文献标识码】 B　【文章编号】 1672-4232(2024)02-0110-04
【DOI编码】 10.3969/j.issn.1672-4232.2024.02.031

国家卫健委于2019年3月、2020年5月、2021年3月，相继发布了《医院智慧服务分级评估标准体系（试行）》《进一步完善预约诊疗制度加强智慧医院建设的通知》《医院智慧管理分级评估》，智慧医院建设的其他配套相关政策与指导文件也陆续印发。在国家政策的鼓励引导和大力支持下，“服务、医疗、管理”三位一体的智慧医院的建设进入高速发展时期。医疗大数据支撑着智慧医院发展，大量医疗数据联通各个系统平台及便捷服务应用程序，如电子病历、医学影像、检查检验等诊疗数据，电子健康档案、个人体检、日常健康体征等个人健康数据，基因组学、蛋白组学等生物数据，这些数据与患者隐私、医疗行为、医学研究紧密相关[1]。

尤其随着面向患者的智慧服务的各项应用的不断拓展到移动互联网，更多的医疗数据走出医院封闭的内网环境。移动互联网医疗通过移动终端或互联网提供医疗健康服务，由于移动终端应用安全保障机制和系统纵深防御不足，导致其面临新的安全风险挑战[2]。虽各方高度重视，但我国医疗行业网络安全仍处于工作起步较晚、整体风险较高、防护水平相对落后的局面，网络安全形势不容乐观[3]。

医院网络安全人才缺乏、等保落实不到位、风险应对被动等问题突出，探索建立一套闭环的网络安全管理机制，从而建设完善并激活调动网络安全防护设备及措施、测评体系、问题处置机制，并在良性的动态循环中解决各类网络安全问题，将成为有效的途径。

1　医院网络安全问题成因及困境

智慧医院的快速发展，导致病毒攻击、黑客入侵、数据泄露、系统篡改等网络安全攻击事件越来越多，网络安全存在的问题也更加凸显，主要有如下几个方面。

1.1　网络安全资金投入不足

工信部明确提出电信等重点行业网络安全投入占信息化投入比例不低于10%，推动能源、金融、卫生医疗等行业领域加强资产识别、设备防护、边界防护、身份认证、数据安全、应用安全等技术手段建设，提升重要系统、关键节点及数据的安全防护能力[4]。调查显示，相对于2019—2020年度，中国医院安全类在信息

[4] 陈思远，陈涛.微信平台在基层胸痛中心院外急救中的应用[J].中国急救复苏与灾害医学杂志，2019，14(1)：33-35.
[5] 郎云丽，王克福，张霞，等.医护一体化联合微信平台在胸痛中心急救患者中的应用[J].齐鲁护理杂志，2019，25(18)：68-70.
[6] 马懿，石蓓，许官学，等.胸痛诊疗远程信息平台对胸痛中心医疗效率的影响与临床决策分析[J].中华老年医学杂志，2019，38(2)：141-146.
[7] Srivastava J，Routray S，Ahmad S，et al. Internet of medical things (iomt)-based smart healthcare system：trends and progress[J].Comput Intell Neurosci，2022，2022：7218113-7218113.
[8] Redón P，Shahzad A，Iqbal T，et al.Benefits of home-based solutions for diagnosis and treatment of acute coronary syndromes on health care costs：a systematic review[J].Sensors，2020，20(17)：5006-5006.
[9] 中华医学会心血管病学分会，中华心血管病杂志编辑委员会.急性ST段抬高型心肌梗死诊断和治疗指南(2019)[J].中华心血管病杂志，2019，47(10)：766-767，783.
[10] 步涨，徐峰.PDCA结合信息化创伤复苏时间轴管理的质量控制在严重创伤救治中的应用[J].医学研究生学报，2021，34(9)：897-901.
[11] 沈红健，杨鹏飞，张磊，等.信息化流程管理系统在急性缺血性卒中救治中的构建及应用[J].中国脑血管病杂志，2018，15(5)：225-230.

通信作者：吴燊荣(1984-)，男，硕士研究生，助理研究员；研究方向：医疗质量管理、医院感染管理、卫生管理研究。
收稿日期：2023-01-05
修回日期：2023-02-22　（编辑　曹晓芸）

化建设中的投入占比由9.43%下降到了8.56%[5]。在医疗网络安全形势愈加严峻的形势下,网络安全资金的投入还需持续保持一定占比、稳定有效地投入。

1.2　等级保护工作落实不均衡、不到位

调查报告显示,三级医院通过等保三级评测比例为86.40%,三级以下医院通过等保二级以上评测比例为58.46%,三级以下医院开展等级保护工作情况明显低于三级医院[5]。对网络安全等级保护备案系统的等级和数量进行统计后发现,超过50%的医院有二级和三级网络安全保护备案系统,但是通过二级和三级等保备案的系统数量以仅有1个的居多[5]。

由此来看,等级保护工作存在两个主要问题:一是三级及三级以下医院之间,等级保护工作落实不均衡,整体落实还不到位;二是医院一般具有HIS、电子病历、PACS、LIS等多个核心系统,系统定级备案与应定级备案情况,存在较大差距。

1.3　专业技术人才缺失

据有关资料统计,到2022年我国重要行业网络安全人才需求达到210余万人,目前,我国网络安全专业人才缺口预估在50万以上[6]。调查显示,医院信息技术人员队伍也在不断壮大,但总体情况仍然不容乐观,医院信息技术部门的职工数量在10人以下的占比仍超过六成[5]。医疗行业中,网络安全专业人才是具有交叉学科知识的复合型人才,涉及计算机、通信、密码、管理等学科,相对于计算机相关专业更加缺乏。培养并配备网络安全专业技术人员,才是网络安全工作长治久安的根本。

1.4　网络安全防护设备及措施部署不够

调查显示,大多数医院都具有多种网络安全防护设备及措施,采用率超过50%的主要有防火墙、入侵检测、网闸、数据库审计、堡垒机、漏洞扫描、用户网络行为审计、VPN设备、终端接入控制,仍有极少数医院未采用任何网络安全防护设备和措施[5]。

为落实等保2.0要求,医院需准确开展网络安全等级保护的定级,尤其是核心业务信息系统、数据中心平台等。按照“一个中心,三重防御”的安全保障体系,需要部署相应的安全防护设备及措施,如计算机环境安全需部署堡垒机、PKI系统、权限与口令管理、系统审计、数据库审计、防病毒网关、非授权禁止等技术设备及措施[7]。

对比等保2.0要求,医院网络安全防护设备及措施明显存在着不完善、不充分问题。网络安全产品的配备不足使得网络攻击者能够轻而易举且不被察觉地入侵医疗信息系统,成为信息泄露、勒索病毒频现的重要原因[3]。

1.5　商用密码应用评估有待进一步推广

线上预约及查询、远程健康监测、远程诊疗、互联网医院等开放的智慧医疗服务应用,促使“封闭式”医疗服务走向“开放式”卫生健康服务,网络边界逐渐模糊。医疗信息包含大量敏感数据,在收集、存储、传输过程中若未实施有效的加密措施,信息将处于极大的泄露风险中[3]。随着云计算、物联网、大数据、人工智能等新业态的出现,密码技术的应用成为保障系统安全不可缺少的手段,但是就目前来看,密码应用范围和程度还不够广泛和深入[8]。

1.6　缺乏网络安全系统化管理

缺乏闭环的系统化的管理方式,通过静态式、基础性的安全防护设备部署,被动式开展等保测评,单点式问题处置,粗放地应对互联网空间的新风险和挑战,将无法满足智慧医疗背景下网络安全的工作要求。依托有效的管理机制,以人员调度为中心,统筹网络安全各类资源并形成良性循环,将会为应对挑战提供重要帮助。

2　网络安全闭环管理的策略要素

引入社会技术服务力量,将院内与院外网络安全资源分类整合,形成闭环管理的重点要素,利用各要素的作用属性,彼此之间建立互相作用、相辅相成的关系,从而形成主动式、动态式、整体式、精准式的网络安全良性循环,不断完善提升网络安全水平。笔者将网络安全闭环管理的要素分为四个部分:人员、技术设备、测评评估、安全运维。

2.1　人员

人员要素包括医院的网络安全和信息化管理委员会(以下简称“网信委”)、专家小组、网络安全和信息化管理委员会办公室(以下简称“网信办”),网信办一般设在信息部门,由信息部门的各领导及信息中心网络安全相关人员承担相关工作职能,其中网络安全专管人员在其中承担关键工作。

2.2　技术设备

技术设备主要指网络安全防护设备及措施,医院常用的主要有防火墙、入侵检测、网闸、数据库审计、堡垒机、漏洞扫描、用户网络行为审计、VPN设备、终端接入控制、病毒防护、态势感知、WAF、密码技术等。

医院需按照等保2.0的要求,部署相对完善的安全设备及措施体系,建立医院网络安全防御屏障,主动抵御外界的各类安全攻击。同时,这也是医院网络安全建设必不可少,也是最为关键的技术投入。目前,网络安全设备及措施相对成熟,需要不断更新升级的是设备的策略及病毒库、特征库等数据库,采用更加适应网

络安全建设需求的措施。

2.3　测评评估

测评评估主要包括信息系统等级保护测评、商用密码评估、日常风险评估、网络安全性检测评估、攻防演练等。随着网络安全形势的不断变化，测评评估的种类也在增加，如自2020年启动并快速发展的商用密码评估、定期化的风险评估服务等。但是，测评评估体系仍然以信息系统等级保护测评为主，商用密码评估、风险评估、网络安全性检测评估等为辅，攻防演练、代码审计等措施为补充，减少漏洞短板，降低风险点。

当前，测评评估活动主要包括准备、方案编制、现场实施、报告编制等活动。通过能力验证活动，及时发现问题，采取相关纠正措施，对质量控制起到补充完善作用，不断提高质量管理水平，保障测评活动的高质量开展[9]。

2.4　安全运维

安全运维主要包括资产管理、安全加固、内外网病毒防护、重保及应急响应等。如安全加固，包括漏洞加固与配置加固。根据安全漏洞扫描、等保测评监测结果等，对应用系统、操作系统、数据库、中间件、网络设备、安全设备等开展查漏补缺的安全整改优化。根据安全配置核查结果，对以上加固对象开展配置完善优化。病毒防护方面，一般以终端安全管理系统为支撑工具，针对医院内外网终端进行统一安全体检，进行打补丁、恶意代码过滤、病毒木马查杀、运维管控，从而保障终端的安全运行。另外，与边界防火墙联动，配置安全准入策略，防御病毒入侵。

3　构建网络安全闭环管理模式

闭环管理模式，坚持以人员为中心，科学有序调动技术设备、测评评估、安全运维三要素形成闭环和动态循环机制，即技术设备建立安全防御体系、测评评估发现防御漏洞、安全运维进行有效加固及复测，通过不断迭代进化，提升安全防护能力与水平，具体情况见图1。

4　网络安全的保障措施及对策建议

4.1　保障资金投入并获取专家技术支持

在医院网络安全管理机构中，面向网信委、网信办、专家小组，网络安全专管人员需及时汇报网络安全

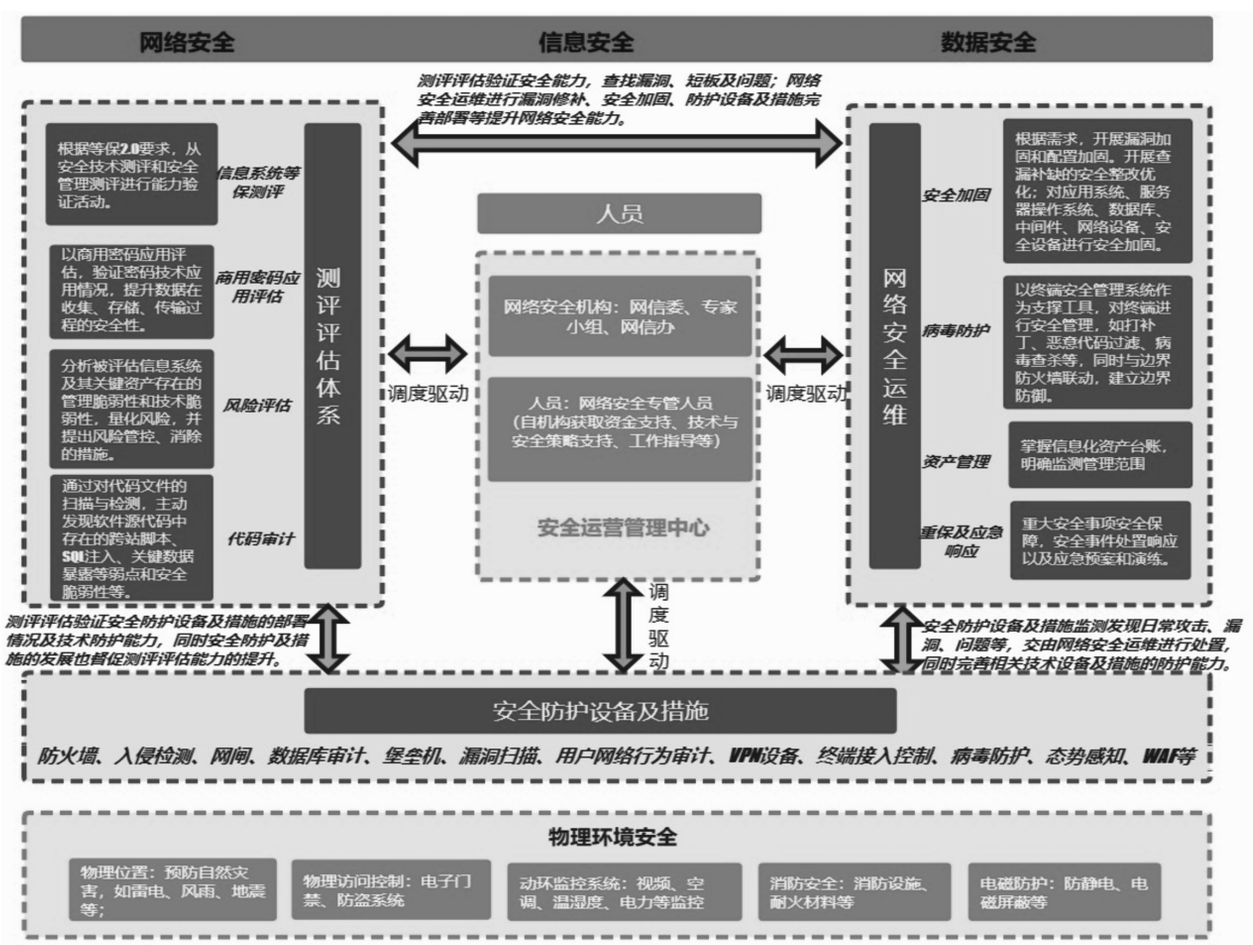

图1　网络安全闭环管理架构图

整体情况、重点工作推进进度、工作计划落实情况等，同时积极争取资金投入、获取技术与安全策略支持、得到工作指导等。面向信息化其他人员、网络安全设施设备及措施、技术服务单位及人员等，网络安全专管人员需围绕“一个中心”即安全运营中心，使用资金投入、技术支持、工作指导等为其高效运作注入强大动力，管理调动各类资源，实现“评估与监测—补足弱项与问题处置—安全能力提升—评估与监测”的动态循环。

4.2　等保测评由政策性强制转向主动性开展

目前，等级测评工作的政策强制性较强，测评需求旺盛，但以政策驱动的等级测评模式是不能保持持久的[9]。网络安全闭环管理中，测评评估作为三大支柱之一，促使医院主动利用等保测评进行能力验证活动，从而要求并鼓励测评机构通过引入新工具、新设施以及配备专职渗透测试人员等方式提高测评质量，为被测单位提供更为有效、切实可行的整改建议，保障测评活动的高质量开展，降低医院网络安全风险。

4.3　系统化运营管理中培养专业技术人才

新的网络安全形势，对网络安全技术人员的复合型能力需求越来越高。在医疗信息化人才都缺乏的背景下，医院可在信息化人员中选拔，确立稳定、可靠的专管人员，通过安全运营管理中心，依托闭环管理的工作机制，在技术设备、测评评估、安全运维动态循环运作的环境中，提升专职人员的管理能力，促使深入学习网络安全防护设备及措施的使用管理，逐步掌握测评评估的工具及原理，并通过引入的安全运维服务类社会专业技术力量实时了解网络安全市场最新的技术及动态，从而以切实、高效、灵活的工作实践，培养出自己的网络安全专业人员。同时，利用社会专业技术力量，可以进一步弥补医院网络安全技术能力的不足，为人才的培养提供机会与环境，以应对未来更高的网络安全风险与挑战。

4.4　测评评估完善设备部署

高质量开展等保测评活动，将真正起到督促完善安全设备及措施部署的目标。等保测评活动测评内容包括安全技术与安全管理测评，其中安全技术测评包括安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心等5个方面的安全测评，将按照等级保护要求对网络安全设备技术及措施进行能力验证，督促完善相关技术设备及措施的配备，并提出存在病毒库、特征库等相关数据库的更新问题，管理软件的升级情况以及相关策略的配置建议。

4.5　“以评促用”推广商用密码应用

公安部发文要求，第三级以上网络运营者应在网络安全等级测评中同步开展密码应用安全性评估[10]。《“十四五”全民健康信息化规划》要求，构建卫生健康行业网络可信体系，全面推广商用密码应用，完善卫生健康行业商用密码应用体系[11]。政策法规与智慧医院建设下的网络安全风险挑战，共同驱动医院把密码技术与管理作为医疗信息安全保护的必要手段。通过商用密码应用评估标准，检验医院密码保护能力，并提出密码技术应用的相关方案与建议，进而提升医院在数据安全保护方面的商用密码应用的方向与范围。

针对智慧医院建设背景需求下，医院面临的网络安全风险，笔者分析了网络安全问题的成因及其困境，从四个核心要素的角度，构建网络安全闭环管理架构，实现封闭式、粗放型、静态化的安全管理。同时，有针对性地探究了网络安全的保障措施及对策建议。该研究能够驱动网络安全技术的应用，构筑网络安全防护屏障，对智慧医院的建设与发展提供了一些建议和思考。

参　考　文　献

[1] 秦盼盼，谢莉琴，陈荃，等.基于健康医疗大数据的分级诊疗实施路径研究[J].中国医院管理，2021，41(6)：75-78.

[2] 中国软件评测中心.移动互联网医疗安全风控技术白皮书(2021)[EB/OL].(2021-12-09).http://www.cstc.org.cn/info/1060/233057.htm.

[3] 中国软件评测中心.医疗行业网络安全白皮书(2020)[Z].(2021-03-25).http://www.cstc.org.cn/__local/3/BD/97/6233 0015CE2AC84CCD253DFC8FF_5C0384C9_942CA.pdf? e=.pdf.

[4] 工信部.网络安全产业高质量发展三年行动计划(2021—2023年)(征求意见稿)[EB/OL].(2021-07-12).https://www.miit.gov.cn/gzcy/yjzj/art/2021/art_34f89fff961b4862bf0c393532e2bf63.html.

[5] 中国医院协会信息专业委员会.CHIMA发布：2021-2022年度中国医院信息化状况调查报告[EB/OL].(2023-02-22).https://www.chima.org.cn/Html/News/Articles/16012.html.

[6] 齐丽钰.企业网络安全人才培养的探索与实践[J].网络空间安全，2022，13(6)：109-114.

[7] 王晓丽，丁月红，陆昊，等.保2.0要求下医疗网络安全建设与管理研究[J].中国数字医学，2020，15(12)：5-9.

[8] 中国软件评测中心.商用密码应用安全性评估白皮书(2021年)[EB/OL].(2021-09-10).http://www.cstc.org.cn/info/1060/231336.htm.

[9] 王云丽，韩珍珍，杨文焕，等.网络安全等级保护测评机构建设与发展探讨[J].河北省科学院学报，2023，40(1)：36-41.

[10] 公安部.贯彻落实网络安全等级保护制度和关键信息基础设施安全保护制度的指导意见[EB/OL].(2020-09-22).https://www.mps.gov.cn/n6557558/c7369310/content.html.

[11] 国家卫生健康委员会.关于印发“十四五”全民健康信息化规划的通知[EB/OL].(2022-11-07).http://www.nhc.gov.cn/guihuaxxs/s3585u/202211/49eb570ca79a42f688f9efac42e3c0f1.shtml.

通信作者：李家栋(1970-)，男，本科，副主任医师；研究方向：医院管理、信息化管理。

收稿日期：2023-04-04

（编辑　马兰）