

医院信息安全建设探索

吴前兵

刘 静

程西雅

(安徽省第二人民医院 合肥 230000)(安徽艾瑞贷信息技术服务有限公司(安徽医科大学 合肥 230000)
合肥 230000)

〔摘要〕 介绍等级保护 2.0 新标准要求变化,以安徽省第二人民医院为例阐述医院信息安全当前存在的问题并提出应对策略,包括总体安全规划、组织管理体系、制度建设、具体防护措施等方面,有助于降低安全风险。

〔关键词〕 等级保护 2.0 标准;医院信息安全;安全策略

〔中图分类号〕 R-056 〔文献标识码〕 A 〔DOI〕 10.3969/j.issn.1673-6036.2020.08.012

Exploration on Hospital Information Security Building WU Qianbing, Anhui NO. 2 Provincial People's Hospital, Hefei 230000, China; LIU Jing, Anhui Airuidai Information Technology Service Co., Ltd, Hefei 230000, China; CHENG Xiya, Anhui Medical University, Hefei 230000, China

〔Abstract〕 The paper introduces the changes of the new standard requirements of classified protection 2.0. Taking Anhui NO. 2 Provincial People's Hospital as an example, it expounds the problems existing in the information security of the hospital and puts forward countermeasures, including the overall security planning, organization and management system, system building, specific protection measures, etc., which can help reduce the security risks.

〔Keywords〕 classified protection 2.0 standard; hospital information security; security strategy

1 引言

信息系统及网络设施的安全性直接关系到医疗工作正常进行,一旦网络出现问题或数据泄漏丢失将会给医院带来巨大损失。医院信息系统保存大量患者私密信息,其泄漏和非法传播将会给医院、社会 and 患者带来风险^[1]。根据《中华人民共和国网络安全法》规定,国家实行网络安全等级保护制度。针对医疗卫生行业,原卫生部先后发布《关于全面

开展卫生行业信息安全等级保护工作的通知》以及《卫生行业信息安全等级保护工作的指导意见》^[2],明确要求全国所有三甲医院核心业务信息系统的安全保护等级原则上不低于第 3 级,等级保护成为医院信息安全建设重要标准^[3]。随着云计算、移动互联网、大数据、物联网、工业控制等先进技术的不断涌现和发展,原标准体系难以满足新形势下网络信息安全等级保护工作的需要,标准的适用性、可操作性需要进一步完善,“等保 2.0”应运而生^[4]。2019 年 5 月 13 日公安部正式发布等保 2.0 相关标准并于 2019 年 12 月 1 日开始实施。安徽省第二人民医院为安徽省三甲医院,高度重视医院信息系统安全建设,积极探索和实践符合新标准的安全解决

〔收稿日期〕 2020-03-16

〔作者简介〕 吴前兵,硕士,中级工程师,发表论文 1 篇。

方案，以切实提升整体信息系统及数据的安全性，为医院核心业务系统如医院信息系统（Hospital Information System, HIS），实验室信息管理系统（Laboratory Information Management System, LIS），影像存储与传输系统（Picture Archiving and Communication Systems, PACS）等建设一个稳定、安全的运行环境。

2 新标准变化及差距分析

2.1 新标准变化

2.1.1 概述 与旧标准体系相比，2.0 标准统一了基本要求与设计要求的安全框架，包括通信网络、区域边界、计算环境，充分体现“一个中心，3 重防护”的纵深防御思路，强化可信计算安全技术要求应用^[5]。

2.1.2 原“信息系统”调整为“定级对象” 新标准体系下，定级对象不仅包括原有基础信息网络和信息系统，范围进一步扩展到云计算平台、大数据平台、物联网和工业控制系统等新技术应用对象。

2.1.3 可信验证技术细化到每个等级需求中 要求针对计算资源构建保护环境：1 级是系统引导程序与系统程序，2 级是重要配置参数与应用程序 + 审计记录，3 级是应用程序重要执行环节，4 级是应用程序所有执行环节。

2.1.4 安全要求调整为通用和扩展要求 安全通用要求针对共性化保护需求提出，不管等级保护对象形态如何，必须响应保护等级的要求，安全扩展要求针对云计算、移动互联、物联网和工业控制系统等个性化保护需求提出，对应特定技术或特定应用场景^[6-7]。

2.1.5 统一安全技术规划思路 通过确定保护对象边界划分安全需求，按照纵深防御设计物理环境、通信网络、网络边界、主机设备、应用和数据多层次的技术防护措施，通过安全管理中心实现安全检测、日常管理、事件处置和分析取证的集中化管控^[8]。

2.2 差距分析

安徽省第二人民医院核心业务系统满足基于

1.0 标准的 3 级等保要求，具有良好的安全防护措施，但依然存在一定问题，与新标准要求仍然有一定差距，具体体现在以下 4 方面：一是终端主机安全性存在安全漏洞易被人攻击，应对登录口令、服务进程、系统补丁、防病毒软件等进行加固升级。二是核心数据均采用本地备份机制未采用异地备份，在条件允许情况下可采用异地备份，在本地机房出现灾难性事故情况下数据不丢失。三是部分设备缺乏有效冗余备份机制，存在一定单点故障隐患。安全区域划分不够明朗，对安全区域和边界防护措施未完全达到等保 2.0 标准。应明确区域划分，提高安全技术防护措施能力。四是安全技术防护措施缺乏有效监管，无安全管理平台，无法感知整个网络态势。需建立安全管理中心，实时监控网络状态。

3 建设策略

3.1 制定总体安全框架

对照等级保护 2.0 标准新要求，根据第 3 方专业测评公司意见和建议，邀请行业专家结合医院系统、网络、管理和相关制度实际情况进行探讨和分析，充分论证的基础上制定针对性强、切实可行的信息安全总体规划和框架，见图 1。

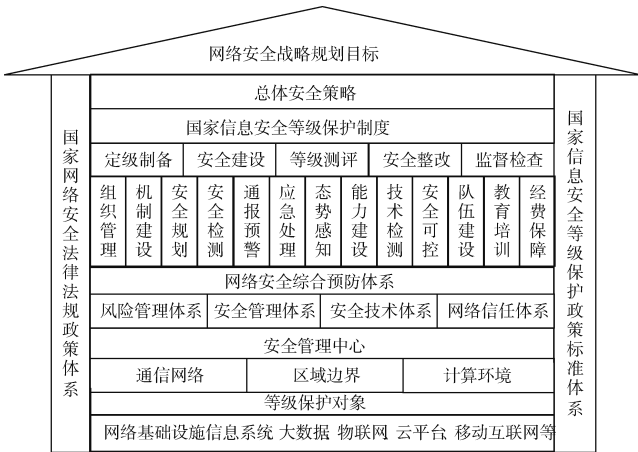


图 1 等级保护 2.0 安全框架

3.2 成立组织管理体系

信息安全建设推进需要专门的组织保障。为明

确网络信息安全责任、保证信息化建设稳步发展，医院需成立信息安全领导小组，由一把手担任领导小组组长。领导小组统筹规划网络安全，建立信息安全管理体系，完善各项管理制度和技术标准，保障信息安全工作正常开展。领导小组下设信息安全

工作组，一般设在信息中心，由信息中心主任担任组长，成员由信息中心人员构成。工作组根据要求建立自己的信息安全组织架构，完成领导小组布置的任务，确保安全措施和各项工作有序开展，保证医院网络安全稳定运行，见图 2。

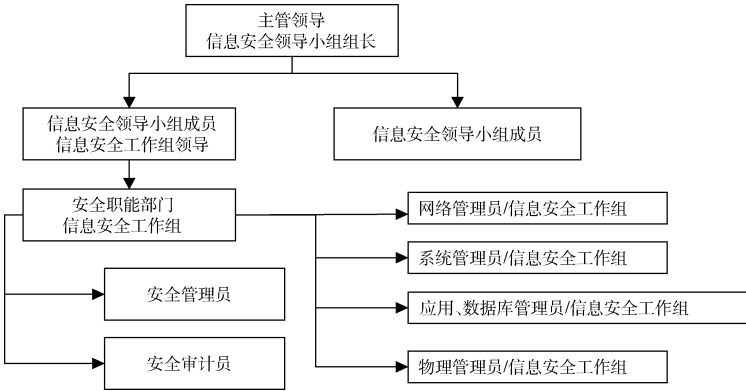


图2 医院信息安全组织架构

3.3 规范制度建设和文档管理

信息安全建设必须坚持“技术与管理并重，3分技术+7分管理”的原则^[1]。2.0 版本标准要求定级对象建立信息安全管理组织机构，制定明确的安全策略、管理制度和工作流程。对照 2.0 版本标准要求，医院制定相应信息安全管理总体策略和方针，指导安全管理工作正常开展。通过 4 级文件分级管理、查漏补缺机制，完善和修订多项管理制度，保证制度建设和管理的合规性，见图 3。

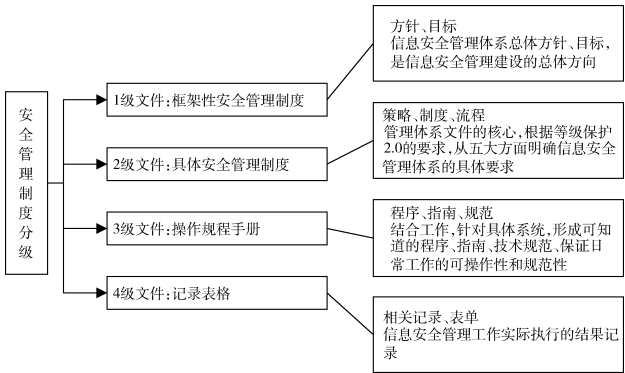


图3 安全管理制度与文档建设

3.4 强化安全防护措施

3.4.1 提升安全物理环境 物理环境是网络安全

的基石，等级保护标准要求医院机房建设至少达到 C 级，其位置选择和建筑结构能够保障设备不被外界环境干扰和危害，具有防雷、防噪声、防电磁干扰、防火、防静电、防尘、防水、防盗等措施，同时需要部署精密空调保证机房温湿度在标准范围内。增加不间断电源（Uninterruptible Power Supply，UPS）等设备，保证机房设备在市电停电情况下可继续运行，提高机房续航能力。建立机房环境监控平台，实时监控机房环境状态。使用视频监控系统和门禁系统，对出入机房人员进行管理控制。通过为机房配置完善的基础设施，降低物理环境安全风险，提高安全性，保障网络、主机和业务的连续性。

3.4.2 加固安全通信网络 安全通信网络要求进行总体规划和详细设计，完善网络拓扑，对关键链路建立冗余，优化配置，提高传输速率，定期进行设备和线路巡查，排除隐患，使用防火墙、网络加密、鉴别和访问控制等安全防护技术提升网络稳定性和安全性。在业务优化访问方面，通过应用负载均衡网关选择最优访问路径，应用交付控制器实现应用性能优化，为大流量业务系统提供高可靠性冗余能力，提升服务器、带宽效率和用户体验，提高系统可用性和业务连续性。

3.4.3 明确划分安全区域 根据“1个中心,3重防护”解决方案,医院需要按照差异性的业务类型和功能划分安全域,确定各安全域的物理边界和逻辑边界,明确不同安全域之间的信任关系。在安

全域边界配置不同安全策略,体现不同防护强度,加强访问控制和攻击检测力度,实现安全域之间隔离与防护,为业务运行创造更安全可靠的环境,见图4。

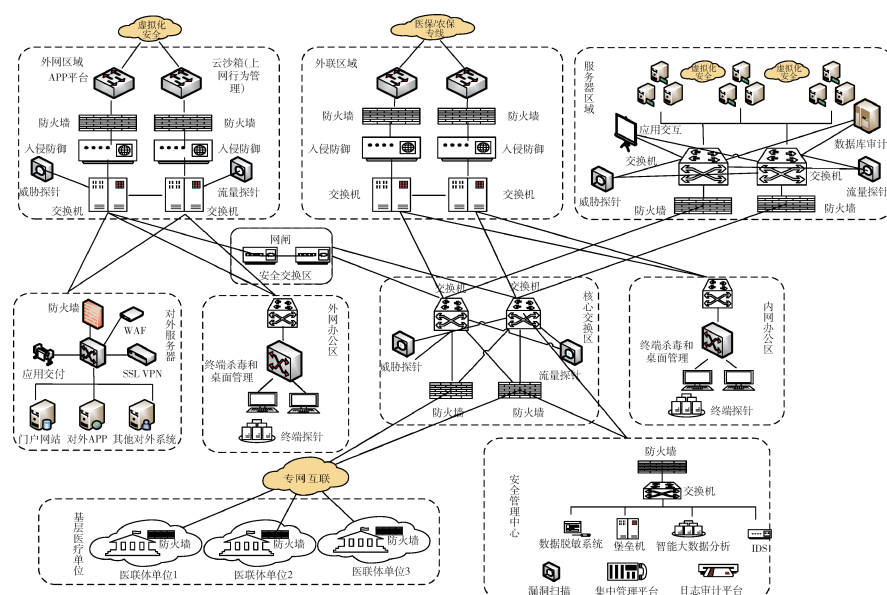


图4 医院安全区域防护解决方案

(1) 外网区域安全防护策略。部署下一代防火墙、入侵防御 IPS (Intrusion Prevention System) 设备,对进出网络的数据进行 L2 - L7 层安全检测,有效防御来自内外网的分布式拒绝服务 (Distributed Denial of Service, DDoS) 攻击、应用层等攻击;同时在外网交换机镜像部署流量/威胁探针,通过和安全管理中心管理平台联动,实现对网络内东西南北流量分析,让管理员直观了解当前网络风险态势。(2) 外联区域及医疗单位接入区域安全防护策略。部署下一代防火墙设备、入侵防御 IPS 设备,综合运用病毒过滤、入侵防护等技术提供综合性安全防护和检测能力。(3) 服务器区域安全防护策略。配置反病毒 (Anti Virus, AV) /IPS 等功能模块,实现对应用层攻击过滤;在虚拟化内部部署安全防护软件,实现对虚拟化内部的可视、隔离防护作用,搭建虚拟化平台,满足云计算区域边界环境访问控制、入侵防范、安全日志合规性要求;部署数据库审计与防护设备,对操作数据库的行为进行有效审计,实时监控、识别、阻断外部黑客攻击以及来自内部高权限用户的数据窃取行为;部署防毒

墙网关对进出网络内部的数据进行检测,发现病毒立即采取手段进行隔离或查杀,保护网络内进出数据安全;部署操作系统漏洞扫描和补丁设备,定期对服务器和网络操作系统进行扫描,根据结果对漏洞进行分析,对高危漏洞立即修复,减少潜在危险。(4) 对外服务器区域安全防护策略。在对外服务器区域边界部署下一代防火墙设备,实现对进出流量进行精细化的策略管控功能;部署防边界部件检测系统、Web 应用防火墙设备和安全日志审计系统,实现对外业务系统安全防护,有效抵御针对 Web 类的攻击;部署应用交付设备提供对超文本传输安全协议 (Hyper Text Transfer Protocol over Secure Socket Layer, HTTPS) 站点的安全套接层协议 (Secure Sockets Layer, SSL) 卸载能力,减轻站点性能压力;部署内外网隔离设备网闸,在内外网之间建立特殊协议传输通道,既可实现内外网之间数据传输,又能实现内外网之间的物理隔离,保障核心业务网络服务器安全。(5) 核心交换区域安全防护策略。核心交换区关键设备和链路做冗余以提高业务容错能力;镜像模式部署流量/威胁探针,通过和

安全管理中心管理平台联动实现对网络内东西南北流量的分析,让管理员直观了解当前网络风险态势;部署入侵检测和防御系统,对流经的每个报文进行深度检测,实现事前危险分析和阻断;部署网络审计设备,对用户操作行为进行记录和跟踪审计,实现事后追踪功能。(6) 内外网办公区域安全防护策略。以代理模式部署终端探针设备,通过与安全管理中心管理平台联动,实时分析监控终端风险态势;在办公区域电脑安装杀毒软件和桌面管理软件,实现对终端设备防护和安全策略设置,保证办公区域环境安全。

3.4.4 优化安全计算环境 安全计算管理要求在系统、应用和数据方面进行全面防护,对不同业务系统与安全风险划分不同虚拟局域网 (Virtual Local Area Network, VLAN),通过设置访问控制、建立身份鉴别、提供安全审计、配置入侵防范、部署恶意代码防范和设备防范措施、进行资源有效控制,对数据进行备份和恢复,定期进行应急预案演练,保证医院数据安全,提高系统可用性。

3.4.5 建立安全管理中心 基于安全技术要求,部署安全管理平台、大数据分析平台,提供有效的集中安全管理及大数据分析,降低用户运维管理成本。综合运用全局性日志管理、统一策略管理、设备状态集中监控、监控数据汇总和报表统计等手段,解决网络安全状况不直观、管理混乱、响应慢、故障定位难等问题,为医院管理提供全面的解决方案,同时满足安全管理中心集中管控的合规性要求。

3.5 加强网络安全保障

为确保医院信息系统处于安全环境之中,应强化队伍建设、教育培训、经费保障和应急预案 4 方面措施。一是配备高技术人才作为坚强后盾,队伍建设要合理、多元化,根据网络安全要求划分不同类别和级别的技术人员。二是加强专业技术培训,提高人员网络安全意识,提升专业技能和应急处置能力,提高医院整体网络信息安全水平。三是提供经费保障用于网络维护以及设备投入和更换,这是医

院网络信息安全健康发展的永续动力。四是应急预案的制定和演练可提高突发事件处置能力,确保在发生危险时可及时控制并快速恢复正常。依据应急演练过程中发现的问题及时完善应急流程,为医院正常业务运行创造安全、稳定、可靠的网络环境。

4 结语

医院信息安全没有绝对性,随着时间推移,管理理念、信息技术以及医院信息化程度的不断变化,医院等级保护建设需与时俱进。新标准的发布与实施一方面带来挑战,另一方面也是切实提升医院安全能力的机会。本文根据等级保护 2.0 新标准要求,分析医院当前存在的问题与差距,制定相应应对策略,提出建立“基于 1 个中心的多重防护体系”,一定程度上消除技术薄弱和管理疏忽环节,降低安全风险,为医院后续开展基于 2.0 标准 3 级等保工作提供支撑。

参考文献

- 1 魏勤,刘艳亭,郭敬鹏,等.基于三级等保标准的医院信息安全体系建设实践[J].医学信息学杂志,2019,40(2):35-39.
- 2 夏冰.网络安全法和网络安全等级保护 2.0[M].北京:电子工业出版社,2017.
- 3 韩作为.医院信息安全等级保护三级建设流程与要点[J].中国数字医学,2013,8(9):37-39.
- 4 高员,黄晓昆,李秀伟.等保 2.0 时代云计算安全要求及测评实践[J].信息安全研究,2018,4(11):25-30.
- 5 何占博,王颖,刘军.我国网络安全等级保护现状与 2.0 标准体系研究[J].信息技术与网络安全,2019,38(3):9-14.
- 6 蔺旭冉.等保 2.0 标准技术要求浅析与初步实践思考[J].网络安全技术与应用,2019(10):12-14.
- 7 王斯梁,冯暄,蔡友保,等.等保 2.0 下的网络安全态势感知方案研究[J].信息安全研究,2019,5(9):828-833.
- 8 杨晨柳,方安,朱峰,等.基于三级等保的信息安全体系构建研究[J].网络安全技术与应用,2019(8):2-4.