医疗机构信息安全探析

周 毅 潘 敢 殷 鸣

（湘潭市中心医院信息科 湘潭 411100）

〔摘要〕 以湘潭市中心医院为例，指出其信息安全存在的问题，从安全策略和管理制度、安全管理机构和人员、安全建设与运维管理、物理和环境安全、网络和通讯安全等方面详细阐述医院信息安全整改措施，提高管理水平。

〔关键词〕 信息；网络；安全；医疗机构

〔中图分类号〕R－056 〔文献标识码〕A 〔DOI〕10.3969/j.issn.1673－6036.2019.05.009

Discussion and Analysis on Information Security of Medical Institutions *ZHOU Yi, PAN Gan, YIN Ming, Information Department, Xiangtan Central Hospital, Xiangtan 411100, China*

〔**Abstract**〕 Taking Xiangtan Central Hospital as an example, the paper point out problems about its information security, detailedly elaborates on measures to better the hospital's information security from the perspectives of security strategies and management mechanism, security management institution and personnel, security building and maintenance management, physical and environmental safety, network and communication security and so on, so as to improve management level.

〔**Keywords**〕 information; network; security; medical institutions

1 引言

迅速发展的网络[1]通讯技术在带给人们极大便利的同时也隐藏着种种危机。2017 年 6 月国家正式实施网络安全法，其中明确规定实行网络安全等级保护制度，要求按照网络安全等级保护制度履行安全保护义务，保障网络免受干扰、破坏或未经授权的访问，防止网络数据泄露或被窃取、篡改。

2018 年 2 月湖南省某医院由于受到勒索病毒[2]的攻击，系统瘫痪 1 天。2016 年 7 月香港卫生署信息系统遭黑客入侵，近 10 万人受影响。2015 年美国第 2 大医疗保险公司 Anthem 遭黑客入侵，8 000 万用户数据遭泄露，同年美国 UCLA 医院遭黑客入侵，450 万份医疗记录遭泄露。医疗行业逐渐成为黑客入侵的高危行业，信息安全[3]必须引起高度重视，做好信息安全工作是医疗行业安全工作的重中之重。三甲医院核心业务保护等级应不低于 3 级。

2 现状及存在的问题

针对信息安全和等保评级，为更清楚地了解信息安全工作现状和最新动态，邀请有专业资质的评测公司对医院信息安全工作进行彻底全面的评估。经评估在安全管理和安全技术[4]方面存在不足，在信息安全方面与 3 级等保要求和自身业务安全需求还在一定差距。第一，安全管理方面，只有普通的信息化相关制度，缺乏专门、体系化制度，包括顶层信息安全管理策略[5]方针、细化的管理制度和流

〔收稿日期〕 2018－11－06

〔作者简介〕 周毅，高级工程师，发表论文 10 篇。

程、外包服务安全管理制度，外包开发系统上线前未进行安全评测。第二，安全技术方面，信息安全基础设施投入不足，没有入侵检测系统、日志审计系统等安全防护设备，多个服务器、中间件、数据库及应用系统存在弱口令，存在入侵攻击风险、服务器补丁更新不及时、漏洞等隐患[6]。

3 整改措施

3.1 概述

针对评测结果给予高度重视，湘潭市中心医院组织科室全体人员学习上级整改意见，参照《信息安全技术 网络安全等级保护基本要求》[7]，见图 1，结合自身实际进行全面整改。

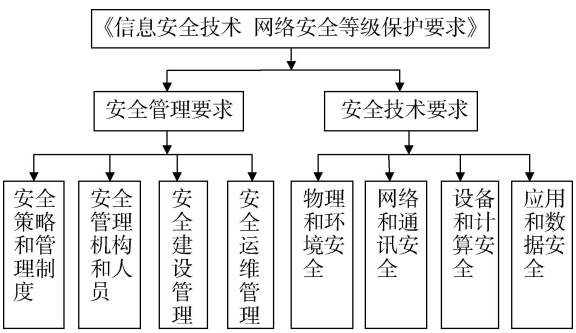

图 1 信息安全技术 网络安全等级保护要求

3.2 安全策略和管理制度

明确“统一领导，责权明确，技管并重，重点防护”的思想。新增和修订《系统管理规定》、《数据管理规定》、《网络管理规定》、《用户管理规定》、《信息系统应急预案》、《外包项目管理规定》，这些制度和章程的确立使管理更加规范。

3.3 安全管理机构和人员

成立以主管院长为组长的信息安全管理领导小组，涵盖部门，见图 2。小组制定信息安全工作总体方针和安全策略，全面负责信息网络安全建设和重大信息网络安全突发事件的应急处理。通过设置该机构能够协调和调动全院资源实施信息网络安全规划，组织应急演练和处置。领导小组配备专职安全、系统、网络、数据库管理员，由专职安全管理员[8]加强与公安网监和市网信办的联络。对人员权限进行清理，对长期闲置账号予以注销，对权限过大的账户进行变更，与关键岗位人员签署岗位责任和保密协议。

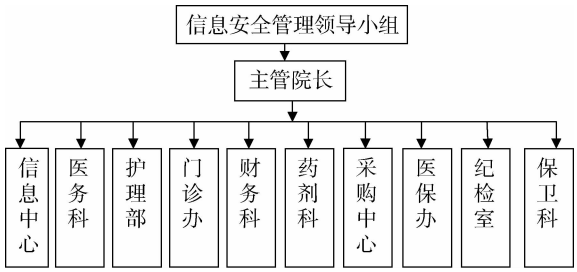

图 2 信息安全管理领导小组

3.4 安全建设管理

根据使用系统的不同和重要性分别划分各部门的保护边界和安全等级并向主管部门和公安机关报批和备案，将等保工作细化。对购入的信息安全产品要求供应商出具权威测评机构的测试报告给院方，要求软件开发单位提供源代码，以审查[9]软件中是否存在已知的后门和隐蔽信道，在上线前进行安全测试。

3.5 安全运维管理

对机房安装门禁，严格机房出入管理并加装监控摄像头，对机房人员活动实时监控。对官方发布的漏洞和风险即时采取必要措施并记录在案。将全院所有计算机进行交换机端口的绑定并将计算机地理位置登记造册，录入自主研发的 IP 登记系统以便于管理，任何没有在交换机上绑定的计算机不能接入内网。所有需开通互联网的计算机应出具书面报告，交领导签字认可并纳入上网行为管理范畴。重新清理网络设备，对设备具体型号、软件组件、版本信息建立科室台账，重新绘制网络拓扑结构图。对原有的备份方法进行优化处理，增加备份方式以提高数据安全性。细化《信息系统应预案》中启动预案的条件、处理流程、恢复流程、事后总结和培训规定，规定每半年举行 1 次多部门合作应急演练[10]。

3.6 物理和环境安全

对现有机房设施进行整改，对机柜、服务器、UPS 等设备加装防雷保护器。将物联网技术加入到药品和试剂冷链系统平台上，实时采集温湿度数据形成报表，超过设定阀值立即发送短信至机房管理员。将原来 3 000 伏安的 UPS 换成 10 000 伏安，达到接入更多设备和供电更长时间的目的。

3.7 网络和通讯安全

在原来 HP 3 层核心交换机基础上增加迈普核心交换机形成网络核心冗余。根据服务器角色的重要性对网络进行安全域划分，在内外网的安全域边界设置访问控制策略，配置到具体端口，禁用不必要的端口。在交换机上添加策略，禁止使用 3 389 和 445 端口。防火墙按照第 1 层基于 IP 的访问控制，第 2 层基于用户身份的访问控制[11]。设置策略控制非法登录次数和超时退出。远程管理使用加密协议 SSH。定期升级特征库。设置字母、数字、符号相叠加的复杂口令并定期更换。在网络边界处部署入侵防护手段，防御并记录入侵行为，对网络中的用户行为日志和安全事件信息进行记录和审计，对安全设备、网络设备和服务器进行集中管理。

3.8 设备和计算安全

实行系统分级管理，操作系统和数据库系统特权用户分离，由不同管理员管理特权。重命名系统默认账户，对权限严格限制并修改口令。采用旁路接入的方式部署数据库审计系统，深度解析访问行为，记录操作人用户名、操作时间、主机名、IP 地址、客户端软件名称等，便于追溯。旁路阻断非授权访问，灵活识别可疑操作并即时短信告警，确保日志安全存储、稳定可靠。操作系统遵循最小安装原则，仅开启需要的服务，安装需要的程序和组件，最大限度降低系统遭受攻击[12]的可能性。建设信息集成平台，监控服务器的 CPU、内存、硬盘和网络资源使用情况。

3.9 应用和数据安全

应用安全策略限制单用户不能同时多点登录，配置应用根据不同用户的资源使用优先级分配系统资源[13]。利用校验和加密技术保证数据在传输和存储过程中的完整性和保密性。对重要信息系统在原来 IBM 双机的基础上再加上 DG 实现异地容灾。

4 结语

习总书记指出“没有网络安全就没有国家安全”，网络安全已经上升为国家战略高度。针对网络安全需要树立动态的综合防护理念。从最初的收费管理到当前的临床大数据，越来越多的医院业务[14]正依靠信息网络技术运行。内外网的融合加大医疗信息的潜在威胁，来自于内外网的大量信息[15]交互使医院信息系统面临日益严重的安全威胁。医院信息系统等级保护测评提供一种良好、具有标准化参考价值的依据，通过定级、备案、建设整改、等级评测以及策划 - 实施 - 检查 - 改进（Plan - Do - Check - Adjust，PDCA）循环迭代的改造，使医院的安全边界更加牢固、安全策略更加可靠。等保是功能的要求，不是设备的罗列，医院信息系统整体安全目标的实现除必要的安全技术手段外还需有相适应的安全管理体系，只有管理和技术并重才能不断提升医院安全管理水平，从而实现为公众提供安全、高效的医疗卫生服务这一目标。

参考文献

1 孟晓阳，朱卫国，李连磊，等. “互联网 +”对医院信息系统安全的挑战与对策探讨［J］. 医学信息学杂志，2016，37（12）：38 - 41.
2 党雷胤，梁利. 关于勒索病毒引起的企业信息安全思考［J］. 电脑知识与技术，2017，13（26）：52 - 53.
3 张智龙. 计算机网络信息安全及其防护对策探讨［J］. 电脑知识与技术，2017，13（21）：25 - 26.
4 付佳伟，海洛德·辛博贝，徐文渊，等. 勒索软件_ 我们如何爬出泥沼［J］. 中国医疗设备，2017，32（7）：167 - 168.

（下转第 47 页）

3.5 数据库审计与加密

3.5.1 数据库保护的重要性 2017 年数据泄露事件数量持续上升，且泄露的数据总量创历史新高。2017 年 3 月公安部破获一起重大数据泄露事件，京东网络安全部试用期员工非法获取用户账号、密码、身份证、电话号码、物流地址等重要信息 50 亿条。2017 年 4 月优酷上亿条用户信息被公开叫卖，售价仅 300 美元。数据库是商业和公共安全中最具有战略性的资产，通常用来保存重要的商业伙伴和客户信息，这些信息需要被安全保护以防止竞争者和非法者获取。针对层出不穷的数据泄露事件，引入数据库审计和加密系统。

3.5.2 数据库审计 数据库审计系统实时监测并记录用户对数据库的各类操作行为。利用探针的方式获取网络中用户操作数据库的行为，记入审计数据库中，对各种风险进行及时预警（如 SQL 注入、违规操作、批量数据泄漏或篡改、违规登录风险），通过对数据库行为的记录、分析和汇总协助客户事后生成合规报告、事故根源回溯，提高数据资产的安全性。

3.5.2 数据库加密 加密系统基于透明加密技术（对数据真正使用者透明）对数据库中的敏感数据进行整列加密存储，这样即使数据库被不法分子窃取，其获取到的数据也无法查看的。

4 结语

目前长沙市第一医院在格凡安信公司的协助下已经完成网络安全保护方案的网络脆弱性扫描、数据安全网关、数据库审计、数据库加密各产品部署，从网络、操作系统、核心数据库、数据共享及上层应用层面出发，全方位保护院内医疗信息化系统、核心数据、医生和患者信息安全。

参考文献

1 王小群，丁丽，李佳，等. 2017 年我国互联网网络安全态势综述［J］. 保密科学技术，2018（5）：4－11.

2 张远林，刘冰. 医院信息系统的数据及网络安全［J］. 医学临床研究，2008（10）：1891－1893.

3 陈华智，张闻，张华磊. 网络安全等级保护实施方案的设计及应用实践［J］. 浙江电力，2011，30（3）：54－57.

4 张磊. 网络安全等级保护技术实现与分析［J］. 电子世界，2018（7）：186－187.

5 傅钰. 网络安全等级保护 2.0 下的安全体系建设［J］. 网络安全技术与应用，2018（8）：13，16.

6 沈晓利，郭璞，樊红彬. 医院网络安全体系构建与实现［J］. 网络安全技术与应用，2017（11）：132，134.

（上接第 43 页）

5 李忠俊，张永峰，宋波. 企业信息安全应对策略探讨［J］. 电脑知识与技术，2017，13（21）：36－37.

6 孟晓阳，朱卫国，黄迎萍，等. 医院网络渗透测试与数据包分析技术实践［J］. 中国卫生信息管理杂志，2017，14（6）：838－842.

7 孙巍，王玉珍，陈韬. 基于等级保护要求 加强医院信息安全管理［J］. 中国卫生信息管理杂志，2017，14（6）：843－845.

8 郭景泰，方愉舒. 计算机信息系统安全问题及其解决措施［J］. 微型机与应用，2017，36（22）：8－10.

9 苏玉成，汪爱勤，张亚娜，等. 医院数据库审计实现方法［J］. 医疗卫生装备，2016，37（9）：69－71.

10 张勇，王佳研，杨凯. 浅谈医院信息系统故障应急演练［J］. 中国医疗设备，2016，31（9）：152－153，158.

11 孙辉，赵颖波，李晶晶，等. 浅析医务工作者对临床数据安全的认知［J］. 中国数字医学，2017，12（6）：82－84.

12 廖彦深. 信息安全等级保护定级的方法与应用［J］. 电脑知识与技术，2017，13（3）：45－46.

13 沈超. 医院信息安全管理［J］. 医疗装备，2017，30（20）：63－64.

14 杨旋，周小甲. 医院信息系统安全等级保护定级与整改结果探讨［J］. 中国医疗设备，2017，32（6）：166－169.

15 李国垒，李亚子，陈庆鲲. 医院医疗保险信息安全隐私保护调查研究［J］. 中国数字医学，2016，11（12）：66－68.