医院信息化建设中网络安全保护方案设计

唐 杰 谭 军

（长沙市第一医院信息科 长沙 410005）

〔摘要〕 介绍网络安全保护方案背景和建设目标，从集成安全控制台、网络脆弱性扫描、数据安全网关、数据库审计及加密几方面详细阐述网络安全保护系统设计，指出其有助于保护医疗信息系统、数据及患者信息安全。

〔关键词〕 “互联网 + 健康”；医疗信息化；网络安全；数据安全

〔中图分类号〕R - 056 〔文献标识码〕A 〔DOI〕10. 3969/j. issn. 1673 - 6036. 2019. 05. 010

Design of Network Security Protection Scheme in Hospital's Informatization Building *TANG Jie, TAN Jun, Information Department, The First Hospital of Changsha, Changsha 410005, China*

〔**Abstract**〕 The paper introduces the background and building goals of the network security protection scheme, elaborates on the design of the network security protection system from the aspects of integrated security console, network vulnerability scanning, data security gateway, database audit and encryption in detail, points out that the design help protect medical information system, data and patients´information security.

〔**Keywords**〕 "Internet plus health"; medical informatization; network security; data security

1 引言

随着“互联网 + 健康”的发展，医院网络复杂度及对外开放程度越来越高。在网络安全威胁日益严重的情况下如何保障各医疗信息系统的安全是需要思考的重要课题。为响应落实党中央对工作的重要部署，对医生、患者的个人隐私信息安全负责，医院有必要建立一套完整的保护方案，有效保障各信息系统和数据安全及患者医疗信息安全。

〔收稿日期〕 2018 - 11 - 14

〔作者简介〕 唐杰，硕士，高级工程师，发表论文 10 余篇。

2 项目背景

2.1 网络安全行业背景

党的十八大以来，以习近平同志为核心的党中央对网络安全工作做出一系列重要部署。2017 年 6 月 1 日我国第 1 部《网络安全法》正式实施，网络安全管理迈入法治新阶段，网络空间法治体系建设加速开展。随着互联网应用的深化、网络空间战略地位的日益提升，网络空间安全问题已经成为各国家或地区关注重点。敲诈勒索病毒盛行，分布式拒绝服务攻击事件峰值流量持续突破新高，联网智能设备面临的安全威胁加剧，网络攻击“武器库”泄露给网络空间安全造成严重威胁，高级持续性威胁（Advanced Persistent Threat，APT）组织依然活跃，这些问题对我国建设成为网络强国不断提出新的挑战。

2.2 网络安全行业趋势

2018 年 4 月国家互联网应急中心（The National Computer Network Emergency Response Technical Team/Coordination Center of China，CNCERT）发布的《2017 年我国互联网网络安全态势综述》显示：据 CNCERT 抽样监测 2017 年我国境内感染计算机恶意程序的主机数量约 1 256 万台。从 2015 年开始国家信息安全漏洞共享平台（China National Vulnerability Database，CNVD）所收录的安全漏洞数量急剧上升。2017 年较 2016 年收录安全漏洞数量增长 47.4%，共 15 955 个，达到历史新高。其中高危漏洞高达 5 615 个（占 35.2%），同比增长 35.4%。安全漏洞主要涵盖 Google，Oracle，Microsoft，IBM，Cisco，Apple，WordPress，Adobe，HUAWEI，ImageMagick，Linux 等厂商产品。网络安全漏洞是黑客发动攻击、窃取信息的突破口，因此当前面临的网络安全问题也越来越多、越来越复杂。

2.3 形势需要

根据公开数据统计 2017 年数据泄露事件数量持续上升，且总量创历史新高。2017 年 3 月公安部公布破获一起盗卖我国公民信息的特大案件，犯罪团伙涉嫌入侵社交、游戏、视频直播、医疗等各类公司的服务器，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。随着信息数据经济价值提高，促使攻击者利用多种手段获取更多敏感数据。在当前网民越来越注重个人信息安全并意识到信息泄露可能带来的个人人身财产安全问题的同时，希望政府加强监管、企业落实数据保护的呼声越来越高。

2.4 建设目标

网络安全保护方案旨在协助医院基于国内、国际的行业规范建立全面的网络安全保护系统，对医院各网络和数据资产进行保护，避免医院网络被不法分子入侵利用以及患者医疗信息被泄露，达到有效保护网络资产和患者医疗信息的目的。

3 网络安全保护方案

3.1 系统设计

长沙市第一医院网络安全保护方案在整体架构上主要由 5 个部分组成：集成安全控制台、网络脆弱性扫描、数据安全网关、数据库审计、数据库加密。系统架构，见图 1。集成安全控制台是网络管理者集中监控网络与数据安全的管控平台。网络安全脆弱性扫描负责对院内所有 IT 设备进行扫描，包括自动测绘 IT 资产，深度扫描各资产网络安全风险，基于国际、国内安全行业权威标准出具专业安全扫描报告。数据安全网关负责院内所有接口统一输出，管理外部应用调用院内接口的权限以及接口返回的数据结果集，对结果集中的敏感数据进行动态脱敏，平滑处理第 3 方应用并发请求数量，缓解院内网络和数据接口的高峰期处理压力。数据库审计负责对数据库的操作行为进行审计，分析审计日志，识别风险操作。数据库加密负责对数据库中的敏感信息进行加密存储并在业务调用时反向解密。

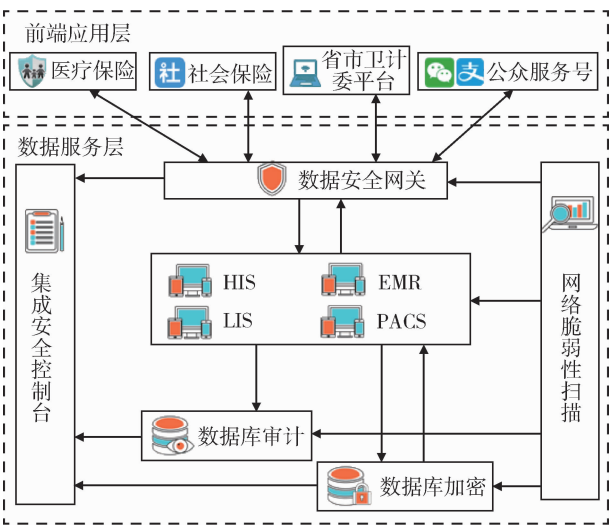

图 1 系统架构

3.2 集成安全控制台

集中监控网络与数据安全的管控平台。对网络和数据库安全关键信息进行分类汇总展示；对各种安全风险行为进行及时预警；协助管理人员全方位

了解院内各网络资产、数据对外共享及核心数据资产安全情况。

3.3 网络安全脆弱性扫描（图 2）

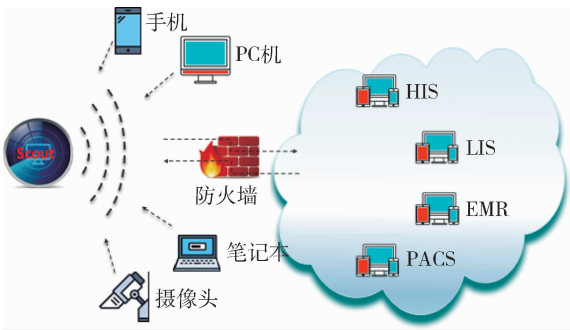

图 2 网络安全脆弱性扫描

3.3.1 Scont 概述 针对日益增长的网络安全漏洞及全攻击行为，需要建立对应机制，及时发现院内网络风险点，针对性地进行安全加固，避免被攻击的可能性。网络安全脆弱性扫描产品 Scout 基于国际、国内安全行业标准，提供完整、实时、深度、权威的网络安全风险评估，给出详细修复建议，通过升级服务、打补丁、更改配置等方式加强网络安全。

3.3.2 脆弱性扫描实现过程 脆弱性扫描通过雷达式探测技术对医院内所有网络设备进行定期、自动测绘，实现对 Windows，Linux，Android，Mac OS 等各种操作系统设备的识别，覆盖服务器、PC 机、物联网、工控设备、摄像头等设备。测绘出所有网络资产后通过高速并发扫描对所有设备进行深度的端口、服务安全扫描，列出各设备详细的开放端口和服务，结合具体业务将各设备无需开放的端口及服务进行关闭，通过减少网络攻击突破口来避免网络攻击。对于正常要提供的常见服务，如文件共享、简单邮件传输协议（Simple Mail Transfer Protocol，SMTP）、文件传输协议（File Transfer Protocol，FTP）、Web 等服务，进行全面详细的安全风险评估，根据其建议通过升级服务版本和补丁、更改配置等方式使其安全性得到有效保障。同时根据国家信息安全漏洞库（China National Vulnerability Database of Information Security，CNNVD）及国际标准漏洞库（Common Vunerbilities and Expsosures，CVE），对所有网络设备进行漏洞扫描，覆盖操作系统、数据库、各种服务，根据其给出的修复建议及时更新安全补丁或修改配置，加强院内网络的安全性。

3.3.3 漏洞脚本更新 跟踪当前全球网络安全状态，针对各种流行性漏洞。如 2017 年全球爆发的勒索病毒所利用的永恒之蓝漏洞、盗取银行账户密码的 OpenSSL 心脏出血漏洞。及时更新脆弱性扫描脚本，发现院内网络中可能被利用的节点，进行定向、定点修复，避免流行性漏洞被不法分子所利用。

3.4 数据安全网关

3.4.1 应用、接口管理方法 医疗信息化建设提高患者就医的便利性，然而患者的医疗信息对外共享至互联网的各个终端上，其中可能出现非法调用、越权调用、数据结果集过大导致泄露、慢渗等安全风险。数据安全网关负责统一管理院内所有对外数据共享，解决患者医疗信息共享中可能出现的安全问题。通过调用数据的服务、接口注册管理的方式对所有对外接口、外部应用进行强监管式管理，将接口、应用和其运营厂家绑定，明确数据接口安全责任人；通过生命周期管理支撑各接口、应用的运营，避免废弃的接口或应用被不法分子所利用。

3.4.2 应用方面鉴权管理 对应用进行严格的鉴权管理，为每个应用分配独特的 ID 和鉴权码，通过 ID 和鉴权码来获取身份识别 Token，定期刷新；限制应用的发起 IP、调用接口权限以及调用时效，防止应用被不法份子用来偷取数据。

3.4.3 返回数据结果集的管理 对所有院内接口返回的数据结果集进行管理，标识其中的敏感项，如身份证、电话号码、家庭住址等，制定敏感项脱敏规则；对同一接口返回的数据结果集，根据不同应用（服务调用方）授权来返回不同数据结果，以保障各应用业务的合理运行，同时防止其不需要的信息被获取利用。平滑处理外部应用并发请求数量，缓解院内网络和数据接口的高峰期处理压力。

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.