医院信息网络安全体系构建

黄家平 鲁 茜

（南宁市第一人民医院 南宁 530022）

〔摘要〕 以南宁市第一人民医院为例，分析医院信息化安全建设需求，对医院网络进行物理隔离，从内网和外网两方面阐述网络安全防护体系设计和应用，从审计分析、巡查制度制定等方面提出安全管理措施。

〔关键词〕 医院；信息系统；网络安全；防护

〔中图分类号〕R－056 〔文献标识码〕A 〔DOI〕10.3969/j.issn.1673－6036.2019.11.010

Building of Hospital Information Network Security System *HUANG Jiaping, LU Xi, The First People's Hospital of Nanning, Nanning 530022, China*

〔**Abstract**〕 Taking the First People's Hospital of Nanning as an example, the paper analyzes the building needs of hospital informatization security, physically isolates the hospital network, elaborates the design and application of the network security protection system from both the internal and external networks, and puts forward safety management measures in terms of audit analysis, inspection system formulation, etc.

〔**Keywords**〕 hospital; information system; network security; protection

1 引言

随着医院信息化不断深入，各业务对信息化的依赖程度越来越高，一旦出现安全问题往往会给医院造成巨大损失。特别是随着电子病历的广泛应用，一旦出现信息泄露或被恶意篡改，后果将不堪设想。信息安全已经成为医院新一代网络建设的关注重点[1]。

2 医院信息化安全建设需求

医院信息网络的应用越来越多、越来越重要、越来越复杂。在医院业务对信息网络非常依赖的同时网络安全形势却非常严峻。医院信息网络安全涵盖传输、网络、数据、业务等各层面，安全漏洞处处存在。网络黑客可能通过医院的互联网出口侵入内部网络，利用服务器漏洞获取控制权限，从而盗取电子病历等资料。社保、医疗行政部门、医疗合作单位等通过专线或虚拟专用网与医院内网相连，也是黑客入侵的主要通道。另外，医院内部存在大量的办公个人电脑，一旦病毒入侵将会成为攻击的主要发起者，若业务系统没有进行合理的隔离和安全防护，势必影响网络的正常使用和重要服务器的安全。医疗行业信息网络安全事件频发，对医院业务、数据信息、患者诊疗造成严重影响。在医院信息化发展初期，主要关注网络连通性和性能，对于网络安全的考虑相对较少，缺乏统一规划。随着网络应用日益复杂，越来越多的安全问题暴露出来。为了解决这些安全隐患，通过添加安全设备的方式给网络打补丁。但是医院网络安全产品种类较多且大多来自不同厂商，缺乏统一的管理手段和联动机制，不利于安全协防和问题追踪定位，安全漏洞无

〔收稿日期〕 2019－05－23

〔作者简介〕 黄家平，高级工程师，发表论文多篇；通讯作者：鲁茜，工程师，发表论文 5 篇。

法及时修补，信息安全问题无法解决[2]。可见传统的网络安全方案已不能满足医院不同区域的安全防护需求。现代化的医院信息网络需要多层次、全方位的立体防护体系，使网络成为智能化的安全实体。本文以南宁市第一人民医院网络信息安全防护架构实际情况为例，将医院网络分为内网和外网，内外网物理隔离。按网络的应用功能、安全防护分成不同区域，按照整体防御、分区隔离，积极防护、内外兼顾，主动防御、技管并重的原则开展网络安全整体防护。

3 内外网物理隔离

医院除了运行业务系统的内部网络外，还建有实现办公自动化和共享互联网的外部网络。传统应用共用一套网络，通过安装代理服务器、防火墙、路由器或在终端安装双硬盘、隔离卡等方式来隔离内外网，这些隔离只是逻辑上隔离且费用较高，不便管理。只有内网、外网各自独立建设才能真正实现内外网络的物理隔离[3]，见图 1。

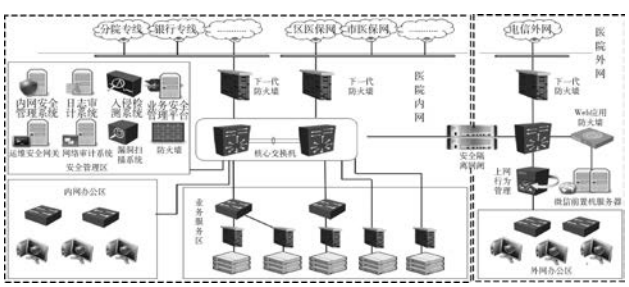

图 1 医院内外网隔离

4 网络安全防护体系设计和应用

4.1 医院内网（图 2）

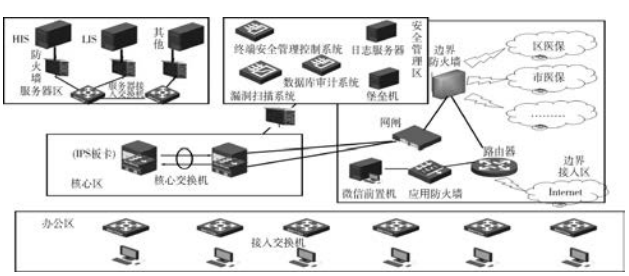

图 2 医院内网分区结构

4.1.1 网络边界 内网的第 1 道安全防线，与外单位专线进行大流量的信息交互。在医院内网边界出口处部署下一代防火墙，两台在边界，其中一台主要连接三塘、青秀、琅东分院专线，另外一台主要连接区医保网、市医保网、卫生厅专线。下一代防火墙在承载大流量数据转发的同时还可以针对各专线对网络的访问进行严格的应用层限制，只允许合法的业务数据通过，提供数据包检测防止第 3 方攻入对端专网内部控制合法主机进而攻击医院信息网络，控制攻击源头，降低各类攻击风险。

4.1.2 业务服务区 主要承载医院各类业务系统的服务器，是医院的数据中心。部署防火墙将所有服务器根据服务类型、安全级别以及重要程度进行虚拟安全域划分和物理分类。这样一旦某个业务系统出现问题能控制在本级业务系统范围内，防止攻击扩散，降低被内部攻击风险。对所有访问服务器的流量进行病毒及漏洞扫描、结构化查询语言注入、入侵防御等安全检查和过滤。部署安全审计系统记录服务器操作系统和数据库及访问者的所有记录，做到日志信息的集中审计与快速的问题排查[4]。

4.1.3 内网办公区 其用户只能处理内网业务，在内网进行各种操作，禁止访问互联网以及与医院外网信息交互。

4.1.4 安全管理区 主要部署各类安全设备，包括日志审计系统、漏洞扫描系统、入侵检测系统、堡垒机、安全网关等。对各类服务器、网络设备、安全防护设备、数据库、中间件等网络资产通过安全运维管理平台集中监控设备 CPU、内存、硬盘、接口等信息，判断软硬件可用性，从而了解业务系统的健康指数，发现问题及时解决，帮助管理员更好地管理信息中心网络资产。根据运维人员的身份和权限进行访问控制、角色划分，授予管理用户所需的最小权限，实现管理用户的权限分离。对运维人员在运维过程中远程访问、路由交换设备调试、网络安全设备的策略设置、数据库修改等操作行为进行安全审计，若出现安全问题，事后提供日志和视频图像相关证据，方便验证和溯源。

4.2 医院外网

4.2.1 安全隔离网闸 通过在医院内、外网之间部署安全隔离网闸，对数据进行细粒度安全过滤后，以私有协议方式在安全隔离网闸内摆渡，彻底切断不同安全级别网络间的任何连接，实现高安全性的隔离和实时信息交换。

4.2.2 下一代防火墙 具备入侵防御系统和防病毒网关的功能集合，能够应对各种应用网络攻击，同时抵御恶意代码攻击（病毒、木马、蠕虫等）。在医院外网边界出口处部署下一代防火墙，实现代理外办公区用户上网功能，同时保护其安全。下一代防火墙只允许合法访问通过，对于非法访问及时阻断，控制攻击源头，降低被外部攻击的风险。

4.2.3 上网行为管理系统 在外网用户办公区前端串联部署上网行为管理系统，针对用户上网提供多种认证方式，在规范用户上网行为方面可通过科学合理的策略设置进行管控，如控制 P2P 下载、流媒体、游戏等大流量的访问，保障主要业务流量的访问。

5 安全管理

5.1 审计分析

对系统所记录和存储的审计数据进行综合分析及处理至关重要。这些审计数据可能来自防火墙、路由器、入侵防御系统、主机系统、防病毒系统和桌面安全系统，对其综合分析有助于更好地管理安全事件，掌握系统整体安全情况。同时通过集中管理，医院可以最大程度地减少重复工作，从而提高安全事件管理效率。

5.2 值班、巡查制度制定

针对全院上网设备和人员进行备案，设备主要登记 IP 地址、MAC 地址、地点、科室并贴标签；人员要登记个人信息并存档。制定一系列网络安全管理制度，主要涵盖病毒防治、机房管理、保密规定、认证授权、访问控制、安全审计、安全教育、故障通报[5]。在物理环境方面有机房设备、网络设备、应用服务器、数据库主机、存储。针对安全保护系统，应急响应方案对如何处理风险、恢复数据、提升响应速度建立明确的操作规范和机制。

6 结语

医院信息安全保障体系从边界区、数据中心区、内网接入和安全管理等几个方面保证网络安全，实现立体、全方位的安全防护，避免网络及业务系统受到外界攻击和病毒感染，确保医院各业务系统在安全环境中运行，业务正常运转。

参考文献

1 王云志，李金余，杨玲. 医院信息化建设中的网络安全分析与防护［J］. 医疗卫生装备杂志，2009，30（6）：34.

2 王园园. 网络环境下学校信息管理系统安全防护体系建设研究［J］. 淮北职业技术学院党报杂志，2014，13（4）：114.

3 李秋甸，陈学涛. 医院整体网络安全防护体系建设论述［J］. 网络安全技术与应用杂志，2017（2）：116.

4 刘锋，曾凡，黄昊，等. 医院信息系统立体安全防护体系设计［J］. 医疗卫生装备杂志，2013，34（11）：44.

5 徐雷. 医院信息化建设过程中的网络安全防护分析［J］. 网络安全技术与应用杂志，2016（5）：106.