新时期医院内外网络安全建设探索

叶庆裕

（广西医科大学第二附属医院 南宁 530007）

〔摘要〕 在梳理当前医院内外网建设概况的基础上，介绍医院网络安全的主要隐患，提出医院内外网安全管理措施，以广西医科大学第一附属医院为例，阐述其内外网络安全建设原则、网络拓扑结构及建设成果。

〔关键词〕 内外网；网络安全；医疗信息化；数据交换

〔中图分类号〕R－056 〔文献标识码〕A 〔DOI〕10.3969/j.issn.1673－6036.2017.06.009

Exploration on Internal and External Network Security Construction of Hospitals in the New Era *YE Qing－yu, The Second Affiliated Hospital, Guangxi Medical University, Nanning 530007, China*

〔**Abstract**〕 On the basis of summarizing the general situation of current internal and external network construction of hospitals, the paper introduces the main hidden dangers of hospital network security, puts forward internal and external network security management measures, and elaborates the internal and external network security construction principle, network topology structure, and network construction achievements of the First Affiliated Hospital of Guangxi Medical University.

〔**Keywords**〕 Inside and outside network; Network security; Medical informatization; Data interchange

1 引言

随着网络技术和医学信息化建设的不断成熟与发展，医院构建了信息系统，在医院自身信息化建设的过程中，以及医院信息系统的运作中，信息网络的安全性越来越受到重视，加强医院信息网络安全已成为信息化建设的当务之急。医院信息网络是所有网络中安全性要求最高的网络之一，因此，目前国内医院网络系统一般由两套网络组成：一是用于支持医院内部日常医疗工作信息交换的业务网，俗称内网，又称局域网；二是用于支持外部网络（Internet）信息内容交互的办公网，俗称外网[1]。医院内网是保障医院业务开展的平台[2]，为保障其安全性，大多数医院均投入巨资从物理层面进行了严格的内外网隔离，使内外网络互不连通[3]。这样的内网相对安全，对保证医院业务系统的安全稳定运行起到了积极作用。

随着互联网的发展与普及，医院基于互联网的医疗业务环节越来越多，如预约挂号、远程问诊、查询化验结果等，甚至国家倡导的区域卫生信息平台的建立，都要求内网和外网能够互联互通。建立内外网合并的网络结构具备经济性、开放性的特点，随着网络安防技术的快速发展，网络防控手段不断增加，内外网合并正日益成为医院建立网络系统的一种新选择[4]。然而，在内外网实现数据库交互时，存在内网核心数据泄露出外网和黑客从外网攻击进内网的风险[5]。安全问题已成为医院内外网融合的一道“考题”，也是新时期下医院内外网络建设的必经途径。

〔修回日期〕 2017－06－14

〔作者简介〕 叶庆裕，初级职称。

2 医院网络安全隐患

2.1 外部（病毒、木马、黑客）攻击

有网络的地方首当其冲就会面临这样的隐患。外部（病毒、木马、黑客）攻击可以视为网络最大的威胁，在医疗行业存在院内信息共享、院外数据交互等连接，存在较大隐患[6]。案例：2015 年 2 月 16 日早晨，大英县某医院工作人员发现医院系统瘫痪，系统挂号、划价、拿药等都无法运行。负责服务器运行的人员检查后发现，医院系统被黑客攻击，系统内的数据已被对方恶意删除。

2.2 权限管理缺失

随着医院信息化的程度不断加深，上线的系统也随之不断增加，每个系统都涉及权限设置，但正是系统繁多，每个系统的权限管理存在缺失，从而造成了非合法用户对数据资源的访问，甚至造成非法获取、使用数据资源。案例：宁波市第一医院率先使用“黑白名单”设置用药管理权限，通过药库管理系统对每个药品设置白名单和黑名单，来实现允许和限制部分医生使用某些药品的功能。

2.3 内外网隔离不当

在目前内外网共存的环境下，很容易在一台电脑上出现内外网共同访问的现象，这样很容易将外部链接的病毒带入内网中，造成医院内部核心数据存在泄密的隐患[7]。案例：澳大利亚皇家墨尔本医院 Windows XP 系统被一种病毒感染，导致医院信息系统陷入瘫痪，不仅很多医疗诊断工作需要采用人工方法处理，就连患者信息也受影响。

2.4 外接设备使用不当

在医院中常常会有医务工作人员自带电脑或移动存储设备（U 盘、移动硬盘等）使用，而这些设备上的病毒在接入医院网络时，没有进行相应检测，易造成网络被攻击以及业务系统瘫痪等问题。案例：广州军区总医院从单核心组网转向多核心组网方式，对网络进行自动化检测分析，深度感知网络基础架构运行状态，能够实时输出准确、详实的分析报告及改进建议，网络运维也从人力巡检、灭火式故障管理转变为智动检测、整体管控[8]。

2.5 管理意识不强

对网络安全管理仍停留在被动监管层面，需要对网络使用者进行安全意识培训，增强主动防护意识，提升操作人员的责任心和安全意识。案例：咸阳西橡医院举办网络信息安全培训，通过大量生动的事例说明网络不安全造成的严重后果。培训会上列举了网络上存在的不安全因素：会感染电脑的恶意 Flash 文件、指向危险链接的短网址、泄露隐私的地理位置服务、过度分享等，提出安全上网的建议。

3 医院网络安全措施新探索

3.1 采用防火墙、入侵检测、应用网关等网络安全设备

从原理上分析，这是一种基于 TCP/IP 协议的内外网安全隔离机制。是一种网络隔离，或是协议隔离。由于没有脱离 TCP/IP 协议，攻击的载体仍然存在，安全的保证是依靠复杂的安全策略设置来实现[9]。

3.2 网闸防护

网闸是为了更多满足客户需求，在内外接口上解析各类应用协议，从两方面入手，一是剥离成数据，二是恢复成应用协议。其可以根据安全等级，符合要求的允许通过，不符合的则阻拦。选择网闸的好处是不仅实现了数据交换，而且可完成业务应用的访问。但其也具有一定弊端，设置不当则会成为一大漏洞，形成危险的源头[10]。

3.3 采用串口、并口、USB 等方式

采用私有协议进行内外网之间的通信，需要自行编写私有通信协议。安全程度与网闸类似，但成本低于网闸。单一应用比较合适，但应用和通信协议比较复杂时不是很合适，通信带宽也有限制[11]。综合以上隔离方式，尽管都可以在不同程度上解决网络安全隔离与数据交换的问题，但也不同程度地存在着局限性[12]。从实际内外交互应用的案例来看，网闸的应用更主流一些。但不论使用网闸还是采取私有协议，还是要与防火墙等安全设备组合在一起使用，所以内外网物理隔离网络环境下进行内

外交互通信，需要较大的投入，同时需要维护人员比较全面的网络安全意识和技能。

4 内外网安全管理措施

4.1 硬件设施选型

从信息技术基础架构出发，从根本上保证医院信息系统的安全运行。信息技术基础架构包含存储、服务器、交换机、数据线、光缆等，在搭建之初要以安全运行为首要目标，避免由基础架构的问题造成系统宕机等事故的出现，借助物理隔离方式将内、外网数据进行隔离，确保数据不泄露[13]。

4.2 软件应用选型

在硬件的基础上，选择正版操作系统，能够实现自动监测和智能升级。实时检查系统漏洞，进行智能扫描和升级，合理配置操作系统的安全决策，同时记录用户的误操作或恶意行为[14]。在软件管理方面，借助桌面管理软件自动从系统中下载补丁，自动检查客户端需要安装的相应补丁、已经安装的补丁以及未安装的补丁。对移动存储介质的接入进行限制或禁止，有效减少病毒的传入，减轻医院网络遭受到病毒威胁。

4.3 建立网络安全管理制度

建立健全安全管理规章制度，完善逐级安全责任制，贯彻执行“谁使用、谁管理”、“谁主管、谁负责”的安全工作原则。从医院管理者角度首先确立网络安全的重要意识，组织相关培训。从医务工作者角度要确立使用责任制度，规定责任到人，违规必究[15]。从信息中心角度要掌握熟练的网络安全技术，坚持管理创新及技术创新，制定应对网络危机的预案。

4.4 多重权限控制管理

医院应将多类别多系统的应用进行权限控制，设置“三重权限级别”[16]：应用程序运行权限、数据库级用户权限和操作系统运行权限。建立相应的黑客入侵系统，将黑客恶意入侵、非法登录、病毒感染以及 DDOS 攻击等进行防控和管理。实时监督分析通道质量状况，对各类终端用户进行级别划分，实现权限管理，对违规行为及时报警。除了上述的 4 种措施外，还有实时监控用户上网行为、数据备份、定期进行安全分析、对新发现的安全隐患进行整改等多种措施实现内外网络安全的管理。

5 广西医科大学第一附属医院内外网安全管理实践

5.1 设计原则

5.1.1 需求、风险、代价平衡分析 对任一网络来说，绝对安全难以达到，也不一定必要。对网络面临的威胁及可能承担的风险进行定性与定量相结合的分析，然后制定规范和措施，确定系统的安全策略。

5.1.2 易操作性 安全措施要由人来完成，如果措施过于复杂，对人的要求过高，本身就降低了安全性。

5.1.3 灵活性、适应性 首先，安全措施必须能随着网络结构、性能及安全需求的变化而变化，要容易适应、修改。其次，采用的措施应尽量不影响业务处理性能、网络性能和拓扑结构，不影响系统正常运行。

5.1.4 多重保护 任何安全保护措施都不是绝对安全的，都可能被攻破，但是建立一个多重保护系统，各层保护相互补充，当一层保护被攻破时，其他层仍可保护信息的安全。

5.1.5 可扩展性 由于网络安全是动态的，虽然现在方案解决了目前安全，但是随着时间的变化，原有的网络安全解决方案可能满足不了其需求，这时就需要对原有的网络解方案进行升级，所以现有网络解决方案应该具有可扩展性。

5.1.6 遵循国家有关计算机信息系统安全标准和规定 在安全技术和安全产品的选择上参照国家的政策和规定，在不与国家有关计算机信息系统安全标准和规定冲突的前提下建立网络信息系统的安全体系。

5.1.7 先进性 采用当今国内、国际上最先进和成熟的计算机软硬件平台、软件设计编程方法、开放式的体系结构和信息安全保障体系，使新建立的系统能够最大限度地适应今后的业务发展变化需要。

5.1.8 管理为本 安全技术是静态的，而解决网络信息安全却是一个动态的过程，只有好的安全管理才能保证安全技术得到正确、合理和及时的使用，三分技术、七分管理就是这个道理。

5.1.9 合理规划，分步实施 一个完整的信息安全解决方案不可能在很短的时间全部实施完成，需要对整个安全建设过程进行合理规划。由于网络系统及其应用扩展范围广阔，随着网络规模的扩大及应用的增加，网络脆弱性也会不断增加，一劳永逸地解决网络安全问题是不现实的。

5.2 整体网络拓扑设计

通过对广西医科大学第一附属医院的业务需求进行分析，结合企业目前的安全防护现状，对网络进行规划，规划安全建设整改拓扑，见图 1。

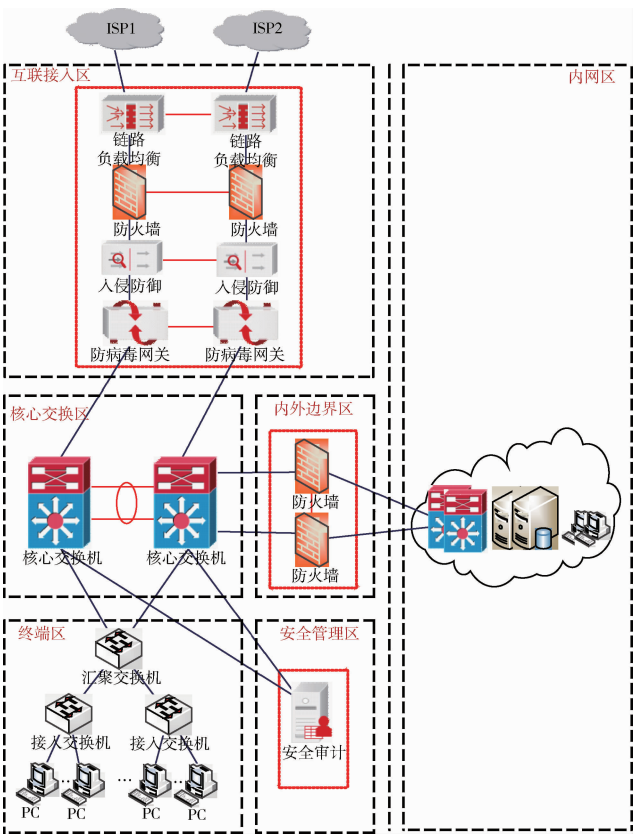

图 1 网络拓扑

5.3 建设成果

5.3.1 形成纵深的防御体系 整个安全防护从局域网边界、局域网外部、内外部之间等各个层次采取了由点到面的各种安全措施，并且保证了各种安全措施的组合从外到内构成一个纵深的安全防御体系。

5.3.2 安全措施互补 各个安全措施既独立工作，又能进行互补，发挥了更大的防护能力。如防火墙能够与入侵防御系统进行联动，当入侵防御系统检测到攻击行为时可以通知防火墙动态生成访问控制规则，阻断连接。

6 结语

要想在安全管控下实现内外网的交互，不能单纯地部署防火墙、入侵检测等传统的网络安全设备，应包括技术和管理两方面，其中技术是手段，管理是技术得以发挥作用的保障。一个好的网络信息安全体系强调从整体上实现信息安全的各方面需求，结合不同功能的网络管理工具结合，由点到面、从内到外都得到有效管理。

参考文献

1 李盛霖. 进一步加大医药价格治理整顿力度 切实维护广大人民群众利益［J］. 价格理论与实践，2004（7）：4－6.
2 马坤. 物理隔离网闸在播出系统网络中的应用［J］. 现代电视技术，2009，（10）：110－112，113.
3 刘景红，朱俊东. 医院档案信息化建设中的信息安全管理［J］. 档案，2009，（4）：56－57.
4 李国亮. 医院网络安全风险分析及应对措施［J］. 医学信息（中旬刊），2010，（11）：3354－3355.
5 朱妍. 医院信息化能力成熟度等级测评实证分析［D］. 北京：首都经济贸易大学，2010.
6 刘聪. 浅析医院网络建设中存在的问题及对策［J］. 电脑知识与技术，2011，（12）：2805－2806.
7 赵浩宇. 浅谈我院网络安全管理［J］. 电脑知识与技术，2011，（6）：1288－1289.
8 曾凡，于鸿飞，黄昊，等. 医院与医保联网存在的安全风险和解决方案［J］. 重庆医学，2011，（35）：3562－3564.
9 成自力，卢道兵. 构建医院计算机信息系统安全防范体系［J］. 中国医疗设备，2013，28（1）：86－87.
10 李安成. 医院信息网络安全管理［J］. 电脑知识与技术，2013，9（1）：32－34.
11 张亮鸣. 关于医院信息化系统内外网隔离与信息交换的研究［J］. 数字技术与应用，2014，（6）：12－121.
12 查玉龙，陈培培. 浅析如何确保医院信息网络安全［J］. 电子世界，2014，（6）：136－137.
13 丁岳. H 医院信息化建设问题及解决措施研究［D］. 保定：河北大学，2015.
14 张军. 医疗信息系统安全运行的思考［J］. 中国新技术新产品，2015，（4）：179－180.
15 高原. 医院内外网合并面临的挑战与对策探析［J］. 网络安全技术与应用，2015，（9）：42，45.
16 陆明健. 浅谈医院信息系统的安全隐患与防范［J］. 网络安全技术与应用，2015，（9）：38，41.