医院信息化建设中网络信息安全问题分层规划设计方案研究

张国富[1] 黄德胜[2 通讯作者] 刘玉转[3]

1. 广州卫生职业技术学院；2. 广州卫生职业技术学院健康大数据管理与服务教研室；

3. 广州市卫生健康技术鉴定和人才评价中心

摘　要：随着医院信息化的发展，互联网医院也在逐步兴起，医院信息化网络安全的问题也面临新的挑战，为尽最大努力巩固医院信息化建设成果，满足临床和各科室的信息化需要，避免出现安全问题，本文从医院实际发生的信息网络安全问题出发进行分析，提出了分层级规划建设的信息网络安全防护体系方案，以供大家借鉴。

关键词：医院；信息化；分层规划设计；信息网络安全

【DOI】10.12252/j.issn.2096-627X.2023.07.082

Research on hierarchical planning and design of network information security in hospital informatizatiion construction

Zhang Guofu

GuangZhou Health Science College

Abstract: With the development of hospital informatization, internet hospital are also gradually emerging, and the issue of hospital informatization network security is also facing new challenges. In order to make our best to consolidate the achievements of hospital informatization construction, meet the informatization needs of clinical and various departments, and avoid security issues, this article here analyzes the actual information network security problems that occur in hospitals, and proposes a hierarchical planning and construction of information network security protection system For your reference.

Key Words: Hospital; Informatization; Hierarchical planning; Information Network Security

引言

习总书记强调，没有网络的安全就没有国家的安全，医院的信息化在为卫生医疗行业的空前发展提供了有力的技术工具支撑的同时，也为医院信息系统网络安全带来一定新的挑战。信息化越深入，涉及的技术也就越广，信息系统受到攻击的渠道也就越多，隐患越大；信息系统受到破坏后，会对社会秩序和公共利益造成严重损害，甚至对国家安全造成损害。很多医护人员对信息网络安全意识不高，对信息系统不熟悉，或者违规操作问题，也会对信息系统的安全造成很大的威胁。因此，医院在信息化建设的同时，要根据医院的实际使用情况，充分分析信息网络安全问题，通过网络安全防护策略，充分利用信息中心网络安全人员的技术，切实落实安全防护措施，加强网络安全管理，才能够促使医院整体信息化建设有计划的高效稳步的发展。

一、医院信息化建设的网络安全问题分析

1.网络架构的不完善造成的网络安全问题

医院在信息化建设初期受资金、技术、规模和场地等因素限制，在网络部署初期一般采用二层的网络架构模式，虽运行简便但组网能力非常有限，吞吐量不高，性能不足，仅能满足运营，有些组网策略难以完成，也增加了病毒的传播概率。另外内外网虽然采取了物理隔离的手段，但是随着医院信息化的发展，医联体和智慧医院的建设使内外网互联成为必然趋势，造成的安全威胁也越大，医院迫切需要完整的网络架构解决方案。

2.网络安全意识不够，安全设备简单

医院的技术人员的安全意识不够。很多医务人员对保密等信息安全问题没有认识，个人的密码设置强度不够，且共享给科室人员，或从不更新，导致安全效能很低，势必造成各种攻击漏洞，方便黑客进入目标系统，

将可能造成严重的财产损失。

医院重视信息系统建设却忽略安全产品投入。无安全防护的医院信息系统如同裸奔，仅有一个防火墙的系统防护能力非常的有限，安全保障率很低。更别说在数据泄漏保护、脱敏等安全防护方面的低投入。由于网络安全产品的缺乏使用，给医疗信息系统埋下众多的安全隐患，安全意识的不够，极易造成信息安全的泄漏，或者勒索病毒的攻击。

3.没有形成完整的安全防护体系，安全制度不健全

由于医院信息技术团队的技术受限，很多医院的信息化建设中网络安全防御体系通常采用单一设点防护的解决方案，主要是以安全设备产品为主要落实手段，没有整体性的解决方案思维，忽略了产品之间的配合与联动，降低了产品的防护效果，对新的安全问题没有进行重新分析研判，使得信息系统面临信息网络安全威胁的概率大大增加。

同时，由于安全防护体系的局限性，有些人为主观意识操作很难得到有效的控制。在医院信息化建设工作开展或维护时，由于受操作人员专业素质、技术能力或团队协作能力不足等影响，在对软件进行编译时极易出现失误与疏忽问题，导致软件内部出现漏洞问题，这些也需要医院建立完善的安全制度。

二、医院信息化建设中信息网络安全分层规划设计方案

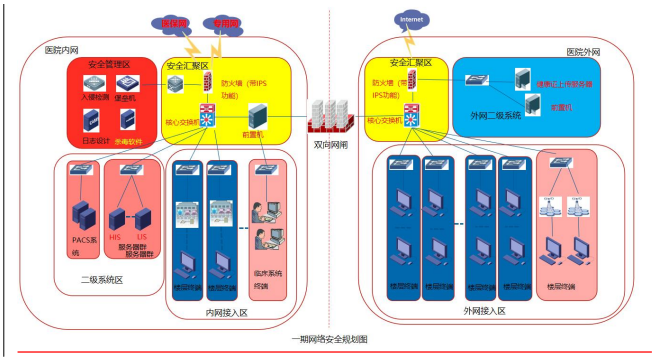
国际标准组织国际电信联盟电信标准化部门（TU-T）在X.805标准中规定了信息网络端到端安全服务体系的架构模型，医院信息化网络安全防护体系要遵循两个基本原则，一个是整体性原则，另外一个是分层性原则，在医院信息网络安全防护体系构建设时，既要考虑分层性的原则，也要重视整体性的原则，两者相辅相成，这样才能避免因为医护人员的安全意识不够而造成的一定程度上的信息网络安全威胁。医院的信息网络安全涉及各个方面，包括机房环境、软件运行环境、电脑终端的使用人员行为、软件环境，所以需要整体统一规划，设计全面的信息安全防护体系，信息网络安全系统适合医院信息网络安全防护就是最好的，所以建议采用分层逐步投入的方式。

1.整体规划，分层级设计信息网络安全防护体系

基于前期医院信息化设备投入的局限性，首先需要升级网络架构，从原来的二层交换的网络架构升级到三层的网络，增强网络的吞吐量，从而提高网络的性能。

在安全技术体系建设方面进行整体规划，分布实施，其整体的设计具有一定的健壮性和可扩展性，考虑到前期信息化系统不多，主要是以内网信息系统为主，在安全技术体系设计中分成三期，第一期主要从安全域划分、安全区域边界、安全通信网络、安全计算环境以及安全管理中心五个方面进行考虑和规划，为网络安全提供技术保障，实现纵深防御、集中管控的目标。

1）第一期总体规划



该规划思路主要是基于安全域和隔离方式，此思路进行安全设计的总体思想是：将原本复杂的系统，根据支撑业务、信息资产、地理位置、使用单位等要素划分为多个相对独立的安全域，然后根据各个安全域的特点来选择不同的防护措施，将大大提升防护的有效性，同时也体现出“整体防护、突出重点”的建设原则。

也就是将医院网络整体划分为医院内网和医院外网，医院内网信息安全等级保护建设技术建议方案分为内网接入区、二级系统区、安全汇聚区、安全管理区，医院外网分为外网接入区、安全汇聚区和外网二级系统区。将原有的大二层网络通过 VLAN 的方式进行网段划分，划分出业务系统网段与办公网段，网关设置在汇聚交换机或者防火墙之上，这样不仅将存在于外网中的前置机，比如微信公众号前置机、健康证上传服务器等置于外网防火墙内的DMZ区，而且内外网之间用网闸进行隔离，内网服务器和终端之间也用防火墙进行安全边界防护，以最小的成本代价取得了很大的效果，保证了服务器的最大安全。

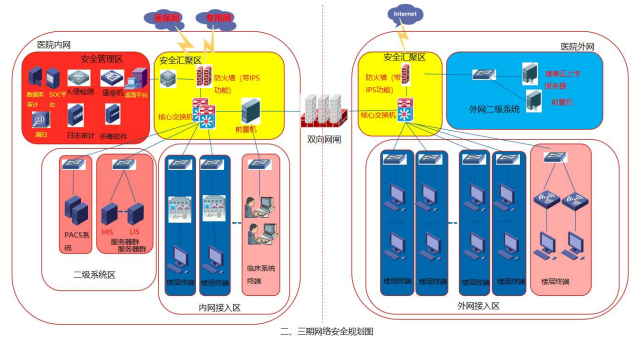
入侵检测系统旁路部署在业务系统所在汇聚交换机上，通过接口流量镜像的方式进行流量监视和检测。监视并记录网络中的所有访问行为和操作，有效防止非法操作和恶意攻击。同时，入侵检测系统还可以形象地重现操作的过程，可帮助安全管理员发现网络安全的隐患。

在汇聚交换机和边界安全设备上均开启日志审计功能，对设备运行状况、网络流量、用户通信行为等进行日志记录，尤其是记录设备及网络中发生的安全事件。并在安全管理区建立集中的安全审计服务器，实现对网络中各种日志数据的统一采集、存储、分析和统计，为管理人员提供直观的日志查询、分析、展示界面，并长

期妥善保存日志数据以便需要时查看，可为后续发生的安全事件及时进行告警并提供追踪溯源的素材，也满足网络安全法对日志留存的具体要求。

2）第二期建设规划

本期主要专注于安全的加固设计，在一期建设基础上进行技术加固，主要侧重于安全产品的加固，需要进行加固的主要包含安全区域边界、安全计算环境与安全管理中心三个方面。



二、三期网络安全规划图

在一期建设的基础上，数据库交换机上部署数据库审计设备，通过旁路侦听的方式进行数据采集，实现对用户访问数据库以及信息系统中业务服务器访问数据库的行为和相关内容的记录、分析和还原，对信息系统用户擅自访问非授权的敏感信息或蓄意篡改和破坏重要信息数据等行为进行监视和警示。

3）第三期建设规划

重点加强网络冗余方面的建设，将医院的安全保护能力能达到安全等保三级的要求，在前期网络建设的基础上，内网新增一台下一代防火墙和核心交换机，与原有的防火墙和核心交换机进行双机热备，当设备出现硬件故障之后，备机可以即时切换成主机进行工作，避免设备出现问题后造成网络瘫痪。

通过整体规划，分步骤分期进行建设，既减少了经济投入上的压力，也让信息网络安全防护体系更加完善。

2.建立一套集中管理的杀毒软件，加强内外部环境建设

针对经常发生的各科室在内网中时有发生的病毒攻击造成的软件或者电脑终端无法正常使用的事件产生的原因进行调查分析，一般是内外网互为使用U盘或者移动硬盘拷贝数据时引起的，因为医院的医护人员尤其行政管理人员喜欢将工作带往家里加班或者医务人员将科研数据资料内外网互相拷贝，除电脑终端外，另外网络中也存在一定的病毒，技术工程师通常采用格式化重装或者特殊处理等方法可以清理病毒，但是会占用大量的时间，不利于工程师技术上的进步，没有将重点放到信息化建设或者核心系统的运维上来，既增加了医院的人力成本，也让临床感觉到体验不好。经过信息科技术团队反复调研认证，认为有引进一套有集中管理功能的杀毒软件必要性，该杀毒软件可以通过集中管理统一禁止使用U盘接口，并且对电脑终端对病毒有很强的防护能力，病毒库可以实时更新。

对于某些特殊的医技科室，比如检验科，有很多的检验设备可能因为禁U造成设备接口无法正常使用，这个科室我们就单独组成局域网，而在该局域网网络边界处采用路由器与外部链接，路由器可以阻止该科室局域网中的病毒向其他网络传播。

对于内外网互拷的数据，我们用两种解决方案解决，信息科设置一台该装有杀毒软件的电脑上设置一共享内网文件交换区，如果想要内外网互拷，由信息科技术人员进行操作拷贝；另外一种解决方案就是文件通过内外网互拷的文件发送给信息科的同事，比如内网中可以采用内网OA，信息科会有一个专用U盘进行互拷操作，但是在互拷前先将该U盘进行杀毒后再使用。对于有些患者想将放射科的检查报告或DICOM检查图像用自己的U盘拷回，我们要求必须由信息科的安全技术人员操作，U盘插上后必须先进行一次格式化并对该U盘进行杀毒后再使用，该杀毒软件上线后，在短时间内就取得了良好的效果，减少了不良事件的发生。

3.提高机房的科学管理，杜绝安全隐患

机房的管理要科学。因为医院的主要信息系统都在信息中心机房，包括服务器、核心交换机、部分汇聚交换机、路由器等设备，其运行环境会影响到医院机房设备的稳定性与安全性，从而会影响网络的安全。首先机房设置要封闭，不能有水管，尤其在天花板上，不能安装在放射科等有电磁辐射的旁边，在机房内外安装监控设备，实现360度无死角的监控，非信息科人员不允许进入机房，驻点工程师的进入必须有信息科人员的允许后，一同陪同操作，当发现不法分子强行进入机房时立即向保卫等部门进行汇报和示警，对机房硬件设备设施的安全性进行保障。同时，通过宣传让医院领导提高对信息化建设及网络安全的重视程度，完善机房门禁、精密空调、动环检测系统等对温度过高进行报警，安装防静电地板防止维护时的静电给电路板造成损坏，以至于影响信息安全。管理人员需要定期组织人员对机房进行其清洁处理，保障机房内部环境的整洁性。

对于机房漏电开关的故障时有发生的情况，或者市电不稳造成的停电，我们在两套市电中安装了断电报警装置，不仅仅可以发出报警的声音，而且还可以按设置的先后顺序及时发送短信至最大5位信息科技术和管理

人员，让技术人员及时处理因为机房断电造成的信息系统无法使用的情况。

4.建立逐步发展的信息网路安全管理制度

建设安全防护体系的过程中，不能忽视网络安全管理制度的重要性，随着医院信息化的发展，信息系统向多样化多技术发展，传统的安全管理制度已经不能满足我们的需求，要求技术人员的专业更加高精，日常操作不仅要熟练，还要规范。

首先信息安全组织架构的成立，建设信息安全组织架构建设是信息安全管理的基础，目的是建立与企业信息安全操作流程、管理流程相适应的组织架构，建立满足信息安全管理要求的人员梯队，保证安全制度、流程、操作的有效落实。我们建立了决策层、管理层、执行层的三级组织架构，成立了信息网路安全管理办公室，并制定了《XXX医院应急预案》，在每年两次的攻防演练中，还需要在全院开展应急演练。组织内部安全技术骨干并邀请行业内或社会上信息安全技术专家、学者成立信息安全顾问专家组，定期或不定期为信息安全管理提供安全动态、面临的风险、先进技术、改进建议、采取措施、接受咨询。安全顾问专家组不必是常设机构，对单位信息安全领导小组负责。

其次，要建设一个安全管理平台，依据 BS7799 安全管理标准，结合安全服务的最佳实践，以风险管理为核心，通过深度数据挖掘、事件关联等技术，实现了网络内部各类安全事件的集中管理和智能分析，供多视角、实时动态的企业风险现状展示。同时，系统内置了多种报警响应、工单机制以及专家建议系统，可以帮助用户采取及时、有效的安全措施以实现闭环的、持续改进的信息安全管理，保证用户的业务不受影响。

5.定期组织培训，提高医护人员安全意识

医护人员由于信息安全意识淡薄，因此我们不仅仅要定期组织安全网络安全培训，在今年的国家网络安全宣传周中详细讲解，提高防范意识，针对统方等主观信息网络安全威胁的行为制定了《xxx医院信息网路安全管理制度》，对各个科室的主要负责人签订了《信息网络安全承诺书》，并制定了《XXX医院数据权限管理制度》，通过此制度，审查了各个科室的权限，将每个人的权限设置最小化，针对非商业行为的统方数据权限走权限申请纸质审批流程，非院长签字不给权限的流程制度。对于其他权限走钉钉审批流程，尽可能的将权限关进制度的笼子。

三、结语

总而言之，随着医院业务的多方向发展，信息化专业团队的技术提高，医联体、互联网医院等方面的发展伴随着“云大移物智”技术的应用，面临的信息网路安全威胁也呈现多样化趋势，来自内部的人为主观意识的网络安全威胁更加难防，为了创造医院良好的信息化发展环境，推动医院业务良性发展，逐步制定相适应的信息网路安全管理制度，加强网络安全培训，提高全员医护人员的整体安全防护意识，通过分层设计的安全防护体系，减少不良事件的发生，保障了医院健康的发展。

参考文献

[1]黄彪.探究医院信息化建设中的网络安全与防护策略[J].网络安全技术与应用，2022（12）：104-106.

[2]韩国梁.医院信息化建设中网络安全问题的研究[J].石河子科技，2022（05）：76-78.

[3]孙佩.医院信息化建设中的网络安全与防护研究[J].电子元器件与信息技术，2022，6（09）：204-207.

[4]徐大志.医院信息化建设中的网络安全分析与防护[J].长江信息通信，2022，35（03）：185-187.

[5]龙智勇，陈姣，阳赣萍，邓丽君，丁长松.医院信息化建设网络安全与防护问题研究[J].医学教育管理，2021，7（06）：675-679.

[6]陈春妮.医院信息化建设中的网络安全管理[J].网络安全和信息化，2023（02）：130-132.

[7]王宗源.推进医院信息化机制建设中存在的问题及对策建议[J].甘肃科技，2021，37（11）：8-10.

[8]许向毅.医院信息化建设中的网络安全与防护[J].信息与电脑（理论版），2020，32（01）：213-214+217.

[9]陈军元.探讨医院档案信息化管理存在的问题及对策[J].世界最新医学信息文摘，2019，19（89）：237-238.

[10]李立峰，翟玉兰，蒙华.广西某大型三甲医院信息网络安全管理实践[J].网络安全技术与应用，2018（09）：116-117.

[11]杨俊义.医院信息化建设面临难题及对策[J].电子技术与软件工程，2018（05）：229.

[12]刁鹏.医院信息网络安全威胁与防范措施探讨[J].科技传播，2016，8（16）：118+143.

基金项目：2022年度广东省教育科学规划课题（高等教育专项）”粤港澳大湾区高职健康大数据专业产教融合路径探析”（编号：2022GXJK577），广州卫生职业技术学院2021年度教学质量与教学改革工程项目“健康大数据管理与服务产教融合实训基地”（编号：20210103）