提高医院信息系统安全性的策略

韩 煜 李 楠

（中山大学附属第五医院 珠海 519000）

〔摘要〕 介绍医院信息系统网络安全在硬件安全、管理措施等方面存在的主要问题，在此基础上提出加强网络安全的措施，包括提高硬件设备安全、加强系统安全管理和数据信息安全、健全管理制度、制定应急预案几方面。

〔关键词〕 医院信息系统；安全管理；信息安全

The Strategies for Improving the Security of Hospital Information System *HAN Yu, LI Nan, the Fifth Affliated Hospital of Sun Yat-Sen University, Zhuhai 519000*, China

〔**Abstract**〕 The paper introduces the existing main problems in network security of Hospital Information System in the aspects of hardware safety and management measures, on this basis, it puts forward the strategies for strengthening network security, including improving security of hardware equipments, system security management and data information security, management system and formulating emergency plans.

〔**Keywords**〕 Hospital Information System; Security management; Information security

医院信息系统（HIS）一旦投入运行，其数据安全问题就成为系统能否持续正常运行的关键。作为一个联机事务系统，要求能每天 24 小时不间断运行，也绝对不允许数据丢失，稍有不慎就会造成灾难性后果和巨大损失。而造成数据不安全问题的原因是多方面的，对于医院信息系统的维护人员来说，保持系统的可用性和业务的连续性变得越来越重要，医院通常 24 小时开诊，这就要求 HIS 系统 7×24小时完全在线运行。不仅要考虑整个系统的备份问题，同时还要保证在系统出现故障时能保持业务的连续性和数据的完整性。因此，在医院信息系统的运行维护中，医院信息系统的安全保障尤为重要。

1 医院信息系统网络安全存在的主要问题

1.1 网络硬件安全问题

网络设备及其他媒体遭受地震、火灾等事故所导致的损害。此类问题技术上无法解决，需各单位做好信息数据的异地备份工作[1]。

1.2 系统安全管理措施不够

认识模糊，对病毒、黑客等危害性认识不够，没有认真地进行安全防护工作。而大多数黑客正是通过系统的安全漏洞，欺骗或盗取计算机资料，致使用户的计算机系统瘫痪。医院需加大网络防毒软件及硬件投入，组建漏洞升级服务器对客户端电脑漏洞自动升级。客户端硬件访问无封锁，现有的客户端均带有 USB 等硬件接口，可随意接入移动硬盘

〔修回日期〕 2010-03-01

〔作者简介〕 韩煜，助理工程师，发表论文两篇。

等外部设备，将危害信息安全的软件及病毒等带入医院的内部网络。技术上采用封堵电脑硬件接口手段实现外设的接入控制。

1.3 医院信息系统数据信息安全涉及的问题

登录 医院信息系统目前的登录操作是通过账号和密码，用户设置不同的权限进入信息系统，一旦密码被盗用就轻而易举地进入医院信息系统[2]。用户需加强对使用账号及密码的管理，做到不外泄，不外借。针对医院内部员工的违规操作和恶意侵入需购置入侵监测设备，便于有效监控恶意入侵等行为。医院需加强对违规人员处罚力度及公示。

网络访问随意性 大医院网络可随意互访，信息流通和共享畅通无阻，在任何一个网络点，均可随意访问整个网络的资源，数据很容易被非法窃取，单位可采用较流行的访问控制软件及硬件，做到对网络资源的权限控制及监控。数据库访问无监测，现有医院信息系统中，很少有对数据库访问的用户进行监测、存档和登记工作，即使数据库的关键数据被窃取或破坏时，也无从查起[1]。为此医院定期更新数据库访问密码，购买或开发针对不同数据库的监控软件进行实时监测。数据库超级用户严格控制开放 1 个。针对不同业务需要开放，面对具有访问权限的用户。

2 加强医院信息系统网络安全的策略

2.1 提高硬件设备安全

防雷防火 为了保证机房里面服务器以及其他设备的安全，机房所在的楼宇及机房内部均安装了防雷针等防雷措施；为保证防火安全，机房内部要放置灭火设备，同时严禁放置杂物；有条件的医院，机房内部要安装火灾自动监测及报警系统，以便监测火灾的发生并启动自动报警系统。

服务器的安全[2] 首先，放置服务器的主机房的环境要符合国家标准，室内温度控制在 20 ~ 25℃，设置防雷装置等。其次，为了保证服务器 24 小时不间断工作，应配备两套 UPS 电源。在突然停电，或其中一组电源有故障时，由另一组承载。再次，要确保服务器的稳定可靠、高效运行，有必要采取双机容错、双机热备的解决方案。

网络设备的安全[1] 对于不同的网络设备，其安全的着重点也不同。路由器：定期检查指示灯显示是否正常，用 ping 命令访问路由器的 IP 地址是否正常。交换机或集线器：定期查看指示灯状态，插头是否松动，注意防垢、防水。网卡：查看与主板是否接触不良，网卡配置是否被篡改。网线：是否有压断、扯坏、错接等故障。RJ ~ 45 头：线插的不到位，线序不一致等。这些均会造成网络不通。

定期进行硬件的检修及维护工作 做好维修记录，有可能的话可以将硬件维护外包系统逐渐扩大。采取定期做机器日常保养和检修的办法，并常做些硬件使用的培训，将故障发生率降到最低。每次做了保养及检修后都做详细的记录，因此对全院的各硬件都有大概的了解，机器出问题后基本上不用到现场，结合操作员的描述便可以大致判断故障原因。

2.2 加强医院信息系统安全管理

防入侵与防病毒 随着网络技术和信息技术的发展，各种各样的病毒泛滥成灾，严重威胁着信息财产的安全[3]。为了避免因为病毒而造成的损失，必须制定严格的病毒防护制度，减少、关闭病毒的来源，周期性对系统中的程序进行检查，利用病毒防火墙对系统进行实时监控。可安装金山毒霸、瑞星等杀毒软件。

集中安全管理 为了便于安全体系的统一运转，发挥各个组件的功能，必须对体系实施集中统一的管理。因此，需要成立相应的管理机构，制定科学的管理制度和严谨的紧急事务处理程序。

与外部网之间采用物理隔离 采用服务器磁盘镜像和双机热备份技术，防止硬盘损坏等造成的损害；过期数据的远程离线备份；日常备份文件；防火墙；杀毒软件；入侵监测系统（IDS）；开机密码、系统密码、实用软件动态密码组成的多级密码机制；分级分配权限；系统审计日志的建立，定期分析系统日志，这类分析工具在 UNIX 中随处可见；文件加密技术[4]。

工作站的安全除了防尘、防水、卸掉光驱、软驱、屏蔽 USB 接口外，还应为系统盘做镜像文件，当系统被破坏时，以便快速修复系统。

2.3 加强医院信息系统数据信息安全

数据库管理安全对策[3] 目前很多医院信息系统的单一用户就可访问整个数据库，为改变这一状况，可对数据库用户划分为超级用户、门诊用户、住院用户、接口用户和管理用户。超级用户可以访问整个数据库的内容，必须严加管理，只允许医院信息科主管（1～2 人）掌握。除非进行系统级的维护需要使用外，一般不允许其他人员使用。门诊用户、住院用户分别只能访问自用数据的设置，对该用户及口令的连接配置信息要进行二进制级别加密，用户口令保密级别与超级用户相同。对于接口用户如 LIS、PACS、RIS，则只能访问有限的几张接口表。管理用户可根据管理性质设定一些相应的权限，如备份数据库、数据库锁管理、访问数据库中需要的表等。如有多个管理员，则可在设定基本用户的基础上，再给每个管理员建立一个自用用户。使用技术手段，建立用户操作跟踪和记录，有良好的审核制度。

应用端安全对策 为防止数据的用户及口令从应用端泄露出去，这就需要采用相关的措施来阻止。目前在用的许多 C/S 系统的连接信息文件是透明的或仅仅做了简单的字符级加密，很容易被非法用户获取，对安全造成重大威胁，所以很有必要对用户连接信息进行更复杂的加密。一般可以采用二进制算法进行加密，如果需要变更，则由医院信息主管将加密后的连接文件再次覆盖到客户端。信息共享与信息安全始终是一对矛盾，医院要进行网络互连和信息共享必定会带来网络安全问题。在任何时候，对 HIS 进行连续不断的保护是非常必要的[5]。最佳途径就是采用多层次安全防护措施，对医院信息系统进行全方位的保护。在现有的网络环境及新技术和新设备不断涌现的情况下，信息安全是一个相对的状态，信息安全是一个过程，是一个防范、监控、实施和不断改进的过程。

2.4 健全各项管理制度

制度的完善也是保障医院信息安全的重要部分[5]。可以从 3 方面来制定：首先，计算机主机房的管理制度：制度包括机房内的安全管理、各硬件设备的管理、服务器日志管理、数据备份管理；其次是工作站管理制度：将每台工作站建立工作日志，记录在该工作站上上机的每位操作员的开机时间、关机时间、操作内容、系统运行情况以及操作员姓名等；再次是人员培训管理制度：每位工作人员在上岗前进行岗前培训，合格后方可上机操作。培训时加强网络安全意识。此外还应建立数据库日常维护操作规程、网络安全保密制度、病毒预防和检查制度等。

2.5 制定安全应急预案，提升应变能力

信息安全技术的日新月异，使安全管理有着很大的不确定性。再严密的安保措施也不能确保网络的万无一失[3]。因此必须提高应对突发事件的处理能力。将中断时间、故障损失和社会影响降低到最低程度，因此制定一整套应急预案显得尤为重要。当医院内网出现意外而又不能在短时间排除故障时，可立即启动“医院信息系统故障时的紧急工作预案”，将计算机系统转为手工操作，确保医疗工作有序进行。应急预案包括两步进行：第 1 步：制定手工工作流程。因长期依赖计算机操作，各部门人员早已将原始的手工操作流程遗忘。所以将门诊服务台、挂号处、收费处、结账处、门诊药房、住院药房、病区、医技科室、手术室、麻醉科的手工操作流程全部发放到各部门，使各部门井然有序地进行工作。第 2 步：制定故障排除预案。由信息部门将各种软硬件故障的排除和解决方案以及软硬件商的联系方式全部整理在案，以便紧急时候能够节省时间。本院已制定了一整套排除故障的应急预案。如：紧急停电的应急预案、远程医保连接故障的应急预案、HIS 系统故障的应急预案、中心服务器故障的应急预案、核心层交换机故障的应急预案、互联网硬件设备故障的应急预案、中心主机房供配电系统故障的应急预案。 （下转第 27 页）