第 4 卷◆第 5 期◆版本 1.0◆2023 年
文章类型：论文|刊号（ISSN）：2737-4580(P) / 2737-4599(O)

医院信息系统中的网络安全与管理

张保华
新疆维吾尔自治区人民医院　信息中心
DOI：10.12238/jpm.v4i5.5964

[摘　要] 随着信息技术的不断发展，医院的信息网络系统也得到了快速的发展，HIS（医院信息系统）在医院的运作和管理过程中，有着不可取代的重要作用。它不仅是医院不可或缺的基础设施，还是保障医院医疗业务能够正常开展的关键所在。因此，如若医院的网络信息系统出现了问题或是发生故障，轻则将会在一定程度上直接影响到医院工作业务的正常开展，重则甚至有可能给医院造成无法挽回的损失。但是，在医院网络信息系统的运行过程中难免或出现一些故障，怎样降低医院信息系统的故障率以及如何在故障出现后尽快弥补成了医院网络管理人员的关注重点。因此，通过一系列的措施，增强医院信息系统的安全，确保网络信息的准确性与安全性，对促进医院的进一步发展和改革的具有重要作用
[关键词] 医院信息系统；网络安全；网络管理

Network security and management in the hospital information system

Bao-hua zhang
Information Center of Xinjiang Uygur Autonomous Region People's Hospital, Xinjiang Urumqi 830001
[Abstract] With the continuous development of information technology, the information network system of hospitals has also been developed rapidly. HIS (hospital information system) plays an irreplaceable role in the operation and management process of hospitals. It is not only an indispensable infrastructure for hospitals, but also the key to ensure the normal development of medical business in hospitals. Therefore, if there are problems or failures in the network information system of the hospital, it will directly affect the normal development of the hospital work and business to a certain extent, and may even cause irreparable losses to the hospital. However, in the operation of hospital network information system, some faults. How to reduce the failure rate of hospital information system and how to make up for the failure as soon as possible have become the focus of hospital network management personnel. Therefore, through a series of measures, to enhance the security of the hospital information system, to ensure the accuracy and security of the network information, plays an important role in promoting the further development and reform of the hospital
[Key words] hospital information system; network security; network management

近几年来，随着计算机网络技术在国内影响范围的不断扩大以及应用的日益广泛，不少医院也将网络信息技术运用到了医院日常工作管理中，医院信息系统应运而生。医院的信息系统以患者为数据采集的线索，以医院的财务管理为中心，以医院的局域网为依托，对患者在医院治疗的各个环节进行网络覆盖，与医院的医疗业务和患者的切身利益有着密切的关系。当前，医院的信息系统在运行过程中，虽然其网络技术的开放性很强，但是同时其中也潜在着诸多的风险和不足之处。所以，这就要求国家相关部门和医院自身要对医院信息系统中的网络安全性给予足够的关注，更加深入的对医院信息系统进行研究，制定出与之相对应的对策，进一步提高医院信息系统的可用性、完整性及保密性，减少医护矛盾的发生，确保医院信息网络系统的正常运作，维护医院医疗程序的正常，以促进我国医院的信息化水平。

一、医院的网络建设

医院网络的建设是一项复杂且工作量较大的工程，其建设设计的合理性，不仅在一定程度上直接决定着医院信息网络的进一步发展，还在很大程度上关乎着医院的经济效益。当下，对于如何建设医院的信息系统，应遵循“总体规划、逐步投入、分步实施”的设计建设思路，合理、科学的对医院信息系统进行设计[1]。同时，在对网络的进行设计与建设时，还需要对建筑物所在位置的地理特征进行充分的考虑根据有关的标准和规定，对综合布线系统进行标准化、规范化建设。其中，医院应选用双路千兆多模的光线敷设医院信息系统的主干线，用屏蔽双胶线对楼层交换机到各个终端的部分进行处理，对楼层的交换机到各个终端的部分采用屏蔽双胶线，与强电之间的距离

文章类型：论文|刊号（ISSN）：2737-4580(P) / 2737-4599(O)

不得小于 30 厘米，以免出现相互干扰情况。此外，网络中心的设置对于医院信息系统来说尤其重要，其不仅是整个医院网络信息系统的核心，还是管理和存储多种重要信息的网络通信中心与数据中心。核心网络设备应选用“双机热备”的方式，在接入层衔接上级设备时应选择“链路双上联”的模式，并且要具备较强容错能力，尽可能减少发生单点故障的几率。而机房电源，最好选用“7x24 小时”UPS 不间断电源。

二、医院信息系统面对的安全威胁

当前,医院信息系统主要面临的安全威胁主要有以下几个方面：第一，自然灾害。例如水、火灾或是地震等不可预知的自然灾害，会对信息系统的基础设施设备，如计算机等造成较为严重的物理性破坏；第二，人为风险。网络信息系统所面临的安全隐患是由人导致的。例如黑客攻击、病毒侵入以及使用不当所造成的设备故障；第三，技术风险。医院信息系统本身存在问题，例如应用系统自身不完善、系统存在操作缺陷等，同时，网络系统设施所在的场地条件、机房的环境等都在一定程度上给计算机网络带来了安全上的威胁，需要做好技术方面防范工作；第四，管理风险。医院的安全制度和保密制度不够健全和完善，例如管理制度不健全、责任权利划分不明确、管理控制不当等，在内一定程度上为医院信息系统带来了风险。

三、医院信息系统管理问题

（一）系统补丁更新滞后

目前，许多医院在使用医院信息系统的时候，一般都会将杀毒软件安装到业务主机上，但是由于主机的数量比较多，对其逐一进行维护比较困难，使得计算机的维护工作人员难以确保所有主机上的系统补丁与杀毒软件都是最新版的，从而，在一定程度上使得医院信息系统在应用过程中潜在着诸多网络安全与管理问题。

（二）地址绑定无现实意义

有的医院会选择在接入层的交换机上将端口与 MAC 地址和 IP 地址进行绑定，以防止外来者随便接入内院网络。但这个方法在实际操作过程中潜在着很大的安全问题：一方面，MAC 地址和 IP 地址在进行绑定时的工作量非常的大，且不是很方便，需要逐一的安装在每一台电脑上；另一方面，这种操作的技术含量较低,稍微会点电脑的人,就可以很容易的修改医院的 MAC 与 IP 地址，因此，地址绑定的意义不是很大[2]。

（三）入侵检查系统失效

目前，大部分医院在使用医疗信息系统的时候，都会配备 IDS 入侵检测系统，但是这个系统仅能够在有异常情况出现的时候进行警示，而无法实现其他功能，所以入侵检查系统很难发挥其应有的作用。

（四）数据库安全审计定位不准

在使用信息系统的时候，大部分的医院都会选择对登录人员的访问权限进行设定，以防止数据被盗取或者篡改，但是这种操作仍然无法对恶意者的不法行为进行较为有效的避免。虽然数据库安全的审计系统可以对数据库的各项操作进行详细记录，并对 IP 地址进行精确定位，但是其很难与 IP 地址所处的人员进行一对一的绑定，所以难以对其进行责任追究。

四、强化医院网络安全的措施

（一）中心机房及网络设备的安全维护

1.环境要求

医院网络信息系统的信息处理中心是中心机房，其作为医院信息系统的中心，需要为其一个创建一个良好的工作环境。首先，机房的温度控制在 2 4 ℃ ± 1 ℃之内最佳；相对湿度尽量控制在 40%至 70%之间。其次，在机房内应设有报警系统，地板应铺设防静电的，且要做好防雷、防火等措施。

2.电源管理

中心机房的供电系统是在很大程度上影响着机房工作的效率，因此，医院信息系统所应用的存储设备、服务器以及交换机都应由 UPS 提供可靠的、稳定的电源。

3.网络设备

网络是医院信息系统传输信息数据的基础，对其的正常运行影响巨大。所以，医院需要定期对网络设备的软件与硬件进行升级与检查。同时，可通过 siteview ecc 软件对网络设备的流量、端口状态进行监测，以便及时对医院网络系统的具体动态进行掌握。

（二）服务器的安全维护

1.加强账号和密码管理

密码保护与账号保护是进行服务器操作的第一层保护，对医院信息系统来说具有重要的实际意义。外来者对系统的攻击在很多时候都是从截获密码和账号信息开始的[3]。外来者一旦进入了系统，其他防护措施的作用会被极大的削弱，所以，服务器的软件系统与操作系统最好使用安全密码的管理方式，特别是服务器的密码，更要进行进一步的加密设置，并要对密码进行定期的更换。

2.定期进行系统日志的监测和审计

医院应对服务器系统日志进行定期分析和监控，以保障系统日志程序的运行正常。依据系统日志来分析系统进行的活动、使用的账号以及最近登录时间等信息状况，让服务器的维护工作人员可以通过分析和统计，对服务器的运行状态进行有效的掌握，从而及时发现与解决信息系统在运行中出现的错误。

3.双机热备

业务服务器是医院信息系统的又一重要核心，在重要程度上与核心交换机不相上下，主导着医院信息系统的运行安全。因此，为了保证信息系统的高效、可靠、稳定运行，医院信息系统应采用双机热备模式，即一台共享磁盘配置两台服务器的阵列，由于其通过有关技术可以实现对集群技术的控制，所以能够维持信息系统的正常运行。

（三）工作站的安全维护

1.外接设备管理

为了避免工作站用户随意安装非法程序以及拷贝文件、数据，因此工作站不得安装光驱、软驱，并使用软件对 USB 存储进行屏蔽，对外来设备进行严格控制，从而降低病毒感染的途径。

2.权限设置

在医院的信息系统中，用户只有一个账户和与之相对应的

密码，且不同的账户有不同的使用权限，在进行操作时不可以越权使用其他账户。

3.桌面管理软件

在对终端桌面进行不定期监控时可运用 landesk 管理软件。将远程监测系统安装在工作站，不仅可以实现远程杀毒、管理、安装等工作，在一定程度上减小了信息系统维护工作人员的工作量，使员工的工作效率得到一定的提高，还能够及时为信息系统打补丁和下载补丁，将不必要的端口进行关闭，在一定程度上对系统漏洞进行了弥补，减少了网络安全风险。

4.内外网隔离

医院信息系统较为敏感，需要使用物理方法隔开终端和其他外部网络。但是对于部分特殊用户，不仅需要掌握和了解医院自身的信息，还需要将一些医疗信息上传到相关上级部门。在这种情况下，最好采用两台电脑分开使用的方式，中间通过 KVM 切换器来切换，不仅在一定程度上减小了成本，还极大的方便了用户使用，提高了安全性。

（四）病毒防护

1.虚拟局域网技术

使用 VLAN 技术，能够依据实际需要将由交换机链接成的物理网络划分成若干逻辑子网。这些子网能够利用访问控制列表对病毒的传播进行阻止，即使有病毒也可以将其限制在同一 VLAN 之内，从而对病毒的传播进行有效控制，降低病毒传播的危害。

2.杀毒软件

因为病毒具有传染性，如果医院的局域网中有终端机器受到了病毒的感染，那么它就有可能感染到网络中的任意一台或者是更多没有保护机制的计算机，进而引起连锁反应，造成医院信息系统无法正常运转，破坏可执行程序以数据，严重时甚至可能造成整个信息网络系统的瘫痪[4]。因此，在面对持续变化、不断更新的病毒与复杂的网络环境时，医院应该对网络病毒的危害进行充的认识，准备和安装专门用于防病毒的服务器，同时要设置好病毒扫描程序，定期、定时对医院的信息系统进行检查，并制定与之相对应的解决策略，将风险扼杀在萌芽状态。

3.防火墙技术

当下，网络防火墙技术已经发展的较为成熟，可以较为有效的对计算机进行保护。防火墙是网络信息系统安全的第一道门户，能够有效隔离内、外部网络和控制访问，从而保障网络服务和网络系统的高可用性。因此，在医院的信息系统中，防火墙通常被安装在医院内外网接口处，或是与其他单位网络的接口处，从而对外界的入侵网络进行抵挡和确保数据的传输安全。

五、数据管理

（一）安全管理

数据安全指的是在数据在网络流通与存储过程中的安全性，它的作用是防止在网络中的数据被复制、篡改、解密、非法的增删、使用以及显示等。对于医院来说，患者的诊断与治疗信息是其信息系统的重要内容，所有的信息都是存储在业务服务器和数据存储上，信息系统中的数据一旦受到破坏，将会给医院带来难以估计的损失。对此，医院应健全和完善监控体系，通过监视服务器当下运行状况，及时的找出信息系统中存在的问题，并对其进行进一步的调整和优化。此外想要进一步推动医院的信息化进程，必须要保证医院医疗数据保存的完整性。因此，医院需要建立健全的恢复和备份机制，进一步保障数据的安全，促进医院的健康发展。

（二）集中管理

医院信息系统的数据种类较多，例如 ris 、lis、pacs、his 等。鉴于此种情况，医院可采取集中管理方式，将所有数据统一存放在集成介质上，由网络信息管理工作人员对其进行集中的统一管理，不仅能够增加方便的恢复与保存信息数据，还可以增强网络性能与降低计算机系统的资源浪费。同时，SAN 存储局域网作为数据集中管理的网络架构，可以实现多点对多点的管理方式，具有高可用性、高可扩展性、高可管理性、高性能以及高可高性等优势。不但使信息系统的工作效率和资源利用率得到了提高还在进一步增强了信息系统的可用性，降低了系统宕机和数据中断的风险。

（三）人员管理

随着信息技术的不断更新与进一步发展，现代社会的人们应积极主动地对新的知识技能进行学习,在提升自身综合素质的同时，推动网络安全管理的发展。同时同时，医院应加大对医院信息系统相关操作员的专业培训，提高其专业知识储备，增强其专业技能水平，更好的维持医院信息系统的运转，降低人为因素失误造成的影响。

（四）完善管理制度

安全管理制度在很大程度上影响着网络的安全，因此加强内部信息的安全管理对医院来说十分必要。所以针对技术管理人员，医院应对信息管理人员的行为进行规范，同时建立健全管理制度，如病毒防范制度、信息系统故障应急方案、机房数据安全保障工作制度等，仅仅一步对工作流程进行规范，避免事故的发生，保证医院信息系统的稳定运行和数据的完整安全。

结束语

医院的网络信息安全管理，是保证医院工作正常运行的重要保证，因此，医院必须对此予以足够的关注，并结合着自身的发展模式，对信息安全措施进行规划，建立和完善的预警处理机制，从而使医院可以与高速发展网络时代相适应，健康、持续的发展。

[参考文献]

[1]王蜀锋. 医院信息系统中的网络安全与管理[J]. 网络安全技术与应用,2022,(06):117-118.

[2]王冠男. 医院信息系统中的网络安全与管理[J]. 信息与电脑(理论版),2020,32(14):208-209.

[3]莫非. 医院信息系统中的网络安全与管理[J]. 计算机光盘软件与应用,2012,(14):8+10.

[4]黄伟. 医院信息系统中的网络安全与管理[J]. 网络安全技术与应用,2010,(12):22-24.