ISSN 1009-3044
Computer Knowledge and Technology 电脑知识与技术
Vol.9, No.1, January 2013.
E-mail: info@dnzs.net.cn
http://www.dnzs.net.cn
Tel:+86-551-65690963 65690964

医院信息网络安全管理

李安成

（四川省隆昌县人民医院，四川 内江 642150）

摘要：医院信息系统的正常运行是保证医院医疗业务正常开展的关键，分析了现阶段医院信息系统面临的安全威胁，详细介绍了医院信息网络安全管理措施，可供同行参考。

关键词：医院信息系统；信息安全；网络安全；网络管理

中图分类号：TP393　　文献标识码：A　　文章编号：1009-3044(2013)01-0032-03

Safety Management of the Hospital Information Network

LI An-cheng

(The People's Hospital of Sichuan Longchang, Neijiang 642150, China)

Abstract: The key to the normal conduct of business of hospital medical is the normal running of the hospital information system, this paper analyses the security threats faced the hospital information system, and it introduces the security management measures of the hospital information network.

Key words: hospital information network; information safety; network safety; network management

随着信息网络技术的迅猛发展，各医院都建立网络来推动医院信息化建设，计算机网络技术将各个信息系统（如HIS系统、PACS系统、LIS系统、OA系统、手麻系统、电子医嘱、电子病例、医保农保接入、体检系统、金蝶财务软件、血费直报系统、病案直报系统等等）联系在一起，信息网络技术给医院的各方面工作带来了很大的便利，大大提高了医院信息的利用率和医院整体运行效率。我院信息网络系统经过多年的建设及运行，已经具备了一定的网络规模，但随着医院业务系统的逐步扩展应用，网络恶意软件及网络黑客相继出现并呈泛滥趋势，这给医院信息系统带来了极大的威胁，给医院信息中心工作人员带来管理难度，如何保障医院信息化网络系统正常运行，已经成为一个亟待解决的问题。

1 医院信息系统面临的安全威胁

医院信息系统是一个多业务、多角色、多模块的信息系统，其受到安全威胁也比较复杂。

1）恶意攻击是医院计算机网络所面临的最大威胁，由于业务的需要医院信息系统与很多合作单位之间通过网络连接共享信息，如医院业务系统需要与医保、新农合等社保网络连接及数据传输，这样就给黑客攻击、病毒及蠕虫等带来入侵机会。

2）信息系统管理权限混乱，存在越岗、代岗现象，存在用户账号被滥用和业务数据被非法读取等安全隐患，有些合法用户利用计算机技术访问其权限之外的系统资源，有些非法用户假冒合法用户的身份访问其应用资源等安全隐患。

3）内外网之间缺乏相关隔离措施，有些医院部门人员需要同时访问内部业务网络及外部Internet，部分医院用户利用同一台计算机进行内外网访问，在访问外部Internet时，容易感染病毒或将木马带入内部业务网络，此外，移动存储介质的广泛应用也成为病毒入侵的重要途径，由于内外网之间缺乏必要的隔离设施，医院的核心业务信息存在互联网泄密的安全隐患。

4）对信息网络缺乏安全管理，缺少行之有效的安全保护措施和审计机制，如存在部分医院内部人员将个人电脑（可能携带病毒）接入医院业务网络，这样会给医院业务网络带来破坏，从而导致业务中断，而当网络受到安全威胁或出现攻击行为时，无法对其进行有效的检测及监控，无法及时报告与预警，并且当事故发生后，也无法提供攻击行为的追踪线索，此外还有些操作人员擅自修改计算机软硬件设置，擅自修改客户端 IP 地址容易造成操作系统，如在计算机上安装游戏、即时通讯等与工作无关的软件，都会导致业务程序瘫痪。

5）操作不当也是信息网络故障的常见原因，如管理人员的安全意识薄弱，保密意识不强，长时间不做修改更新密码或密码过于简单，这容易导致密码被非法用户破解，管理人员的个人素质不高，如操作人员对操作流程不熟悉或工作责任心差，都给信息网络带来安全隐患。

6）操作系统漏洞给黑客入侵及恶意攻击提供了便利，这需要系统及时更新造作系统补丁，如不及时打补丁，即使有正版杀毒软

收稿日期：2012-11-03
作者简介：李安成（1975-），男，四川隆昌人，中级职称。

© 1994-2013 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

件的保护,黑客、非法用户也会通过多种方法实施攻击,截获、窃取及破译机密信息。

7)网络设备工作环境恶劣也会给信息网络带来安全隐患,医院信息系统要求网络设备全天不间断的运行,这要求设备工作环境(特别是中心机房环境)必须满足规程要求,另外自然灾害的影响,如火灾、静电、地震、电磁干扰、雷电、鼠害等会造成的系统数据损坏或丢失的安全隐患。

2 网络安全管理

通过建立技术先进、管理完善、机制健全建立医院信息网络安全管理体系,保证医院信息网络安全可靠畅通运行。

2.1 医院网络内部管理

1)建立网络安全管理规章制度

加强医院网络安全管理的重要措施之一就是建立健全网络安全管理规章制度,提高医院全员认识到医院网络安全管理重要性,设立以院领导为核心的信息安全领导小组,明确领导小组相应责任并落实信息管理人员责任,加大投入资金,对网络安全管理软硬件设备进行更新升级,对网络安全管理专业队伍需要加强建设,信息网络人员必须要有责任心及熟练的网络应用技术,同时要坚持管理创新及技术创新,根据本院信息网络的运行情况,制定应对网络危机的预案。

2)网络安全教育

网络安全工作的主体是人, 医院的各级领导、组织和部门工作人员从思想和行动上都要重视医院信息系统网络安全,提高全员安全意识,树立安全人人有责,由于医院的内部网络涉及临床科室、医技科室、职能科室等部门,计算机操作水平参差不齐,因此,必须定期培训计算机网络客户端的使用人员,使他们具有一些计算机方面的专业知识,尽量减轻医院计算机网络信息系统管理人员的工作压力,当其客户端出现问题之后能得到及时的解决,减少人为的差错及故障发生。

3)网络设备管理

网络设备是整个信息网络安全的基础, 整个网络中的关键设备包括服务器、数据储存、中心交换机、二级交换机、光缆等,因此这些设备的性能直接影响到整个信息系统的安全运行,从可靠性、稳定及容易升级等方面对网络设备进行选择,对重要设备最好采用双机热备份的方式实现系统集群,还要配备两套UPS电源,避免突然断电造成服务器数据流失,提高系统可用性,服务器以主从或互备方式工作,当一旦某台设备发生故障,另外一台设备可以立即自动接管,变成工作主机,将系统中断影响降到最低;此外,使用物理隔离设备将外部互联网和内部信息系统进行隔离,确保重要数据不外泄。

4)软件选择

从软件选择上来说, 统一购买正版操作系统,完成自动监测和智能升级,使用正版软件,并时常更新操作系统漏洞补丁及应用软件的版本。利用安全扫描系统软件定时进行网络安全漏洞扫描和智能升级,检查系统是否存在漏洞,合理配置操作系统的安全策略,对关键操作应开启审计,对用户的误操作或恶意行为进行记录,关闭默认共享,采用虚拟局部网络(VLAN),保障内网中敏感数据安全。

5)实时监控用户上网行为

应用主机安全监控系统,实现对用户上网行为的实时监控,从而让网管及时了解和控制局域网用户的的上网行为,在加强安全防护的同时也可以提高工作效率。主机安全监控系统可以对内部人员上网行为日志、客户端访问行为、终端行为日志、医院IT开发运维人员访问行为等信息进行监控、记录、审计能力,结合日志数据挖掘技术和关联分析功能,实现对非法行为的实时告警,输出符合医院纪委监察部门要求的完整的事件报告,既能够及时发现并阻断非法行为,也可以监控某些人员利用其特权对敏感数据进行非法复制。

6)多重的权限控制管理

采用多重的权限控制管理策略,将应用程序运行权限、数据库级用户权限和操作系统运行权限分为三重权限。在系统中的每个用户有唯一的账号及密码,且对应着相应的权限,服务器操作系统和软件系统最好采用安全的密码管理方式,特别是服务器密码要严格按照安全密码所采用的加密算法来进行设置,采用数字、字母和大小写混合的方式,并定期更换密码。

7)数据备份

为了防止信息系统中的数据丢失,可以采用双机备份方式。两台服务器采用相同的配置,安装相同的系统和数据库系统,实时将主服务器上数据库备份到备用服务器上,当主服务器无法正常工作时,启用备用服务器项替工作,同时信息系统管理部门可以采用一些有关的备份软件对其医院计算机网络信息系统的数据进行及时的监测,当这些数据出现安全方面的问题时,及时对其数据进行备份;此外,也可采用实时备份数据库,采用数据镜像增量备份方式。

8)定期进行安全分析,对新发现的安全隐患进行整改

运用技术手段定期进行安全分析,及时发现安全隐患并快速清除是完善医院网络安全管理的重要措施。定期进行安全分析是研究信息系统是否存在的漏洞缺陷,是否存在风险与威胁,针对发现的安全隐患,制定出相应的控制策略,主要是从软件设置、物理环境、电源配送、权限分配、网络管理、防火、防水、防盗、服务器交换机管理、温度湿度粉尘、人员培训及安全教育等各方面进行分析,寻找出当前的安全隐患,针对这些隐患提出有针对性的解决方案。

2.2 防止外来入侵

1)中心机房管理

作为医院信息系统的“神经中枢”及数据存储中心的机房安全是整个信息系统安全的前提,中心机房的安全应注意机房用电安

© 1994-2013 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

全技术、防火、计算机设备及场地的防雷和计算机机房的场地环境的要求等问题，为了避免人为或自然破坏设备，应尽可能保证各通信设备及相关设施的物理安全，使系统和设备处于良好的工作环境，对于信息网络的可靠性，可以通过冗余技术实现，包括设备冗余、处理器冗余、链路冗余、模块冗余、电源冗余等技术来实现。

2)计算机病毒防护

杜绝病毒传染源是防范病毒最有效的办法，除特殊科室需要外，将所有网络工作站的外部输入设备(如光驱、软驱等)撤除，所有内网的计算机不准接U盘，在服务器及每个工作站点采用多层的病毒防卫体系，此外，还可以使用桌面管理软件来自动从系统厂商下载补丁，自动检查客户端需要安装的补丁、已经安装的补丁和未安装的补丁，以及限制或禁止移动存储介质的接入，减少病毒传播的途径，从而减少医院网络受到病毒的威胁。

3)防止黑客入侵

防止黑客入侵是医院网络安全工作的重点，可以采用防火墙技术、身份认证与授权技术等技术防止黑客入侵。其中，防火墙技术是在医院内部网和医院外部网之间的界面上构造一个保护层，对出入医院网络的访问和服务进行审计和控制；在防火墙基础上，建立黑客入侵检测系统，对黑客入侵、非法登录、DDOS攻击、病毒感染与传播、非法外连等进行监控，对网络设备、网络通讯通道等进行监控，详细掌控各类网络设备的运行状态，实时监督分析通道质量状况，对各类终端用户的补丁安装、软件安装、外接设备(U盘)等操作进行实时监控管理，发现有违规行为及时报警，也可以自动启动阻止机制来控制非法行为；在医院信息系统中，采用数字签名技术实现系统信息内容安全性，完整性和不可抵赖性等方面的要求，特别是通过采用安全审计或时间戳等技术手段解决传统纸质病历无法解决的信息可靠性问题，此外，还采用信息加密技术可以有效的保护网内的数据、文件、口令和控制信息，保护网上传输的数据。

3 结束语

随着医院业务的不断拓展和医疗政策的不断发展，医院信息网络也由满足医院业务需求的封闭网络发展成为一个面向公共的信息系统，面临着巨大的安全威胁，这要求医院信息系统应具有更高的安全性，而医院信息系统安全管理是一项动态管理工程，随着外部环境(新病毒、新漏洞、新木马等)的变化而发生变化，其涉及技术、管理、使用等方面；因此，网络管理人员在对医院信息网络进行管理中，需要不断调整网络管理的安全方法，并制定出网络安全应急预案，确保医院信息系统的安全可靠运行。

参考文献：

[1] 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).
[2] 赵浩宇.浅谈我院网络安全管理[J].电脑知识与技术,2011(6).
[3] 曾凡等.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).
[4] 刘景红.医院档案信息化建设中的信息安全管理[J].档案,2009(4) .

(上接第28页)

通过服务器找到对方并实现双方对话的功能，服务器的信息转发机制具有信息过滤功能，一定程度上保证了客户的信息安全，也很好的提高了整个系统网络通信的多用户通信的稳定性。

4 结束语

为了提高嵌入式网络通信的稳定性，解决在嵌入式网络多对多通信中出现网络拥塞造成网络性能指标下降、引起网络带宽资源浪费的问题，该文在嵌入式Linux通信开发技术基础上，提出一种单一进程的多目标睡眠等待的信息转发机制方法，经过在嵌入式Linux平台上实验测试，既实现了进程与多个数据通道进行通信的目的，又使信息转发保持了较高的效率。该研究成果对网络化的嵌入式系统有一定的积极推动作用。

参考文献：

[1] 邹国霞,黄廷磊.嵌入式网络通信中RED算法的优化[J].广西民族大学学报(自然科学版),2010,04:60-64.
[2] 安佰秀,曹景龙,史大光. 基于以太网和嵌入式Web服务器的监控系统设计[J].工矿自动化,2011,05:79-82.
[3] 钱琛,陈耀武.嵌入式VOD码流传输同步优化方案[J].计算机工程,2012,18:268-272.
[4] 周芳,蒋建国,王培珍.无线传感器网络中视频传输的控制仿真[J].系统仿真学报,2010,02:443-448.
[5] Cheng Yuan zhong, Du Ping an. Analyses of I/O mode in winsock[J]. Computer Engineering, 2001, 27(1):178-180.
[6] Anthony Jones, Jim Ohlund. Network programming for Microsoft windows[M]. Beijing: China Machine Press, 2003.
[7] 毛丽荣,马兆丰,黄建清,杨义先,钮心忻.支持细粒度授权的电子文档防泄密系统网络通信设计[J].小型微型计算机系统,2011,2:242-247.

© 1994-2013 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net