· 医院管理 ·

# 加强军队医院信息安全管理实践与体会

张 稳[1],袁 波[2]

[摘要] 信息网络技术的应用为军队医院的发展创造了契机,同时也带来了新的问题。面对新形势下军队医院信息安全管理的挑战,本文根据军队医院建设发展需要,结合某医院信息安全的管理实践,从技术策略与管理制度两方面探讨了加强军队医院信息安全管理问题。

[关键词] 信息安全;军队医院

[中图分类号] R197.32 [文献标志码] A doi:10.3969/j.issn.1672-271X.2013.02.040

医院信息系统的安全性直接关系到医院医疗工作的正常运行,网络瘫痪或数据丢失、失密将会给医院和患者带来巨大的损失。随着改革开放的不断深入、高科技的迅猛发展及广泛应用,军队医院信息化水平的不断提高,临床、医技、管理等各个部门的日常工作已经越来越依赖医院的网络和信息系统,但也同时为医院信息安全带来了许多新的问题和挑战[1]。如何在新形势下,根据信息传播本身的特点,加强军队医院信息安全管理,确保信息保密安全,已成为医院管理的新课题。笔者结合本院信息安全管理实践,从技术策略与制度管理两方面谈点粗浅体会。

## 1 技术策略

医院信息安全的维护需要专业技术保证。信息系统安全防护技术的研发与应用是保证医院信息系统的稳定性、可靠性、安全性、可用性的利器[2]。为保障医院信息系统安全稳定,我院采取如下技术策略以提升安全性。

**1.1** *异地备份策略* 异地备份的目的是在数据信息丢失与损害的情况下保证数据的恢复使用。我院在保证日常操作的主数据中心正常运转的基础上,设立异地的灾难备份中心,采用冗余备份技术、双机热备技术、集群和负载均衡技术等以保持与主数据中心运行系统的数据完全同步,保证数据的安全性[3]。对于介质故障所引起的信息数据丢失可对数据库完全恢复;对于导致系统不能正常使用的人为错误可通过不完全恢复将数据恢复到误操作前的时间点。

作者单位:210002 江苏南京,南京军区南京总医院,1.政治部,2.医务部

通讯作者:袁 波,E-mail:ybo_2001@163.com

**1.2** *物理安全策略* 物理安全策略的目的是保护计算机系统、网络服务器、打印机等硬件实体和通信链路免受自然灾害、人为破坏。我院对医院所使用的"军字一号"系统、院内政工网、办公自动化网互联网等网络之间严格实行物理隔离;通过 Nokia 防火墙硬设备防止外部入侵,确保各种信息安全;同时,对中心机房进行改造,配备了机房动力设备及环境集中监控系统,可对机房内专用空调、配电系统进线与系统主要支路、UPS、防漏水检测、门禁、温湿度等进行监控。通过遥测、遥信、遥控和遥调等功能实时监控机房内各类设备的运行状态,并在被监控设备出现故障后实时通过发送手机短信的方式通知值班人员[4-5],确保机房设备安全。

**1.3** *访问控制策略* 访问控制是网络安全防范和保护的主要策略,它的主要任务是避免网络资源被非法使用与访问。医院网络用户分散处理、高度共享,用户涉及医生、护士、医疗技师、管理人员等。为此,我院网络中心取消网络中的共享资源,对必须共享的资源设置为只读或加访问密码以控制访问权限。通过设定权限控制用户对特定数据的使用,使每个用户在整个系统中只具有唯一账号,既方便灵活地操作自己的程序和调用数据,又禁止用户对无关目录进行读写。由网络管理员进行网络安全配置,包括入网访问控制、网络权限控制、网络监测和锁定控制、网络服务器安全控制和防火墙控制等网络属性安全控制,从而保证了数据信息安全,避免网络资源滥用。

**1.4** *信息加密策略* 加密技术是网络安全一项有效的技术,它不但可以防止非授权用户的搭线窃听和入网,而且也是对付恶意软件的有效方法。信息加密的目的在于保护网内的数据、文件、口令和控制信息,保护网上传输的数据。我院对于涉密信息

进行加密处理,根据一定的算法将原始数据变换为不可直接识别的格式,并定期进行口令管理,配合访问用户权限的设定以降低信息使用风险。

**1.5** 防病毒控制策略 网络病毒的散播严重威胁着医院信息安全与网络稳定,病毒防治是目前信息化医院网络安全策略的重点。我院在服务器安装网络版杀毒软件,并通过统一的控制台对数据中心的所有病毒防范系统进行管理。指定专人对杀毒软件进行管理与维护,每周更新病毒代码,并实现防病毒产品升级无需人工干预,在预定时间自动从网站下载最新的升级文件,并自动分发到局域网中所有安装防病毒软件的机器上。

## 2 管理策略

除采用上述网络安全技术措施外,我院还加强网络安全管理,制订有关规章制度及应急预案,从而确保各类信息的保密安全和网络数据安全。

**2.1** 加强安全保密教育 定期组织全院人员进行保密安全教育,不断强化保密和信息安全意识。通过组织学习保密规定和网络系统操作使用安全管理规定,明确信息安全相关法规制度;通过举办信息系统操作应用培训,不断提高全体员工的网络安全维护和信息系统安全操作技能。

**2.2** 制定应急处置预案 为保障信息系统的不间断运行,保证事故发生时以最短时间、最小损失恢复系统,我院信息安全部门制定了各类应急预案。根据信息安全风险评估情况,对有可能造成损失的系统优先制定应急方案,并在发生问题时优先启动、恢复,对重点部门、关键业务重点保护;对于不同故障情况,如针对网络系统、服务器、病毒感染等,制定了不同的技术性应急预案。为熟练应急预案操作过程、检验系统安全备份策略的可靠性,我院信息部门定期组织应急预案演练,不断提高应急处置能力。

**2.3** 严格各项管理规定 认真遵守《中国人民解放军计算机信息系统安全保密规定》,严格执行"军字一号"工程技术组行政法规、用户手册和其他计算机安全使用规定;建立并完善医院网络安全责任制与上报制度;实行计算机网络系统安全等级保护和用户使用权限划分,安全等级和用户使用权限以及用户口令密码的划分、设置由计算机中心负责制定和实施。为促进医院信息安全制度落实,我院还定期组织保密和医疗信息安全检查,及时消除安全隐患[6]。

**2.4** 注重病人信息保密 我院除了担负普通官兵、老干部及家属、社会群众的医疗服务保障任务,还肩负着军区高级领导干部的医疗服务保障任务。对于高级领导干部的个人信息以及相关治疗内容,严格按照保密规定要求,控制知密范围。对反映高干病区的临床信息统计,严格把关、仔细审查,隐去个人信息,在保证试验描述完整性的同时,竭力做好保密工作。对于一般患者的个人信息,也注意做好保密工作,凡涉及患者姓名、ID号码、家庭住址等信息均予以删除,确保个人隐私[7]。

**【参考文献】**


[1] 甄保社. 军队医学图书馆信息安全保密工作[J]. 中华医学图书情报杂志,2008,17(1):58-60.

[2] 陈海东,宋 斌,余赛玉,等. 区域医疗信息系统的设计[J]. 东南国防医药,2011,13(1):82-84.

[3] 胡 敏,徐旭东,张曙光,等. 医院信息性系统容灾方案的设计与实施[J]. 医疗卫生装备,2009,30(11):44-45.

[4] 杨霜英,胡新勇,杨国斌,等. 大型医院网络信息系统的安全保障策略[J]. 中国医疗设备,2009,24(10):36-38.

[5] 王杭兵. 南京军区南京总医院智能化楼宇信息系统的设计与实施[J]. 医学研究生学报,2012,25(4):402-405.

[6] 王 浈,雷万生,徐劲松. 设立"六到位"医疗安全管理目标的实践[J]. 东南国防医药,2012,14(1):86-88.

[7] 汪惠霞,王慧琳,李风华. 住院患者护理信息系统的应用[J]. 医学研究生学报,2011,24(1):72-74.


(收稿日期:2012-09-27;修回日期:2012-12-07)

(本文编辑:史新中)