大型医院网络信息系统的安全性设计

随着计算机网络技术应用的深入，系统安全性问题变得日益突出[1]。如何确保医院信息系统持久、正常、安全地运行是设计和建设医院信息系统时必须考虑的。我院是一所集医疗、教学、科研、急救、预防为一体的综合性三级甲等医院，年收住院病人近3万人次。本文将针对我院计算机网络信息系统的安全性解决方案进行论述，并对医院信息系统安全性建设作一些初步探讨。

1　计算机网络信息系统安全性的实现策略

为了保证我院信息系统高效、安全、稳定地运行,我们在医院网络信息系统的安全性设计方面,采用了以下一些策略:

1.1　采用高性能、高稳定性的网络服务器

我院信息系统的核心服务器选用的是两台IBM公司的PSERIES650小型机。该型机器具有以下安全特点:(1) 杰出的TPC-C性能。PSERIES650小型机是业界高端UNIX服务器产品IPC-C性能领先者，可配置2到8个处理器-具有 1.2 GHz、64位处理器速度和从2 GB到64 GB的主内存。(2)基于铜芯片和绝缘硅技术的高性能CPU。(3)高性能的Date Switch(数据交换通道)技术。可以同时提供多条总线通道而减少内存总线拥挤的问题，是目前SMP UNIX系统技术的领先者。(4)领先的UNIX 操作系统AIX。AIX操作系统连续6年被D.H Brown公司评为操作系统第一，并且充分考虑了用户对安全保密性的要求，达到了美国NCSC的“C2”级别。(5)最高级别的系统整体可靠性。达到欧美的计算机系统安全的最高级别。(6)领先的CPU制造工艺。(7)CPU动态再分配。(8)冗余设备设计。(9)先进的SSA技术。(10)高可用性的集群方案(HACMP)。

1.2　建立完善的数据存储和备份机制

我院的数据存储整体架构采用了存储局域网(SAN)的方式：后端采用IBM FAStT600磁盘阵列作为统一的存储设备；中间层面采用两台IBM H08 SAN光纤交换机作为SAN的骨干设备；前端的两台IBM PSERIES650小型机通过光纤控制卡(HBA卡)直接接入到SAN中。两台小型机之间由一根串口心跳线连接，组成双机机群，并通过VERITAS NetBackup软件对系统信息和数据库文件进行备份。实现灾难的冗余，保证业务的不宕机运行。

1.3　选择高性能的网络交换设备

我院整个网络系统全线采用了美国CISCO公司的千兆以太交换机。其中网络边缘交换机选用了CISCO的Catalyst 2950系列产品,部门级的交换机则采用了Catalyst3550系列产品,核心骨干交换是由2台CISCOCatalyst6506企业级交换机组成的双机热备系统。

1.4　根据用户的分类划分虚拟局域网,以提高网络的安全性和保密性

虚拟局域网(VLAN)以交换式网络为基础，把网络上的用户(终端设备)划分为若干个逻辑工作组，每个逻辑工作组就是一个 VLAN。它不受网络用户的物理位置限制。我们在医院网络建设中,根据用户的工作性质和楼宇的不同分布，把医院网络用户依次分类,分为医保子网、财务子网、临床子网等近20个不同的VLAN。目的在于不用改变网络的硬件环境下可以将物理上不同的子网设定为一个逻辑子网,这样有效隔离广播风暴并简化

了网络的结构和管理。

1.5　应用网管和防病毒软件及防火墙技术防止黑客和病毒的入侵

随着医院网络信息系统的不断扩大，对网络和应用系统进行综合监控和管理，保障信息系统的通畅、稳定运行，保证信息服务的质量，已经成为信息系统管理人员的核心任务[2]。采用高效、便捷的网管软件将会为管理好网络起到事半功倍的效果[3]。我院采用的是由上海北塔公司开发的BTNM网络运维管理系统。

我院网络信息系统的医保接入是通过网通线路连接市、区两级医保中心的,为了保证网络的安全，防止黑客入侵，我们在网络出口加装了防御FIREGATE型硬件防火墙。防御防火墙充分考虑了用户对效率的重视性，拥有足够的数据吞吐能力。它除了防火墙模块外，还集成了入侵检测功能。实现了动静结合，立体防御，能够随着新攻击手段的出现而不断升级，真正做到全周期的动态安全保护。此外，为了防止网络病毒的侵袭，我们设立了防病毒服务器，安装了网络版趋势防病毒软件，以求及时发现或侦测病毒的入侵，并能及时杀灭病毒，从而保证整个系统程序和数据的安全。

1.6　UPS电源保护和网络防雷的策略

UPS电源保护是保证整个医院网络信息系统正常、安全运行的重要举措。为确保医院信息系统7*24 h的连续运行，在精确计算了医院网络设备的电流负载量并作相应的冗余设计后，我院实施了三级UPS电源保护机制。首先在信息中心机房配置了2台EAST EA8600系列UPS电源组成了双机热备UPS系统，保证了中心服务器、核心交换机等主要设备在断电8 h内仍能正常运转；其次在各楼宇通信机房内配置了1台EAST EA900系列 UPS电源，保证了各部门级交换机及其它网络设备在断电4 h内仍能正常运转；再次在各底层工作站旁都配置了EAST EA200系列 UPS电源保证了断电1 h内仍能正常工作。

我院的网络传输线主要使用的是光纤和双绞线。其中光纤不需要特别的防雷措施，但我们还是将光纤的金属部分接地。而双绞线以太网是目前应用最多的方式，由于双绞线屏蔽效果较差，因此感应雷击的可能性比较大，对于跨越房间、接近窗口或在室外的双绞线和网络设备之间均良好接地，以防止双绞线引入的过电压损坏与之相连的网络设备。

2　信息系统的安全性评价

基于上述安全策略构建的我院网络信息系统，在运行中，一直保持了安全稳定的运行态势，基本上没有出现异常的情况，有效地保证了我院日常业务工作的正常运行。我们认为，采用了上述安全性设计方案，基本达到了设计要求，并能有效地保证医院信息系统的正常运行。可以说还是一个实用性较强的方案。

参考文献:

[1]刘其奇, 赵翠霞. 企业网络安全性机制的建立[J]. 计算机工程, 2000, 12-4.

[2]魏洪波, 晏蒲柳, 王海燕. 分布式系统的网络安全性分析及策略[J]. 微计算机信息, 2002, 11-3.

[3]马丽娅. 医院信息系统的风险分析和安全策略[J].医学信息，2000, 10-2.

回结果列表