医院面临的信息安全问题与应对分析

穆成欢

(宁波市中医院信息科,浙江 宁波 315010)

摘要:近年来,随着信息技术和网络安全技术的快速发展,医疗行业的信息化水平得到了显著的提高。医院的总体网络环境也变得逐渐复杂,使信息安全的要求逐渐提高。本文通过分析医疗行业信息系统在基础设施安全、服务器终端安全、网络安全、数据存储安全、软件应用安全和管理安全方面存在的问题,并结合当前的网络安全技术和安全管理手段,实现保障医院信息系统安全,提高医疗数据安全质量。

关键词:医院信息安全;安全应对;机房建设;管理与维护;网络安全

中图分类号:R197 **文献标识码**:B **DOI**:10.3969/j.issn.1006-1959.2024.01.007

文章编号:1006-1959(2024)01-0041-04

Analysis of Information Security Problems and Countermeasures Faced by Hospitals

MU Cheng-huan

(Department of Information,Ningbo Hospital of Traditional Chinese Medicine,Ningbo 315010,Zhejiang,China)

Abstract:In recent years, with the rapid development of information technology and network security technology, the informatization level of medical industry has been significantly improved. The overall network environment of the hospital has also become increasingly complex, so that the requirements of information security have gradually increased. This paper analyzes the problems of medical industry information system in infrastructure security, server terminal security, network security, data storage security, software application security and management security, and combines the current network security technology and security management means to ensure the security of hospital information system and improve the security quality of medical data.

Key words:Hospital information security;Security response;Machine room construction;Management and maintenance;Network security

近些年,信息安全在医院信息化持续发展的今天显得格外重要。维护医疗秩序,确保医疗救治工作,提高医院工作效率,对于加强医院信息安全管理意义重大。根据国家信息安全等级保护制度,医院信息安全从 5 个维度分析,主要涉及物理环境、网络安全、主机安全、数据安全、应用安全等方面[1]。经研究发现,现医院面临诸多信息安全问题,导致医院信息系统面临安全风险,若不重视医院网络信息的安全防护,那么医院的各项信息安全都无法得到保障,这对于医院的运行和管理有着很大的隐患[2]。本文以医疗信息系统存在的问题,通过基础设施、服务器、网络、数据存储、软件应用和管理方面进行分析,分别描述当前医院信息系统存在的风险和问题,并寻找采取相应的应对措施。

1 医院信息安全问题分析

1.1 基础设施安全 医院信息系统的基础设施安全包括了整体机房安全和信息设备安全,是承载医院信息系统的基础条件。首先医院难免会经历停电,如果停电时间过长,压力会集中在 UPS 系统上,长期负载会导致 UPS 故障[3]。另外中心机房的环境会很大程度影响设备的运行情况,机房的温度、湿度、尘埃、照明等因素影响机房内设备的使用寿命和运行状态。然而,信息安全人员一般常将重点关注在机房的信息设备上,机房的环境容易忽视,温度过高,湿度过大,粉尘过多,机房环境杂乱,将各种杂物堆放,设备的堆叠放置等因素都会对机房的安全产生巨大影响,也影响了机房设备的可靠性。

1.2 服务器终端安全 服务器作为医院信息系统运行的环境,终端主机作为实现医院信息化平台的媒介,其重要性不言而喻。医院服务器和网络设备是承载业务系统的重要基础设施,服务器安全直接影响到全院业务安全[4]。当前医院服务器操作系统主要以 linux 系统和 windows 系统为主,终端主机的操作系统大部分均以 windows 操作系统为主。在目前的网络环境下,服务器终端面临的安全问题也是多种多样的,主要包括身份鉴别、访问控制、安全审计、入侵防范和恶意代码防范[5]。黑客通过一般互联网、U 盘的形式利用蠕虫、病毒、木马等工具对现有的主机环境进行破坏,利用服务器操作系统的漏洞对其进行攻击。

作者简介:穆成欢(1993.8-),男,浙江宁波人,本科,主要从事网络安全管理

1.3 网络安全 随着医疗业务的拓展以及各个系统之间数据的不断交互,医疗系统的网络结构也变得越来越复杂,网络规模也逐渐扩大,趋于覆盖整个医疗环境。但还有部分医院的网络结构存在问题,网络设备和安全设备等已经使用较长时间,呈老化状态[6],单链路的网络环境使医院的可靠性受到了影响,当出现某台设备故障时将直接对医院的业务产生影响;未做访问控制策略也会对医院的安全造成巨大的隐患,这也就意味着网络环境没有限制,即同时访问内外网系统,这也大大加增加了医院的系统感染外网病毒的风险;随意地接入各种未知设备会使医院的网络结构变得更加混乱,例如未经规划而随意地接入了交换机后,可能导致医院网络产生环路。随意接入的家用路由器由于未关闭默认开启的 DHCP 功能,导致医院的网络环境中可能会存在各种干扰的 DHCP 服务,影响医院网络的正常运行;医院网络结构问题还包括随意的端口映射引起的 DOS 侵入等黑客攻击。

1.4 数据存储安全 在当今的医疗环境下,随着信息化技术的全面普及,医院信息的存储方式也趋于无纸化,数据的存储安全成为了信息安全的核心内容。数据存储有着真实性高、速度快、数量大、种类多等特点。而医院的数据存储安全也存在着诸多的隐患。数据的丢失会影响医院业务的正常运行,对医院造成巨大的损失。而数据资料的外泄,困扰的不仅仅是患者的隐私,医院的声誉也会受到影响。在医院的日常管理工作中,数据库的安全管理问题往往被忽视,这就为不法分子创造了便利条件[7]。

1.5 软件应用安全 在当前的网络环境下,运维管理者往往将安全防护的重心放在网络和操作系统层面,通过防护外界对操作系统的攻击实现系统防护,从而忽略了应用本身存在的漏洞。而与安全相关的程序缺陷可以被恶意程序利用,使程序宿主机器受到侵害[8]。攻击者经常通过软件的漏洞攻击医院系统,而在 web 应用中常常出现 XSS 攻击,攻击者通过植入代码到 web 页面中盗取用户账号信息,控制医院数据,盗取医院重要数据等;SQL 注入是将 SQL 命令插入 web 表单,通过欺诈服务器执行恶意 SQL 命令,攻击一旦成功轻则获取网站敏感信息,重则植入木马,控制服务器。此外,软件应用安全威胁还包括错误的安全配置和失效的身份认证等。

1.6 管理安全 医院信息系统的安全管理包括机房管理、设备管理、软件管理、数据管理、人员管理、系统管理、操作管理、备份管理、配置管理、应急预案等。医院安全管理的建立和完善,可以使医院在突发事件的处理上更好。而医院当前存在的安全管理问题主要为信息化安全制度不完善、审计不全面、疏于巡检、访问控制不细致、权限分配不合理、缺乏信息安全培训、文档资料不积累等。另外部分医院对内部医护人员的网络安全教育较少,在出现问题后将所有责任归结于网络科技公司[9]。上述问题会导致医院系统面临异常时,无法尽快恢复到现有的状态,并造成资料的缺失和数据的错误,给医院的工作带来影响。

2 医院信息安全应对策略

2.1 基础设施安全 首先是对机房场地的选择。选择机房的场地应为相对独立的区域,保证周围没有噪音污染,没有水源,没有粉尘污染,且避开磁场。另外在建设网络中心机房时,要选择使用不间断的供电电源,保证网络服务[10]。为方便信息技术人员的日常巡检和运维,建议机房选择距离办公室较近的区域,当出现紧急状况时方便信息技术人员第一时间赶到现场。信息机房的建材需选择抗静电的地板,选择的吊顶材料应具备一定的防水,防火等效果,拆装方便,并且具有一定强度。作为墙体的建筑材料,必须满足防火、耐雨、防震等效果。其次是对机房的整体监测。需安排专人对机房进行监控和维护,并在机房安装环境监控系统,监控机房的温度,湿度,烟感等情况;通过安装电子门禁对出入机房的人员进行记录;通过安装监控摄像头对机房人员的行为进行监控记录。最后是对机房设备的安全管理。机房的设备应按相应的区域进行安装上架,且设备的间隔保持 1 U 的空间,防止设备应无法充分散热导致的设备故障,并且需在机房配置 UPS,防止因断电导致系统瘫痪。

2.2 服务器终端安全 安装杀毒软件是对服务器终端安全最基础也是最有效的应对方案。安装杀毒软件不仅可以防止网络环境中大部分病毒对主机的攻击,也可以对系统中已存在的恶意软件和病毒进行清理。一些简单的,常用的密码常常容易遭到暴力破解,对密码的选择,需要根据等保要求,选择具有一定复杂程度的密码,密码的复杂度需满足有数字,大小写字母以及特殊符号的 8 位以上字符串;对服务器而言,增强安全性的方式可以通过修改默认的用

户名。对于服务器主机存在的安全漏洞，常通过漏洞扫描技术对系统内存在的漏洞进行探查，并根据存在的系统漏洞进行相应修补。服务器的操作也需要进行相应的规范。通过堡垒机或集中管理平台对服务器操作系统进行统一管理，能够及时更新补丁，并实行统一的登陆账号密码管理和访问控制入口[11]。

2.3 网络安全 医院的网络架构采用核心、汇聚、接入的结构，为保障网络稳定，首先需对核心交换层选择使用双核心机构，汇聚交换层则采用双汇聚结构[12]；其次是对边界的路由器或防火墙的高可用性配置；最后是优化系统的网络质量，配置相应的 QOS 以减少传输延时、减少数据丢包率、延时抖动等。内外网隔离技术减少了医院网络受到外界的攻击，可以通过核心交换机或防火墙配置的访问控制策略实现网络的逻辑隔离，也可以通过使用网闸设备来实现物理隔离。对于必须要访问外网的设备，可在内外网的安全域边界设置访问控制策略，配置到具体端口，禁用不必要的端口[13]。为防止外来人员接入医院的网络，入网规范管理设备可以允许经过认证的设备接入医院网络，而未经认证的设备无法访问；针对 DHCP 攻击的防范措施可以通过使用固定的 IP 地址，该方式不仅可以防止接收 DHCP 服务器下发的地址分配，防止 IP 地址的变更，还可以方便医院信息人员通过 IP 地址定位使用人员。

2.4 数据存储安全 数据安全对医院的重要性可谓不言而喻，为防止数据泄露，侵犯患者的隐私权，可以对医院的主机限制 U 盘、移动硬盘等存储媒介接入，只有经过审核的存储媒介才能接入医院主机，不仅可以防止医院信息数据外泄，还能防止外来病毒扩散到医院网络。还可以采用数据库核查技术，对访问数据库的行为进行安全核查[14]，保证数据的安全性。另外内外网隔离也可以使医院内网的信息系统数据无法通过互联网的方式对外传播。对医院的信息系统进行数据备份能够防止医院数据丢失，当出现主系统存储故障时可以通过备份系统还原数据，保障医院业务工作正常进行。对于医院的核心业务，不仅需要通过本地备份，还需要使用异地备份。以免因地震、火灾、水灾等因素破坏机房后导致的数据丢失。在保证内部的数据不丢失的情况下，对数据的审计也至关重要。医院内很多数据的传输涉及到医生和患者的信息安全和个人隐私等，在这个过程中，进行关键数据审计工作，及时对数据读取使用进行回溯，防止医疗纠纷的出现[15]，并可以对医院内员工的操作行为进行监督。当出现网络安全恶意行为或操作失误时，可以通过回调审计日志对员工的行为进行追责。

2.5 软件应用安全 为避免因软件应用而导致的系统故障，对软件应用的处理方式需采用测试、修复、审计和防护。测试即软件应用系统的测试，主要通过对测试软件的加密机制，用户的认证机制等内容。在代码测试前建议开发人员提前对代码进行扫描，减少代码的出错率。在测试阶段通过安全测试执行，通过安全漏洞检测，检查软件的跨站攻击，sql 注入等漏洞，并形成漏洞检测报告，并对相应的漏洞进行修复，确保软件系统在交付时经过全面的测试流程。软件在开发和使用的过程中如果有完善的软件测试机制在一定程度上可以降低软件的安全隐患问题[16]。修复即对系统的软件漏洞进行修复，在现有的业务环境中，当检测到业务系统存在系统漏洞，应提前做好好必要的安全测试，确保不会和系统中已有的应用程序相冲突，保障其正常运行[17]，修复后再次测试并记录报告。审计是检测相关的安全事件，辨别该事件是否需要记录，或报警，对存在威胁的日志发出报警，并形成安全审计报告过程。安全审计能够震慑潜在的攻击者，收集遭到破坏的证据并提供有价值的日志，确保遭到攻击后找出事故的原因。

防护即通过使用安全设备和访问控制策略实现的安全防护。在医院的信息系统中，通常通过防火墙，WEB 应用防护、入侵防御系统等安全设备对网络中的漏洞扫描、漏洞攻击等恶意行为进行阻断；通过访问控制策略，仅开放使用的服务端口，拒绝所有其他端口，减少安全隐患。

2.6 管理安全

2.6.1 人员管理 人员管理的内容分为两种，一是对人员的培训，为加强信息安全人员的技术水平和操作水平，在面临应急故障时能尽快排查故障原因，减少系统中断时间；另外对医院的各职工进行安全意识培训，普及信息安全事故导致的危害，认识信息安全的重要性，并定期对员工进行考核，考核的基本内容包括对信息安全认知及技术的考核，从而保证每位工作人员在工作过程中都能履行其保护医院信息安全的责任[18]，从而减少人为因素引起的信息安全事故。二是对人员职责和权限的合理分配，只有分配

合理的权限，员工按照自己的职责根据流程执行工作，不仅能防止越权事件的发生，还能提高工作的效率。

2.6.2 设备管理 保障设备管理的主要方式为巡检，巡检分为日常、月度和季度巡检。日常巡检需要每天关注机房设备的运行状态并记录，对安全审计的设备实时关注，及时处理日常的安全问题；月度巡检需要记录服务器状态，所有安全设备的运行状态，以及对设备的版本进行等；季度巡检需要检查所有的网络设备和安全设备运行状态，并对该设备的配置备份到本地。此外，网络设备、主机、数据库、应用系统等也需要通过漏洞扫描的方式来检查自身存在的问题，提高对黑客攻击和病毒攻击的防御力。

2.6.3 文档管理 在医院工作过程中，由于工作内容不会是一成不变的，复杂的工作内容和工作量，随着时间的推移会逐渐的遗忘当初的工作内容和工作思维，因此对系统操作内容和原因的记录尤为重要。通过制定相关的文档管理制度，对工作中配置产生的变更进行审核管理和记录，加强了档案管理工作的标准化 、程序化、规范化[19]，当信息系统出现故障时能够更有效的寻找故障原因，并提供了丰富的台账资料，有利于总结信息安全的历史趋势。

2.6.4 应急预案 为保证处理应急事件的能力，医疗机构应安排每年两次以上的应急演练，通过模拟网络、服务器、数据库、存储等设备故障，提高对突发事件的认识和处理流程，熟练面对突发事件的应对措施，当医院真正发生突发事件时可按应急预案处置，最大限度的避免影响医院业务。

3 总结

随着医院的信息化安全快速的发展，当今医院存在的问题也日益严峻，对医院的信息化发展造成巨大的安全隐患，甚至会影响正常的业务使用。因此，只有高度重视信息安全问题，全方位、多角度地考察网络安全漏洞和弱点。有针对性的对当前存在的问题采取相应的措施，结合医院的安全体系和规章制度，应对面临的风险，保证医院系统的稳定运行和业务的正常使用。

参考文献：

[1]王建英,陈文霞,胡雯,等.医院信息安全分析及措施[J].中国病案,2013,14(9):56-57,47.

[2]刘小宇,李璐.基于“互联网+”背景下医院网络的信息安全防护[J].科技与创新,2022,(12):112-114,122.

[3]黄波.大型综合医院数据中心机房建设的实践[J].微型电脑应用,2022,38(7):140-143.

[4]蔡颐.三甲医院信息安全建设策略研究[J].海峡科学,2016(4):18-21.

[5]魏帅岭,李星,侯立根.基于三级等级保护的医院信息安全体系建设与评估[J].中国医疗设备,2020,35(11):142-145.

[6]臧璆,汪春亮.基于安全等级保护的医院网络安全优化方案实践[J].医学信息学杂志,2022,43(3):79-83.

[7]何娇楠,杨世龙.医院计算机网络信息系统的安全风险与控制策略[J].电脑知识与技术,2018(8):17-18,21.

[8]李舟军,张俊贤,廖湘科,等.软件安全漏洞检测技术[J].计算机学报,2015,38(4):717-731.

[9]贾维.数字化医院信息安全建设与管理策略[J].网络安全技术和应用,2021(2):129-130.

[10]陈谊.网络中心机房建设解决方案分析[J].数字化用户,2018,24(15):16.

[11] 吴汉耿. 基于灾害脆弱性分析的医院信息安全建构策略[J].管理观察,2019(21):182-184.

[12]唐超琪.医院信息安全等级保护整改设计研究[J].电脑编程技巧与维护,2022(4):160-162

[13]周毅,潘敢,殷鸣.医疗机构信息安全探析[J].医学信息学杂志,2019,40(5):41-43,47.

[14]何启红,曾理.如何确保医院信息安全[J].中国卫生质量管理,2018,25(6):80-82.

[15]王晨旭,李刚荣,吴昊.浅谈医院信息安全管理[J].中国卫生信息管理杂志,2011,8(5):33-35.

[16]杨鹏.计算机软件安全及其防范的研究[J].中文信息,2018(11):5-6.

[17]苗智翔.信息安全漏洞浅析[J].数字化用户,2018,24(51):113.

[18]李大鹏.基于等级保护要求加强医院信息安全管理[J].网络安全技术与应用,2019(7):103-104.

[19]丁嘉颖.浅谈医院办公室的文档管理[J].卷宗,2019,9(31):50.

收稿日期：2023-02-02；修回日期：2023-03-07

编辑/成森