基于物联网技术的医院网络安全保护方案的设计与实施

邱成江
（郓城县程屯镇中心卫生院 山东 菏泽 274700）

摘 要 随着时代的发展与技术的进步，现代医院的运行与服务模式也发生了一些变化，加强医院网络安全保护与管理已成为技术人员需要解决的关键课题。文中以医院网络安全防护需求为切入点，分析了物联网技术在医院网络安全中的应用价值，并基于准入控制、漏洞管理、态势感知等角度，设计了医院网络安全保护方案，最后对物联网技术支持下的医院网络安全保护方案的应用成效进行了探究，以期能为有关从业者提供参考。

关键词： 物联网技术；医院管理；网络安全保护；方案设计
中图分类号 TN915.08

Design and Implementation of Hospital Network Security Protection Scheme Based on Internet of Things Technology

QIU Chengjiang
（Chengtun Town Central Health Center,Yuncheng County,Heze,Shandong 274700,China）

Abstract With the development of the times and the progress of technology, the operation and service mode of modern hospitals have also undergone a series of changes, and strengthening the protection and management of hospital cyber security has become a key issue that technicians need to solve. This paper takes the hospital cyber security protection needs as the starting point, analyzes the application value of Internet of Things technology in hospital cyber security, and designs the hospital cyber security protection scheme based on the perspectives of access control, vulnerability management and situational awareness. Finally, the application effect of the hospital cyber security protection scheme supported by Internet of Things technology is explored, in order to provide reference for relevant practitioners.

Key words Internet of Things technology, Hospital management, Network security protection, Scheme design

0 引言

物联网技术可以通过信息传感设备实现物体与网络的相互连接，有效提升信息传输效率，实现智能化的识别、定位、跟踪与监管，在安防管理与网络整合等领域发挥着重要作用。相关从业者应认识到物联网技术对医院网络安全建设带来的影响，推动医疗服务质量的不断提升。

1 医院网络安全防护需求分析

1.1 物理安全需求

在医疗事业发展与网络服务的过程中，设备设施安全有着关键作用。在设计与规划医院网络安全防护体系的过程中，技术团队应考虑网络设备的物理位置选择，避免人为因素或环境因素对网络设备造成影响，提升设备运行环境的稳定性与安全性，为医院网络的安全运行提供基础。

1.2 入侵防范需求

受到特定目的的影响，一些不法分子可能会利用网络中的漏洞对医院网络安全展开攻击，导致其网络设备及网络服务失效，使相关数据面临泄露的风险。因此，技术团队在建设网络安全防护体系时，也应加强对入侵防范的关注与重视，实现内外网之间的有效隔离，做好对恶意应用及病毒威胁的防范与控制，使医院网络的运行更加高效[1]。

1.3 访问识别需求

在开展医院网络安全保护工作的过程中，对网络用户的身份进行识别，能有效避免信息泄露，保障医院内部管理的正常开展。相关技术团队应积极引进身份辨识技术及访问控制技术，实现对内部网络系统通信的有效保护，避免无授权的恶意访问。

1.4 容错控制需求

受医院业务流程与特点的影响，其对网络体系运行的

作者简介：邱成江（1967—），专科，初级工程师，研究方向为电子信息工程

稳定性提出了较高的要求，但在长期管理和运行过程中，医院网络设备可能会产生大量数据冗余，这不仅增加了网络系统的维护成本，还可能会对医疗服务的质量产生影响。在建设与规划安全防护体系时，相关技术人员应当具备与时俱进的视野，加强对容错控制及冗余处理的关注，增加网络系统内部空间，及时优化医院网络系统存在的故障与问题，避免对医疗服务造成影响。

1.5 信息管理需求

医院网络系统内部涵盖了大量有关患者隐私的信息数据，这些信息数据是医院开展医疗服务的必要内容，但也对网络系统的性能形成了较大的压力。在网络安全防护体系内部，技术团队应进一步落实医院信息管理工作的要求，建立详细的信息分类管理机制，进一步提升网络系统的安全性，提高患者的满意度。

2 物联网技术在医院网络安全领域中的应用价值

为使医院网络安全保护方案的规划与设计更具可行性，加强对物联网技术的引进、开发与利用，相关从业者应结合实际案例，进一步明确物联网技术在医院网络安全中的应用价值，为后续工作的开展奠定基础。

2.1 威胁实时识别

在医院网络的运行过程中，受到业务形态、运行环境等因素的影响，导致其往往面临着一系列威胁与风险，对医疗服务的正常开展造成了较大的冲击与影响。将物联网技术引进医院网络安全保护体系中，能全面加强网络体系对外部威胁的感知与辨识能力。技术团队可采用射频标签技术，协同管理医院内部网络设备的运行状态，使安全管理人员能实时捕捉网络设备的运行状况及个性化特征，全方位感知网络设备面临的威胁，同时采取相关措施处置外部威胁，减少外部环境威胁对医院网络安全造成的影响[2]。

2.2 信息可靠传输

信息内容的稳定传输是医院网络安全的另一项重要前提。依托物联网技术，能全面整合医院内部不同网络设备的运行信息及反馈数据，实现信息格式的统一转换，使医院内部网络设备信息实现实时安全传输，有效加强设备之间的信息交互，为系统内部安全保障、威胁处置及故障诊断工作的开展提供依据。

2.3 数据高效处理

医院内部网络安全保护与管理工作的开展，离不开对数据的分析和处理。借助物联网技术，能对医院网络设备的运行信息进行全方位存储、分析与应用，实现对网络设备的智能化识别、监测与控制，使其能适应医院网络的差异化应用需求，为医患提供更加完善的网络服务。

3 医院网络安全保护方案设计

为进一步加强医院网络安全防护力度，提升安全保护工作水平，实现物联网技术支持下的安全保护目标，技术人员可以基于以下几方面开展保护方案的规划与设计工作。

3.1 安全准入控制体系

完善的身份验证与准入控制不仅能避免未授权用户的恶意访问，减少医院网络面临的安全风险，还能实现物理层面的设备安全，减少人为因素及环境因素对网络设备的影响，实现网络设备的高效运行与服务。

（1）在设计安全准入控制体系的过程中，应对终端设备进行类别划分，为后续网络体系安全保护与管理工作的开展提供支持。现阶段，医院物联网终端设备可分为传统终端与亚终端两种（按照应用方向及应用策略），其中传统终端涵盖了有线终端与无线终端，亚终端则涉及传感器设备、感应设备、激光扫描设备、定位设备、智能监控设备等。技术人员可结合实际情况合理划分设备终端，将其接入网络体系，为安全保障工作的开展提供助力[3]。

（2）应做好物联网终端与医院网络体系之间的相互关联与识别控制工作。在医院网络安全保护工作的开展过程中，应积极开展终端识别工作，以规避外来威胁，减少安全风险及安全隐患。因此，在将物联网终端接入医院网络体系的同时，技术团队还应将终端硬件编码、网络地址等信息录入网络中枢，使网关能有效识别、管理、控制终端，感知物联网终端的威胁特性，减少外部威胁对医院网络安全造成的影响，实现网络体系服务的可持续发展。

（3）应做好物联网终端的准入控制工作。为使物联网技术支持下的医院网络安全管理工作开展得更加高效、便捷，使终端识别与管控工作更加准确、可靠，应分别通过MAC地址、IP地址等标识符来标记物联网终端，使医院内网能更加有效地管控与协调入网设备，避免非法设备进入网络内部，提升终端管控效果。

3.2 威胁漏洞管理体系

医院网络体系内部的漏洞往往是外界攻击与威胁的主要渠道，因此加强对网络威胁漏洞的管理，成了医院网络体系安全管理的一项重要手段。在物联网终端接入医院内部网络的同时，受其接入形态、接入渠道等因素的影响，导致以亚终端为代表的设备终端大多面临着严重的安全隐患及威胁，大量物联网亚终端采用的密码口令较为简单，部分终端甚至未设置服务密码，导致其成为外部威胁攻击医院网络的重要途径。技术人员在应用物联网技术规划与设计医院网络安全保障体系的同时，也应考虑上述因素带来的影响，尽可能解决网络安全面临的威胁与漏洞，使医院内部网络安全得到有效的保护。

（1）在网络安全防护体系的规划与建设过程中，应配置漏洞识别与漏洞修复功能。技术团队可引进威胁采集探针等技术手段，分别对医院网络体系内部的漏洞情况及物联网终端接入威胁进行综合性的分析与探查，从实际出发，充分识别与分析医院网络服务运行过程中产生的安全风险及安全威胁，为漏洞的修复与处理工作提供支持。完成漏洞

识别工作后，技术团队可针对网络安全漏洞的形态与特点进行综合分析，同时采用密码口令变动、固件升级、补丁更新等方式实现对网络漏洞的及时修补，结合网络威胁分析等策略，判断安全威胁漏洞的状态，减少外部威胁对网络漏洞的影响。

（2）应做好对网络威胁信息的跟踪与整合。在物联网技术的应用与发展过程中，基于医院网络漏洞产生的威胁与攻击呈现出一定的规律性特征，这对漏洞修复及威胁控制等工作的开展提供了相应的帮助。技术团队在基于物联网技术设计医院网络安全保护方案的同时，应结合实际情况采集与整合外部威胁攻击信息，使相关数据信息能成为未来威胁管控、漏洞修补的依据，同时有效减少网络漏洞对信息化医疗服务开展造成的影响。安全技术团队可结合物联网平台反馈的网络威胁信息，明确其攻击规律，同时对未来攻击模式及攻击策略进行预测，并采取有效的措施来遏止相关攻击，避免其对医疗服务网络造成不利的影响[4]。

3.3 态势感知管理体系

在基于物联网技术开展医院网络安全保护工作的过程中，应结合网络环境进行态势感知，较为精准、全面地实现对医院网络威胁的识别与分析，推动医院网络安全防护措施的全面联动，提升防护效果，控制威胁要素对医院网络安全造成的影响与冲击。

（1）相关技术团队应认识到在物联网技术的支持下建设医院网络安全态势感知体系的意义，结合物联网传感器技术及终端信息反馈技术，建立起信息格式一致的态势感知管理平台，打造威胁识别、物联网防护及信息互联网保护三位一体的安全防护策略，遵循《网络安全等级保护2.0》的相关原则与要求，全面识别物联网技术支持下的医院网络环境及网络服务状态，综合判断院内网络终端接入情况及网络安全风险，使医院网络面临的安全威胁得到更加有效的控制与防范，减少其对医院医疗服务的影响。

（2）在态势感知管理体系的建设与应用中，应进一步强化传统流量网络的安全管理能力。为进一步减少恶意攻击及外部环境威胁对医院网络服务造成的冲击，技术团队在规划建设态势感知平台时，应引进特征匹配及白名单识别机制，结合医院网络历史运行数据及当下运行环境进行综合判断，将存在威胁的网络流量主体纳入管理名单，使医院网络能较为高效地分析和判断网络安全威胁及恶意攻击，提升医院网络对恶意攻击的监测与感知能力。

（3）应做好用户信息泄露的管理与控制工作。受医院网络服务内容及病患信息特点等因素的影响，在传统医院网络安全管理工作中，患者信息泄露等问题时有发生，对患者的合法权益造成了严重影响，同时对医院的社会口碑也形成了一定的负面影响。因此，相关技术人员应借助物联网技术，加强医院内网防篡改机制建设，有效减少病患信息泄露等问题的产生，提升医院网络的安全性，提高其安全保障能力与水平。

（4）应做好全周期数据安全管理工作。在传统的医院网络数据管理与应用工作中，受管理模式、管理流程等的影响，对技术团队的违规操作往往难以实现有效的识别、溯源和处理，导致数据库安全无法得到充分保障。技术团队在基于物联网技术建设医院网络安全体系时，应加强对数据库操作记录机制的开发，详细记录不同用户对数据库的操作，以便开展安全责任追溯工作，提升医院网络数据库的综合安全水平。

4 医院网络安全保护方案的应用成效

构建了物联网技术支持下的医院网络安全保护方案后，有效适应了新时代医院网络的发展与推广要求，使医院内部医疗服务数据的采集、传输、整合与存档工作的开展更加便捷，有效提升了医院患者隐私信息的保护水平，实现了从末端到源头的安全防范与安全治理，全面提升了医院网络内部的安全管理水平，使网络管理成本得到了有效控制。

5 结语

加强网络安全防护工作，对提升医疗质量、规避安全风险具有重要意义。相关从业者应结合物联网技术，积极开发医院网络安全保护方案，推动医院医疗网络的安全、稳定发展。

参考文献

[1] 孙唯一，沈崇德.基于物联网的医院智慧安全保卫云平台建设实践[J].中国卫生信息管理杂志，2022，19(5)：654-659.

[2] 陈庆龙，石春花，郝文延.物联网医疗系统安全和隐私保护方法研究[J].医学信息学杂志，2022，43(1)：67-72.

[3] 任斌，蒋昆，娄苗苗，等.一体化医疗物联网的建设框架与关键内容探讨[J].中国医疗器械杂志，2022，46(6)：686-690，700.

[4] 黄捷，潘愈嘉，莫禹钧.浅析医院物联网安全风险及防护体系的建立[J].中国数字医学，2021，16(5)：111-114.