医院网络安全建设中的社会化攻击防范技术与应用

杜东林

身份证号：440602198903201510

摘　　要： 医疗行业数字化转型加剧了医院网络安全风险，社会化攻击通过钓鱼邮件、身份伪装等手段威胁医疗数据与业务连续性。研究提出融合动态威胁感知、AI 行为检测与分层培训的一体化防护体系，结合《医疗卫生机构网络安全管理办法》（2024年5月）的“三化六防”要求，构建多层次防御架构与威胁情报共享机制。案例分析表明，AI 邮件过滤系统可降低90% 钓鱼攻击成功率，而零信任架构与区块链技术为医疗物联网安全提供新路径。研究为应对新型攻击与合规挑战提供理论支撑与实践参考。

关 键 词： 社会化攻击；医院网络安全；动态防御架构

Social Attack Prevention Technology and Application in Hospital Network Security Construction

Du Donglin

ID: 440602198903201510

Abstract: The digital transformation in the healthcare industry has exacerbated cybersecurity risks for hospitals, with social engineering attacks threatening medical data and business continuity through means such as phishing emails and identity spoofing. This study proposes an integrated protection system that combines dynamic threat perception, AI behavior detection, and tiered training, in line with the "three transformations and six defenses" requirements outlined in the "Cybersecurity Management Measures for Medical and Health Institutions" (issued in May 2024), to build a multi-layered defense architecture and threat intelligence sharing mechanism. Case analysis shows that an AI email filtering system can reduce the success rate of phishing attacks by 90%, while zero trust architecture and blockchain technology provide new pathways for securing the Internet of Medical Things (IoMT). This research provides theoretical support and practical references for addressing new types of attacks and compliance challenges.

Keywords: social engineering attacks; hospital cybersecurity; dynamic defense architecture

引言

随着医疗数字化转型，医院信息系统开放性和互联性增强，网络安全威胁也更复杂。社会化攻击如钓鱼邮件、伪装身份等，因其隐蔽性和针对性成为数据泄露和业务中断的主要风险。据统计，91% 的勒索病毒攻击源自内网设备漏洞，医护人员安全意识薄弱加剧了风险。2024年《医疗卫生机构网络安全管理办法》要求落实“三化六防”措施，并强化数据全生命周期安全管理。现有研究多关注传统防护，忽视社会工程学攻击的防范，尤其是在医疗设备互联和跨机构数据共享方面的防护技术与管理机制不足。需构建融合动态威胁感知、智能行为检测与分层人员培训的防护体系，以应对新型攻击和合规要求，确保医疗业务连续性和患者隐私安全。

一、 社会化攻击对医院网络安全的威胁分析

（一）社会化攻击的定义与主要类型

社会化攻击（Social Engineering Attack）利用心理操纵或信息欺骗，诱导目标泄露敏感信息或执行危险操作。在医疗领域，这主要体现为三类：钓鱼攻击，如伪造医疗通知诱使医护人员点击恶意链接；伪装攻击，仿冒权威身份骗取系统权限或患者数据；诱骗式攻击，通过虚假医疗信息扰乱医院运作或勒索。医护人员因职业压力大、需快速响应，更易受攻击，特别是在紧急状况下易出现决策盲区，使得攻击者有机可乘，窃取医疗系统登录凭证或患者信息[1]。这种攻击不仅威胁信息安全，还干扰诊疗过程，严重时危及患者生命安全。

（二）医院网络安全的脆弱性特征

医院网络安全脆弱源于业务与技术架构的特殊性。技术上，医疗设备如影像设备、生命监护仪通过物联网互联，但因设计时侧重功能而非安全，导致固件更新慢、默认密码未改等问题，终

端防护薄弱。为满足数据共享需求，医院网络需频繁与外部平台交互，扩大了攻击面。人员方面，医护人员缺乏系统的网络安全培训，在高压环境下易忽视安全规范，如随意连接公共 WiFi 或点击未知链接[2]。加之医院组织结构复杂，不同角色权限差异大，攻击者可利用低权限账户横向渗透。这种技术和意识上的“双重短板”，使医院成为社会化攻击的主要目标，亟需制定并实施针对性的安全策略以加强防护。

二、 社会化攻击防范技术体系构建

（一）技术防护体系设计

针对医院的社会化攻击，需构建多层次防御架构。网络层通过深度包检测（DPI）识别异常通信模式，并结合医疗设备白名单机制阻止非授权访问；终端层部署用户实体行为分析（UEBA）模型，对医护人员操作习惯建模，实时监控异常登录和数据导出等风险行为；数据层采用动态加密与脱敏技术保护敏感信息，在存储、传输及共享过程中最小化暴露患者隐私[3]。建立动态威胁情报共享机制，整合内部安全日志与外部威胁情报平台（如医疗物联网漏洞库、社工攻击案例库），通过自动化分析生成防御规则，实现跨机构的风险联防联控，提升整体安全性。

（二）关键技术应用与实践

AI 驱动的异常行为检测技术利用机器学习模型分析邮件内容和发件人行为模式，精准识别钓鱼邮件特征，如仿冒域名、紧急诱导话术，实验显示其误报率可低于2%。结合生物识别与多因素认证技术，在医疗系统登录、处方开具等关键环节采用指纹或虹膜识别，并辅以数字证书和动态令牌，有效防止身份伪造攻击[4]。模拟攻击演练平台根据医疗场景定制社工攻击剧本，如虚假患者咨询、紧急设备故障通知，对医护人员进行实战测试，通过攻击路径回溯与行为分析报告，量化评估并针对性培训，形成“测试－培训－复测”的闭环机制，显著增强医院整体防御能力。

三、 医院网络安全风险管理体系

（一）风险管理机制设计

1. 风险识别与评估

风险识别与评估需基于医疗业务流程的威胁建模方法，结合 HITECH 法案等合规要求，系统性分析潜在攻击面。通过梳理患者挂号、电子病历调阅、检验结果传输等核心环节的数据流，构建攻击树模型（Attack Tree），量化评估各节点面临的社会化攻击可能性与影响程度[5]。例如，在远程诊疗场景中，视频问诊平台的身份认证漏洞可能被伪装攻击利用，需依据威胁等级配置差异化的访问控制策略。同时，引入自动化风险评估工具（如 FAIR 框架），整合历史安全事件数据与行业基准值，动态生成风险热力图，为资源分配提供决策依据。

2. 应急预案与响应

针对数据泄露、勒索攻击等高频风险，应急预案需明确分级响应机制。一级事件（如核心业务系统瘫痪）触发全系统隔离与备用数据中心切换，同步启用加密通信渠道协调跨部门处置；二级事件（如局部数据泄露）启动溯源分析并冻结涉事账户权限，通过区块链存证技术固定攻击证据[6]。响应流程需嵌入法律合规要求，确保在48小时内完成患者通知与监管报备，同时利用离线备份与分布式存储技术实现关键数据快速恢复，最大限度降低业务中断时长。

（二）人员安全意识培训体系

1. 分层培训内容设计

分层培训内容设计需匹配医院组织架构特点。医护人员培训聚焦日常操作风险，通过真实社工攻击案例（如伪造医嘱系统升级通知）解析，强化钓鱼邮件辨识、敏感信息保护等实操技能；IT 管理员侧重技术防御能力提升，涵盖威胁情报分析、日志审计工具使用等进阶内容；管理层培训强调合规责任与资源统筹，结合《网络安全法》《个人信息保护法》解读，明确数据安全治理的权责边界。培训形式采用微课模块化设计，支持按角色定制学习路径，并嵌入电子病历系统登录前的强制答题环节，确保知识即时转化。

2. 培训效果评估

培训效果评估依托模拟攻击测试与量化考核体系。通过部署内部红队开展定向社工攻击演练（如伪造医疗设备厂商的漏洞修复邮件），统计不同岗位员工的误操作率与响应时效，生成个人安全能力画像。考核结果与绩效管理系统联动，对高风险群体实施强化培训，并基于反馈数据迭代优化课程内容。例如，针对医护人员在紧急状态下易忽略链接验证的问题，开发压力情境模拟训练模块，通过虚拟现实（VR）技术还原攻击场景，提升条件反射式防御能力，形成“监测－干预－验证”的闭环管理机制[7]。

四、 应用案例分析

（一）国内医院成功实践

1. 某三甲医院通过 AI 邮件过滤系统降低钓鱼攻击成功率90%

该医院采用基于自然语言处理（NLP）和图神经网络的 AI 邮件过滤系统，通过分析邮件语义、发件人行为及附件哈希值，构建动态风险评估模型。特别针对医疗场景中的钓鱼话术（如“紧急设备故障通知”“医保结算异常”）设立识别规则，并结合威胁情报库更新恶意域名黑名单[8]。部署后，钓鱼邮件识别准确率提升至98.5%，人工审核工作量减少70%，钓鱼攻击成功率从15%降至1.5%。系统与医院 OA 系统集成，自动隔离可疑邮件并触发告警，形成“识别－阻断－溯源”的闭环管理。通过每月更新训练数据集，持续优化模型以应对新型攻击，确保防御能力不断提升。

2. 区域性医疗联盟的威胁情报共享平台建设成效

某省级医疗联盟联合12家医院建立威胁情报共享平台，使用 STIX/TAXII 协议整合防火墙日志、终端告警和社会工程攻击数据。通过分析跨机构攻击模式，如同一 IP 对多医院发起的钓鱼攻击，平台自动产生防御规则并同步至各成员的安全设备[9]。例如，发现勒索软件利用默认密码渗透后，3小时内向联盟内所有 CT

和 MRI 设备推送密码重置策略。运行一年，成员应急响应时间缩短40%，跨院区勒索攻击减少62%。平台采用区块链技术确保情报的可信性和责任追溯，但也面临数据主权争议和技术兼容性挑战。

（二）国际经验与教训

1. 美国某医院因社工攻击导致患者数据泄露的根因分析

美国某大型医疗集团遭遇攻击，攻击者伪装成 IT 人员通过电话诱导医护人员提供 VPN 凭据，导致45万份患者病历泄露。技术上缺乏多因素认证，默认允许内部号码跳过身份验证；管理上未建立针对社工攻击的应急预案，响应延迟超过72小时，违反 HIPAA 法案30小时通告要求。事后，医院投资300万美元升级身份管理系统，引入基于行为生物特征（如打字节奏）的持续认证，并要求高风险操作需二次授权。此案例揭示医疗机构普遍存在的“重技术合规、轻人员行为管控”问题，强调防御社工攻击需要技术和管理协同优化。

2. 欧盟 GDPR 框架下医院安全防护的合规性实践

德国某大学附属医院依据 GDPR 第32条“数据保护设计原则”，重构医疗信息系统安全架构[10]。技术层面，对电子健康记录（EHR）实施动态数据脱敏，医生仅可访问当前诊疗所需字段；管理层面，设立数据保护官（DPO）岗位，每季度审核第三方供应商安全资质。为应对 GDPR 严苛的罚款条款（最高全球营收4%），医院部署自动化合规监测工具，实时检测数据跨境传输路径，拦截未加密的国际会诊请求。实施后，患者数据泄露事件同比下降55%，但因过度加密导致急救场景数据调取延迟增加，反映隐私保护与医疗效率的平衡难题。该实践为医疗行业提供“合规驱动安全”的参考范式。

（三）优化建议

1. 技术层面

需建立基于设备指纹的物联网准入认证体系，通过硬件 ID、固件哈希值与行为基线三重验证确保设备合法性。对联网医疗设备（如胰岛素泵、心脏监护仪）实施强制证书认证，禁止未签名固件更新。部署网络微隔离技术，限制设备仅能与授权服务器通信，阻断利用血糖仪作为跳板攻击核心数据库的横向渗透路径。同时，引入轻量级终端检测与响应（EDR）代理，实时监控设备异常数据外传行为，结合医疗设备专用漏洞库（如 ICS-CERT）进行威胁狩猎。探索零信任架构在 IoMT 场景的应用，按需动态调整设备访问权限。

2. 管理层面

医院需组建由临床科室、信息中心、法务部及管理层代表组成的网络安全治理委员会，制定统一的安全策略与责任矩阵。委员会每月召开风险研判会议，基于业务影响分析（BIA）调整资源分配优先级，例如将急诊科系统的容灾等级设为最高。建立“安全左移”机制，在医疗信息化项目立项阶段嵌入安全评审流程，要求供应商提供符合 IEC 62443标准的证明。定期开展红蓝对抗演练，模拟勒索攻击导致 CT 系统停机的极端场景，测试多部门协同处置能力。该模式可解决传统医疗 IT 管理条块分割问题，但需高层持续支持以避免形式化执行。

五、 总结与展望

社会化攻击防范需在医院网络安全建设中实现“技术 – 管理 – 人员”多维协同，通过动态防御、智能检测工具和分层培训构建防护体系。AI 驱动的异常行为检测、威胁情报共享等技术可降低钓鱼攻击和数据泄露风险，但医疗数据共享与隐私保护的矛盾及新型攻击迭代仍制约效能。未来研究应探索轻量化加密算法和零信任架构在医疗物联网的应用，解决设备资源与安全需求的冲突；区块链可增强数据溯源和跨机构协作的可信度，但需克服性能和合规难题。针对医护人员的行为特征发展主动防御模型，以及基于联邦学习的威胁情报分析框架，是可能的创新路径。医疗网络安全治理需平衡业务效率与安全韧性，以应对不断变化的社会化攻击威胁。

参考文献

[1] 王磊 . 浅谈基于等保的医院网络安全建设及改进 [J]. 甘肃科技 ,2019,35(9):14-15.

[2] 郭丛庆 . 医院信息化建设中的网络安全防护措施研究 [J]. 中国卫生产业 ,2019,16(19):160-161.

[3] 仝晖 . 以区块链为基础的医院网络信息安全管理研究 [J].IT 经理世界 ,2023,(08):36-39+65.

[4] 刘阳 . 基于实战化安全运营的智慧医院网络安全保护体系构建与应用 [J]. 中国医疗设备 ,2023,38(11):127-132.

[5] 周博 . 北京医院网络管理系统的设计与实现 [D]. 四川：电子科技大学 ,2013.

[6] 刘海一 . 医疗设备维护管理与医院网络安全探讨 [J]. 中国数字医学 ,2023,18(09):9-12.

[7] 程莹 . 基于攻击路径威胁分析的网络安全度量技术的研究 [J]. 电子技术与软件工程 ,2021,(15):253-254.

[8] 臧道逸 . 主动防御技术在医院信息网络安全中的研究与应用 [J]. 网络空间安全 ,2024,15(04):353-356.

[9] 吴灵菲 . 医院网络安全纵深协同防御体系建设实践 [J]. 福建电脑 ,2023,39(12):44-47.

[10] 廉成绪，陈立军，李宪坤，等 . 基于攻击路径威胁分析的网络安全度量技术 [J]. 网络安全技术与应用 ,2022,(10):17-19.