A SYSTEMATIC REVIEW OF CYBERSECURITY ATTACKS ON MEDICAL DEVICES

Tadeu Marcos Borges Paes[1]

Francisco Nicolás Isnardi Begot[2]

Carlos Kiyoshi Yanaguibashi Menezes[3]

Eudes Danilo da Silva Mendonça[4]

Resumo: A crescente integração de dispositivos médicos com redes de comunicação e sistemas digitais tem ampliado significativamente a superfície de ataque das infraestruturas de saúde modernas. Esse cenário, impulsionado pelo avanço da Internet das Coisas Médicas (IoMT, do inglês Internet of Medical Things), introduz novos desafios de cibersegurança que podem comprometer a confidencialidade de dados sensíveis, a integridade dos sistemas e, principalmente, a segurança dos pacientes. Diante desse contexto, este trabalho apresenta uma revisão sistemática da literatura sobre ataques cibernéticos direcionados a dispositivos médicos, orientada por quatro questões de pesquisa: (RQ1) Quais tipos de ataques cibernéticos têm sido reportados contra dispositivos médicos conectados? (RQ2) Quais vulnerabilidades são mais frequentemente exploradas nesses dispositivos? (RQ3) Quais categorias de dispositivos médicos apresentam maior exposição a riscos de segurança cibernética? (RQ4) Quais estratégias de mitigação e contramedidas são propostas na literatura? A revisão foi conduzida seguindo o protocolo PRISMA, com buscas realizadas em seis bases de dados acadêmicas (IEEE Xplore, ACM Digital Library, PubMed, Scopus, ScienceDirect e Web of Science),

1 Doutorando em Inteligência Artificial, Senai Centro Desenvolvimento da Amazônia, Orcid: https://orcid.org/0009-0002-2978-2117

2 Discente de Engenharia Computação, Universidade Federal do Pará, Orcid: https://orcid.org/0009-0009-0944-6336

3 Discente de Engenharia Biomédica, Universidade Federal do Pará, Orcid: https://orcid.org/0009-0005-7942-2680

4 Mestre em computação aplicada, Senai Centro Desenvolvimento da Amazônia, Orcid: https://orcid.org/0009-0006-6439-408X

abrangendo publicações de 2008 a 2024. A partir de um conjunto inicial de 1.247 registros, 58 estudos foram selecionados após a aplicação de critérios de inclusão e exclusão previamente definidos, por meio de um processo de triagem em três etapas envolvendo leitura de títulos, análise de resumos e avaliação de textos completos. Os resultados indicam que as vulnerabilidades mais prevalentes estão associadas a mecanismos de autenticação fracos, protocolos de comunicação inseguros, firmware desatualizado e ausência de criptografia. Bombas de infusão emergem como a categoria de dispositivo com maior exposição, com 75% das unidades apresentando vulnerabilidades conhecidas, seguidas por sistemas de chamada de enfermagem (48%) e marca-passos e desfibriladores implantáveis (40%). Ataques remotos via comunicação sem fio, exploração de redes hospitalares e manipulação de software embarcado figuram como os vetores de ataque mais frequentemente reportados. Com base nesses achados, propõe-se uma taxonomia de ataques IoMT em três camadas, organizada nos níveis de percepção/sensor, rede/comunicação e aplicação/sistema, contribuindo com um framework de classificação estruturado para a área. Adicionalmente, a revisão identifica seis lacunas de pesquisa relevantes, incluindo a escassez de estudos conduzidos em ambientes clínicos reais, a insuficiente validação de soluções de segurança leves para dispositivos com recursos computacionais limitados e a ausência de frameworks padronizados de teste de penetração para IoMT. Os achados evidenciam a necessidade urgente de adoção de práticas de segurança desde o projeto (security by design) no desenvolvimento de dispositivos médicos, do fortalecimento de políticas regulatórias e da promoção de colaboração internacional para a proteção das infraestruturas de saúde digitais.

Palavras-chave: Cibersegurança; Dispositivos Médicos; Engenharia Biomédica; Internet das Coisas Médicas (IoMT); Segurança de Sistemas de Saúde; Revisão Sistemática.

Abstract: The increasing integration of medical devices with communication networks and digital systems has significantly expanded the attack surface of modern healthcare infrastructures. This scenario, driven by the advancement of the Internet of Medical Things (IoMT), introduces new

cybersecurity challenges that can compromise the confidentiality of sensitive data, the integrity of systems, and, most critically, patient safety. In this context, this paper presents a systematic literature review on cyberattacks targeting medical devices, guided by four research questions: (RQ1) What types of cyberattacks have been reported against connected medical devices? (RQ2) What vulnerabilities are most frequently exploited in these devices? (RQ3) Which categories of medical devices exhibit the greatest exposure to cybersecurity risks? (RQ4) What mitigation strategies and countermeasures are proposed in the literature? The review was conducted following the PRISMA protocol, with searches performed across six academic databases (IEEE Xplore, ACM Digital Library, PubMed, Scopus, ScienceDirect, and Web of Science) covering publications from 2008 to 2024. From an initial set of 1,247 records, 58 studies were selected after applying predefined inclusion and exclusion criteria through a three-stage screening process involving title review, abstract analysis, and full-text assessment. The results indicate that the most prevalent vulnerabilities are associated with weak authentication mechanisms, insecure communication protocols, outdated firmware, and the absence of encryption. Infusion pumps emerged as the most exposed device category, with 75% of units presenting known vulnerabilities, followed by nurse call systems (48%) and implantable pacemakers and defibrillators (40%). Remote attacks via wireless communication, hospital network exploitation, and embedded software manipulation appear as the most frequently reported attack vectors. Based on these findings, a three-layer IoMT attack taxonomy is proposed, organized across the perception/sensor, network/communication, and application/system layers, contributing a structured classification framework to the field. Furthermore, the review identifies six key research gaps, including the scarcity of studies conducted in real clinical environments, the insufficient validation of lightweight security solutions for resource-constrained devices, and the absence of standardized penetration testing frameworks for IoMT. The findings underscore the urgent need for adopting security-by-design practices in medical device development, strengthening regulatory policies, and fostering international collaboration to protect digital healthcare infrastructures.

Keywords: Cybersecurity; Medical Devices; Biomedical Engineering; Internet of Medical Things (IoMT); Healthcare Systems Security; Systematic Review.

Introdução

A transformação digital no setor de saúde tem promovido avanços significativos na qualidade do atendimento ao paciente, na precisão dos diagnósticos e na eficiência dos processos clínicos. Dispositivos médicos modernos, como bombas de infusão, marca-passos, monitores cardíacos e sensores de glicose, passaram a integrar redes de comunicação sem fio e sistemas hospitalares conectados, formando o que se convencionou chamar de Internet das Coisas Médicas (IoMT, do inglês Internet of Medical Things). Essa interconexão, embora benéfica sob a perspectiva clínica, introduz uma série de vulnerabilidades que podem ser exploradas por agentes maliciosos, comprometendo a confidencialidade, a integridade e a disponibilidade dos dados e sistemas de saúde (Coventry & Branley, 2018).

Historicamente, o desenvolvimento de dispositivos médicos priorizou desempenho e segurança clínica, relegando aspectos de cibersegurança a um plano secundário. Williams e Woodward (2015) demonstraram que a complexidade do ambiente hospitalar, aliada à presença de sistemas legados e protocolos de comunicação inseguros, cria um cenário propício para ataques cibernéticos. Trabalhos pioneiros, como o de Halperin et al. (2008), evidenciaram que dispositivos implantáveis como desfibriladores cardíacos podem ser comprometidos remotamente por meio de rádios definidos por software, permitindo a interceptação de dados do paciente e a manipulação de terapias. De forma semelhante, Li, Raghunathan e Jha (2011) demonstraram ataques bem-sucedidos contra sistemas de monitoramento de glicose e entrega de insulina, reforçando a criticidade dessas vulnerabilidades.

O cenário regulatório também tem evoluído em resposta a essas ameaças. A Food and Drug Administration (FDA) dos Estados Unidos publicou, em 2023, diretrizes finais sobre cibersegurança em dispositivos médicos, exigindo que fabricantes incorporem avaliações de risco de segurança

cibernética durante as fases de pré e pós-mercado (FDA, 2023). Na União Europeia, o Cyber Resilience Act (CRA) busca estabelecer requisitos obrigatórios de segurança para dispositivos conectados. Apesar desses avanços, a literatura aponta que a implementação efetiva dessas medidas ainda enfrenta desafios significativos.

Diante desse contexto, este trabalho apresenta uma revisão sistemática da literatura sobre ataques cibernéticos direcionados a dispositivos médicos. O objetivo principal é identificar, categorizar e analisar os principais vetores de ataque, as vulnerabilidades recorrentes, os tipos de dispositivos mais afetados e os impactos potenciais desses incidentes em ambientes de saúde conectados.

Questões de Pesquisa (Research Questions)

Para orientar a condução desta revisão sistemática e delimitar o escopo da análise, foram formuladas as seguintes questões de pesquisa:

RQ1 – Quais tipos de ataques cibernéticos têm sido reportados contra dispositivos médicos conectados?

RQ2 – Quais vulnerabilidades são mais frequentemente exploradas nesses dispositivos?

RQ3 – Quais categorias de dispositivos médicos apresentam maior exposição a riscos de segurança cibernética?

RQ4 – Quais estratégias de mitigação e contramedidas são propostas na literatura para a proteção de dispositivos médicos?

Essas questões estruturam a extração e a análise dos dados ao longo da revisão, permitindo uma contribuição analítica clara e alinhada com as práticas metodológicas de revisões sistemáticas internacionais.

Metodologia

A presente revisão sistemática foi conduzida seguindo as diretrizes do protocolo PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses), com o objetivo de garantir a reprodutibilidade e a transparência do processo de seleção e análise dos estudos.

Estratégia de busca

A busca por estudos relevantes foi realizada em seis bases de dados acadêmicas: IEEE Xplore, ACM Digital Library, PubMed (MEDLINE), Scopus, ScienceDirect e Web of Science. As buscas foram conduzidas entre janeiro e março de 2025, abrangendo publicações de 2008 a 2024, período que compreende desde os primeiros trabalhos sobre vulnerabilidades em dispositivos médicos implantáveis até as publicações mais recentes sobre segurança em ambientes IoMT.

As combinações de termos-chave utilizadas com operadores booleanos foram: ("cybersecurity" OR "cyber attack" OR "security vulnerability") AND ("medical device" OR "Internet of Medical Things" OR "IoMT" OR "implantable device" OR "infusion pump" OR "pacemaker"). Buscas complementares foram realizadas por meio de referências cruzadas dos artigos selecionados (snowballing) e em repositórios de documentos técnicos da FDA e do CISA (Cybersecurity and Infrastructure Security Agency).

Critérios de inclusão e exclusão

Foram incluídos estudos que: (a) abordassem diretamente ataques cibernéticos, vulnerabilidades ou ameaças de segurança relacionados a dispositivos médicos; (b) apresentassem demonstrações experimentais, análises teóricas, estudos de caso ou revisões sistemáticas sobre o tema; (c) estivessem disponíveis em inglês ou português; e (d) fossem publicados em fontes

revisadas por pares. Foram excluídos trabalhos que: tratassem exclusivamente de segurança de redes hospitalares sem foco específico em dispositivos médicos; abordassem apenas aspectos regulatórios sem componente técnico; ou consistissem em resumos de conferências, editoriais e cartas ao editor sem dados originários.

Processo de seleção e filtragem

A busca inicial nas seis bases de dados retornou um total de 1.247 registros. Após a remoção de 312 duplicatas, restaram 935 registros para triagem. Na primeira etapa, a leitura de títulos e resumos resultou na exclusão de 743 registros que não atendiam aos critérios de inclusão. Na segunda etapa, 192 artigos foram submetidos à leitura integral, dos quais 134 foram excluídos por não apresentarem foco suficiente em ataques a dispositivos médicos específicos (n = 68), abordarem exclusivamente aspectos regulatórios sem componente técnico (n = 42) ou constituírem resumos expandidos sem dados originais (n = 24). Ao final do processo, 58 estudos foram incluídos na revisão sistemática.

Para cada estudo selecionado, foram extraídas informações relativas a: tipo de dispositivo médico analisado, vetor de ataque utilizado, vulnerabilidade explorada, metodologia de ataque, impacto potencial sobre o paciente e/ou sistema de saúde, e contramedidas propostas. Essa abordagem é consistente com revisões sistemáticas anteriores na área (Newaz et al., 2021; Kruse et al., 2017).

Resultados

A análise dos 58 estudos selecionados permitiu identificar padrões recorrentes em relação aos tipos de vulnerabilidades, vetores de ataque, dispositivos mais visados e impactos reportados na literatura. Os resultados são organizados em resposta às questões de pesquisa formuladas.

Tipos de ataques reportados (RQ1)

Os vetores de ataque mais relatados podem ser agrupados em três categorias principais: ataques remotos via comunicação sem fio, exploração de redes hospitalares e manipulação de software embarcado. Halperin et al. (2008) demonstraram que é possível interceptar e manipular comunicações entre um desfibrilador cardíaco implantável e seu programador externo utilizando rádios definidos por software. Li, Raghunathan e Jha (2011) evidenciaram ataques passivos e ativos contra sistemas de bomba de insulina. Marin et al. (2016) estenderam essa análise ao demonstrar vulnerabilidades na geração mais recente de desfibriladores implantáveis.

A exploração de redes hospitalares constitui outro vetor crítico. O ataque WannaCry de 2017 afetou mais de 80 organizações do National Health Service (NHS) do Reino Unido, comprometendo dispositivos IoT e interrompendo o atendimento a pacientes (Kruse et al., 2017). Vulnerabilidades como as identificadas no protocolo Bluetooth Low Energy (BLE) através das falhas SweynTooth (2020) demonstraram que dispositivos vestíveis e de monitoramento podem ser forçados a reiniciar ou tornarem-se inoperantes por meio de pacotes BLE malformados (Thomasian & Adashi, 2021).

Vulnerabilidades mais exploradas (RQ2)

As vulnerabilidades mais frequentemente associadas a dispositivos médicos incluem: mecanismos de autenticação fracos ou inexistentes, protocolos de comunicação sem fio inseguros, firmware desatualizado e ausência de criptografia nas transmissões de dados. Camara, Peris-Lopez e Tapiador (2015) identificaram que muitos dispositivos implantáveis utilizam protocolos proprietários que carecem de mecanismos básicos de segurança. A análise de Sánchez-Guerrero et al. (2023) identificou 661 vulnerabilidades distintas em dispositivos adquiridos por sistemas nacionais de saúde em 36 países, das quais mais da metade foram classificadas como críticas ou de alta severidade segundo o sistema CVSS.

A pesquisa da Palo Alto Unit 42 (2022), que escaneou mais de 200.000 bombas de infusão, constatou que 75% apresentavam vulnerabilidades de segurança conhecidas, sendo o vazamento de informações sensíveis e o uso de credenciais padrão os problemas mais recorrentes. O FBI reportou, em 2022, uma média de 6,2 vulnerabilidades por dispositivo médico, com mais de 40% dos dispositivos em estágio de fim de vida sem patches de segurança disponíveis (FBI, 2022).

Dispositivos com maior exposição (RQ3)

A Tabela 1 apresenta a síntese dos dispositivos médicos mais frequentemente citados na literatura como alvos de ataques cibernéticos, com base na proporção de dispositivos com vulnerabilidades conhecidas e os respectivos vetores de ataque.

Tabela 1 – Dispositivos médicos, percentual de vulnerabilidades e vetores de ataque

Dispositivo Médico	% Vulner.	Principais Vetores de Ataque	Referências
Bombas de infusão e insulina	75%	Credenciais padrão, comunicação em texto claro, manipulação remota de dosagem, firmware desatualizado	Palo Alto Unit 42 (2022); Li et al. (2011); FDA (2019)
Sistemas de chamada de enfermagem	48%	CVEs críticas não corrigidas, protocolos legados, ausência de segmentação de rede	Armis (2023); Forescout (2024)
Marca-passos e desfibriladores implantáveis	40%	Interceptação de comunicação sem fio (SDR), reprogramação remota, ataques DoS de bateria	Halperin et al. (2008); Marin et al. (2016); FDA (2017)
Sistemas de dispensação de medicamentos	32%	Contas padrão, exploração de vulnerabilidades Windows, ransomware via rede hospitalar	Armis (2023); Forescout (2024)
Estações DICOM / PACS	28%	Protocolo DICOM sem autenticação, exposição à internet, exfiltração de imagens médicas	Forescout (2024); Sánchez-Guerrero et al. (2023)
Monitores de sinais vitais	25%	Vulnerabilidades BLE (SweynTooth), spoofing de leituras, ataques KRACK via Wi-Fi	Thomasian & Adashi (2021); Forescout (2024)

Fonte: Elaboração própria com base nos estudos analisados.

Estratégias de mitigação propostas (RQ4)

As contramedidas identificadas na literatura podem ser classificadas em quatro categorias: medidas tecnológicas, regulatórias, organizacionais e de monitoramento. No âmbito tecnológico, os estudos propõem a adoção de criptografia leve (lightweight cryptography) adequada às restrições computacionais dos dispositivos médicos, autenticação mútua baseada em sinais fisiológicos do paciente, atualização segura de firmware via canais autenticados e segmentação de redes hospitalares em VLANs dedicadas para dispositivos IoMT (Camara et al., 2015; Rushanan et al., 2014).

No âmbito do monitoramento, a aplicação de sistemas de detecção de intrusão (IDS) baseados em inteligência artificial tem demonstrado resultados promissores. Newaz et al. (2021) apontam que algoritmos de deep learning e redes neurais recorrentes podem identificar tráfego malicioso em redes de dispositivos médicos com alta acurácia. A adoção de arquiteturas de confiança zero (zero trust) também é discutida como estratégia de proteção para ambientes IoMT.

No âmbito regulatório, as diretrizes do FDA (2023) e o PATCH Act (2022) nos Estados Unidos, bem como o Cyber Resilience Act na União Europeia, representam avanços ao exigir que fabricantes incorporem Software Bill of Materials (SBOM) e planos de cibersegurança em suas submissões de pré-mercado.

Tabela de análise dos estudos selecionados

A Tabela 2 apresenta uma síntese dos principais estudos incluídos nesta revisão, classificados por dispositivo estudado, tipo de ataque, metodologia empregada e impacto reportado.

Tabela 2 – Síntese dos principais estudos analisados

Estudo	Dispositivo	Tipo de Ataque	Metodologia	Impacto
Halperin et al. (2008)	Desfibrilador cardíaco implantável (ICD)	Interceptação e reprogramação via rádio definido por software	Engenharia reversa de protocolo de comunicação + ataques com GNU Radio	Acesso a dados do paciente, alteração de terapia, possibilidade de choque fatal
Li et al. (2011)	Bomba de insulina e monitor de glicose	Ataques passivos (espionagem) e ativos (manipulação de dosagem)	Demonstração laboratorial com hardware comercial off-the-shelf	Administração de doses incorretas de insulina, risco de hipo/hiperglicemia fatal
Marin et al. (2016)	Desfibrilador implantável (nova geração)	Ataques de replay, spoofing e man-in-the-middle	Análise criptográfica e testes de penetração em protocolo proprietário	Reprogramação não autorizada, depleção de bateria, interrupção de terapia
Palo Alto Unit 42 (2022)	Bombas de infusão (200.000 unid.)	Exploração de CVEs conhecidas, credenciais padrão, comunicação não cifrada	Varredura crowdsourced contra 40+ CVEs e 70+ vulnerabilidades IoT	75% das bombas com vulnerabilidades; risco de interrupção de medicação
Sánchez-Guerrero et al. (2023)	Diversos (36 países)	Análise de vulnerabilidades em dispositivos adquiridos por SUS nacionais	Cruzamento de dados OCDS + CVEs + ICSMA (92 milhões de registros)	661 vulnerabilidades; mais de 50% críticas ou de alta severidade (CVSS)
Forescout (2024)	Estações DICOM, PACS, bombas, monitores	Exploração de contas padrão, KRACK (Wi-Fi), vulnerabilidades de SO	Análise de 162 CVEs em dispositivos IoMT + honeypot (1,6M ataques/ano)	Exfiltração de dados de pacientes, comprometimento de estações de imagem
Armis (2023)	Sist. chamada de enfermagem, bombas, dispensadores	CVEs críticas não corrigidas em dispositivos IoMT e IoT hospitalares	Análise de plataforma de inteligência de ativos (3+ bilhões de dispositivos)	Ranking de risco: sist. enfermagem > bombas > dispensadores

Fonte: Elaboração própria com base nos estudos analisados.

Taxonomia proposta de ataques em dispositivos IoMT

A partir da análise sistemática dos estudos selecionados, propõe-se uma taxonomia estruturada de ataques cibernéticos em dispositivos médicos, organizada em três camadas do ecossistema IoMT, conforme descrito a seguir.

Camada 1 – Ataques à camada de percepção/sensor: Englobam ataques direcionados aos sensores e atuadores dos dispositivos, incluindo interferência eletromagnética em eletrodos de marca-passos, falsificação de leituras de sensores de glicose (spoofing), manipulação de atuadores de bombas de insulina e ataques de jamming em canais de comunicação de curto alcance.

Camada 2 – Ataques à camada de rede/comunicação: Compreendem a interceptação de comunicações sem fio (eavesdropping via SDR), ataques man-in-the-middle em protocolos proprietários, exploração de vulnerabilidades em protocolos BLE (SweynTooth) e Wi-Fi (KRACK), ataques de negação de serviço (DoS) por esgotamento de bateria e replay attacks em sessões de programação de dispositivos.

Camada 3 – Ataques à camada de aplicação/sistema: Incluem a exploração de credenciais padrão em interfaces de gerenciamento, injeção de malware em firmware de dispositivos, ransomware propagado via redes hospitalares (ex.: WannaCry), exploração de vulnerabilidades em sistemas operacionais legados (ex.: EternalBlue em Windows XP) e acesso não autorizado a sistemas DICOM/PACS para exfiltração de imagens médicas.

Essa taxonomia em camadas permite que pesquisadores e profissionais de segurança identifiquem os pontos de entrada mais críticos e direcionem as contramedidas de forma estratificada ao longo da arquitetura IoMT.

Discussão

Análise dos achados

Os resultados desta revisão sistemática evidenciam que a cibersegurança de dispositivos médicos constitui um desafio multifacetado, que transcende a dimensão puramente tecnológica e envolve aspectos regulatórios, organizacionais e humanos. Essa perspectiva é corroborada por Williams e Woodward (2015), que caracterizaram o problema como resultado da convergência entre

vulnerabilidades de tecnologia, riscos de software e fatores humanos.

Um aspecto central identificado nesta revisão diz respeito à tensão entre inovação e segurança. A pressão para acelerar a entrada de dispositivos no mercado frequentemente resulta em testes de cibersegurança insuficientes ou realizados apenas na fase de pós-mercado. Coventry e Branley (2018) argumentam que a cibersegurança deve ser tratada como uma questão de segurança do paciente e integrada desde as fases iniciais do projeto dos dispositivos, seguindo a abordagem de "security by design".

Implicações regulatórias

No âmbito regulatório, observa-se uma evolução positiva, porém ainda insuficiente. A publicação da seção 524B do FD&C Act nos Estados Unidos e as diretrizes do FDA de 2023 representam marcos importantes ao exigir que fabricantes incorporem planos de cibersegurança e Software Bill of Materials (SBOM) em suas submissões de pré-mercado (FDA, 2023). Na União Europeia, o Cyber Resilience Act promete impactar significativamente o ecossistema de segurança da IoT. No entanto, a fragmentação regulatória entre diferentes jurisdições permanece um obstáculo à adoção uniforme de padrões de segurança. Em países em desenvolvimento, como o Brasil, a ausência de regulamentações específicas sobre cibersegurança de dispositivos médicos pela ANVISA cria uma lacuna normativa que expõe pacientes e instituições de saúde a riscos adicionais.

Impacto na engenharia biomédica

Os achados desta revisão têm implicações diretas para a engenharia biomédica. O paradigma tradicional de desenvolvimento de dispositivos médicos, centrado exclusivamente em desempenho clínico e segurança funcional, mostra-se inadequado frente ao cenário atual de ameaças. A integração de requisitos de cibersegurança no ciclo de vida do dispositivo — desde a concepção do hardware

e firmware até a descomissionamento — exige uma reconfiguração dos processos de engenharia. Engenheiros biomédicos precisam incorporar modelagem de ameaças (threat modeling), análise de superfície de ataque e testes de penetração como etapas padronizadas do desenvolvimento, em complemento aos testes clínicos e de biocompatibilidade já estabelecidos.

Desafios de segurança em dispositivos com recursos limitados

Um desafio técnico particularmente relevante reside nas restrições computacionais inerentes a dispositivos médicos implantáveis e vestíveis. Esses dispositivos operam com capacidade de processamento, memória e energia severamente limitadas, o que inviabiliza a aplicação direta de protocolos criptográficos tradicionais (como TLS/SSL) ou sistemas de detecção de intrusão convencionais. A literatura aponta para o desenvolvimento de criptografia leve (lightweight cryptography), protocolos de autenticação baseados em sinais fisiológicos (como variabilidade cardíaca ou padrões de glicemia) e soluções de segurança assistidas por dispositivos vestíveis intermediários (gateway devices) como alternativas viáveis para mitigar essa limitação (Camara et al., 2015; Rushanan et al., 2014).

A presença predominante de sistemas legados em ambientes hospitalares agrava significativamente o panorama de segurança. Dispositivos médicos possuem ciclos de vida longos, frequentemente superiores a dez anos, o que significa que muitos equipamentos em operação executam sistemas operacionais obsoletos e não recebem mais atualizações de segurança. O relatório do FBI (2022) constatou que mais de 40% dos dispositivos em estágio de fim de vida não dispõem de patches de segurança.

Lacunas de pesquisa (Research Gaps)

A análise dos estudos selecionados permitiu identificar as seguintes lacunas na literatura que

representam oportunidades para investigação futura:

Escassez de estudos em ambientes clínicos reais: A maioria dos ataques demonstrados na literatura foi realizada em ambientes laboratoriais controlados. Há uma carência significativa de estudos que avaliem a viabilidade e o impacto de ataques cibernéticos em condições clínicas reais, com dispositivos em uso ativo em pacientes.

Insuficiência de soluções de segurança validadas para dispositivos com recursos limitados: Embora diversas propostas de criptografia leve e autenticação fisiológica tenham sido apresentadas, poucas foram validadas em dispositivos médicos comerciais com restrições reais de processamento, memória e energia.

Ausência de frameworks padronizados de teste de penetração para IoMT: Diferentemente do setor de TI tradicional, não existem metodologias amplamente aceitas e padronizadas para a condução de testes de penetração específicos para dispositivos médicos conectados.

Limitada investigação sobre ataques multi-vetor: Poucos estudos abordam cenários de ataques que combinam múltiplos vetores simultaneamente (por exemplo, exploração de rede combinada com manipulação de firmware), os quais representam cenários mais realistas de ameaça.

Sub-representação de dispositivos emergentes: Tecnologias emergentes como monitores de saúde baseados em IA, dispositivos de neuroestimulação conectados e sensores ingeríveis ainda são pouco investigados do ponto de vista de cibersegurança.

Lacuna regulatória em países em desenvolvimento: A grande maioria dos estudos concentra-se no contexto regulatório dos Estados Unidos e da União Europeia, com escassa investigação sobre o panorama de cibersegurança de dispositivos médicos em países da América Latina, África e Sudeste Asiático.

Limitações desta revisão

Cabe ressaltar as limitações desta revisão. A busca foi restrita a publicações em inglês e português, o que pode ter excluído trabalhos relevantes em outros idiomas. A rápida evolução do campo implica que novas vulnerabilidades e ataques podem ter surgido após o período coberto pela revisão. A heterogeneidade dos estudos analisados, que variam de demonstrações experimentais a revisões teóricas, dificulta comparações diretas entre os achados. Adicionalmente, os dados quantitativos de vulnerabilidades baseiam-se em varreduras de fabricantes e contextos específicos, podendo não ser generalizáveis a todos os ambientes hospitalares.

Conclusão

Esta revisão sistemática proporcionou uma visão abrangente do estado atual da literatura sobre ataques cibernéticos a dispositivos médicos, respondendo às quatro questões de pesquisa formuladas. Os achados indicam que vulnerabilidades como autenticação fraca, protocolos de comunicação inseguros e firmware desatualizado permanecem prevalentes em dispositivos amplamente utilizados em ambientes clínicos (RQ1 e RQ2). Bombas de infusão, marca-passos e sistemas de chamada de enfermagem emergem como as categorias de dispositivos com maior exposição a riscos (RQ3). As estratégias de mitigação identificadas abrangem soluções tecnológicas, regulatórias e organizacionais, com destaque para criptografia leve, arquiteturas zero trust e frameworks regulatórios como o PATCH Act e o Cyber Resilience Act (RQ4).

A taxonomia de ataques proposta, organizada em três camadas do ecossistema IoMT (percepção, rede e aplicação), constitui uma contribuição conceitual deste trabalho e pode servir como referência para pesquisadores e profissionais de segurança na identificação e mitigação estratificada de ameaças.

Os resultados reforçam a necessidade urgente de adoção da abordagem de segurança desde o

projeto (security by design) no desenvolvimento de dispositivos médicos, bem como a harmonização internacional de padrões de cibersegurança. A colaboração entre fabricantes, instituições de saúde, órgãos reguladores e a comunidade acadêmica é essencial para o desenvolvimento de frameworks de segurança que acompanhem a rápida evolução tecnológica do setor.

Como direções para pesquisas futuras, destacam-se: o desenvolvimento de sistemas de detecção de intrusão otimizados para dispositivos com recursos computacionais limitados; a investigação de protocolos de comunicação leves e seguros específicos para IoMT; a avaliação da efetividade de arquiteturas de confiança zero em ambientes hospitalares; a condução de estudos em ambientes clínicos reais; e a criação de frameworks regulatórios para países em desenvolvimento. A proteção das infraestruturas de saúde digitais é, em última instância, uma questão de segurança do paciente.

Referências

Armis. (2023). Armis Identifies the Riskiest Medical and IoT Devices in Clinical Environments. Armis Newsroom.

Camara, C., Peris-Lopez, P., & Tapiador, J. E. (2015). Security and Privacy Issues in Implantable Medical Devices: A Comprehensive Survey. Journal of Biomedical Informatics, 55, 272–289. https://doi.org/10.1016/j.jbi.2015.04.007

Coventry, L., & Branley, D. (2018). Cybersecurity in Healthcare: A Narrative Review of Trends, Threats and Ways Forward. Maturitas, 113, 48–52. https://doi.org/10.1016/j.maturitas.2018.04.008

Federal Bureau of Investigation – FBI. (2022). Unpatched and Outdated Medical Devices Provide Cyber Attack Opportunities. Private Industry Notification, PIN-20220912-001.

Forescout Vedere Labs. (2024). Unveiling the Persistent Risks of Connected Medical Devices. Forescout Technologies.

Halperin, D., Heydt-Benjamin, T. S., Ransford, B., Clark, S. S., Defend, B., Morgan, W., Fu, K., Kohno, T., & Maisel, W. H. (2008). Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defenses. In 2008 IEEE Symposium on Security and Privacy (pp. 129–142). IEEE. https://doi.org/10.1109/SP.2008.31

Kruse, C. S., Frederick, B., Jacobson, T., & Monticone, D. K. (2017). Cybersecurity in Healthcare: A Systematic Review of Modern Threats and Trends. Technology and Health Care, 25(1), 1–10. https://doi.org/10.3233/THC-161263

Li, C., Raghunathan, A., & Jha, N. K. (2011). Hijacking an Insulin Pump: Security Attacks and Defenses for a Diabetes Therapy System. In 2011 IEEE 13th International Conference on e-Health Networking, Applications and Services (pp. 150–156). IEEE. https://doi.org/10.1109/HEALTH.2011.6026732

Marin, E., Singelée, D., Garcia, F. D., Chothia, T., Willems, R., & Preneel, B. (2016). On the (In) security of the Latest Generation Implantable Cardiac Defibrillators and How to Secure Them. In ACSAC '16 (pp. 226–236). ACM. https://doi.org/10.1145/2991079.2991094

Newaz, A. I., Sikder, A. K., Rahman, M. A., & Uluagac, A. S. (2021). A Survey on Security and Privacy Issues in Modern Healthcare Systems: Attacks and Defenses. ACM Computing Surveys, 54(7s), 1–44. https://doi.org/10.1145/3453176

Palo Alto Networks – Unit 42. (2022). Know Your Infusion Pump Vulnerabilities and Secure Your Healthcare Organization. Unit 42 Research Report.

Rushanan, M., Rubin, A. D., Kune, D. F., & Swanson, C. M. (2014). SoK: Security and Privacy in Implantable Medical Devices and Body Area Networks. In 2014 IEEE Symposium on Security and Privacy (pp. 524–539). https://doi.org/10.1109/SP.2014.40

Sánchez-Guerrero, R., Mendoza, F. A., Díaz-Verdejo, J., Casilari, E., & Crespo, A. (2023). Cybersecurity Vulnerability Analysis of Medical Devices Purchased by National Health Services. Scientific Reports, 13, 19548. https://doi.org/10.1038/s41598-023-45927-1

Thomasian, N. M., & Adashi, E. Y. (2021). Cybersecurity in the Internet of Medical Things. Health Policy and Technology, 10(3), 100549. https://doi.org/10.1016/j.hlpt.2021.100549

U.S. Food and Drug Administration – FDA. (2023). Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions – Final Guidance. FDA.

Williams, P. A. H., & Woodward, A. J. (2015). Cybersecurity Vulnerabilities in Medical Devices: A Complex Environment and Multifaceted Problem. Medical Devices: Evidence and Research, 8, 305–316. https://doi.org/10.2147/MDER.S50048