

MDR, CRA und NIS2 im Überblick

Regulatorische Anforderungen an vernetzte Geräte und Komponenten in der Medizintechnik:



© Shutterstock/raker

Ausgangslage: Vernetzte Systeme als neue Realität

Die technische Entwicklung in der Medizintechnik hat in den letzten Jahren zu einer signifikanten Zunahme an Vernetzung, Interoperabilität und Softwareabhängigkeit geführt. Geräte, die früher als abgeschlossene Einheiten funktionierten, sind heute häufig in übergeordnete IT-Systeme eingebunden, vernetzt mit anderen medizinischen Komponenten oder sogar mit cloudbasierten Diensten verbunden. Dies gilt insbesondere für moderne Diagnostiksysteme, OP-Assistenzsysteme und automatisierte Labortechnik.



Autor:
Daniel Heinzler
Business Development Manager
HMS Networks
www.hms.de

Vorteile und Herausforderungen

Dieser Wandel bringt nicht nur funktionale Vorteile – wie Telemedizin, Ferndiagnose oder Updatefähigkeit – sondern auch neue Herausforderungen. Denn in Zukunft verschmelzen funktionale Sicherheit („Safety“) und Informationssicherheit („Security“) immer mehr zu gemeinsamen Engineering-Aufgaben. Safety schützt Patienten vor unvermeidbaren Risiken durch das Produkt; Security schützt das Produkt und sein Umfeld vor Angriffen, Manipulation und Missbrauch.

Für Hersteller und Zulieferer stehen somit auch Komponenten, Baugruppen und eingebettete Systeme zunehmend im Fokus regulatorischer Anforderungen. Die Einhaltung technischer Normen reicht in vielen Fällen nicht mehr aus. Vielmehr fordert der Gesetzgeber nachvollziehbare Prozesse, dokumentierte Risikobetrachtungen und in manchen Fällen sogar produktbezogene Nachweise zu IT-Sicherheit und Cyberresilienz.

„Statischer“ Prozess wird zum Risiko

Früher war Versionsfixierung ein probates Mittel: Komponenten wurden „eingefroren“, Änderungen vermieden - und damit Test-, QM- und Zulassungsaufwand planbar gehalten. In vernetzten Systemen ist das heute der falsche Reflex. Neue Schwachstellen (CVEs) werden wöchentlich aufgedeckt, Supply-Chain-Abhängigkeiten (Libraries, Treiber, OS) ändern sich laufend. Ein „statischer“ Prozess wird so vom Sicherheitsnetz zum Risiko.

Kurzüberblick: Die drei großen Rechtsrahmen

- **Verordnung (EU) 2017/745 über Medizinprodukte („Medical Device Regulation“, MDR):**
Diese verpflichtet Medizinprodukte-Hersteller zu Risikomanagement über den gesamten Lebenszyklus, klinischer Bewertung, Post-Market Surveillance (PMS) und Post-Market Clinical Follow-up (PMCF). Cybersecurity ist dabei Teil der grundlegenden Sicherheits- und Leistungsanforderungen (u. a. Schutz vor unbefugtem Zugriff, sichere Updates, Protokollierung).

- **Verordnung (EU) 2024/2847 über horizontale Cybersicherheitsanforderungen („Cyber Resilience Act“, CRA):**

Sie legt für „Produkte mit digitalen Elementen“ (z. B. IPCs, Gateways, Embedded-Plattformen) verbindliche Security-by-Design-Pflichten fest - inklusive Schwachstellenmanagement, Updates, Sicherheitsdokumentation und Software-Stückliste („Software Bill of Materials“, SBOM). Ein Medizinprodukt kann vom CRA ausgenommen sein; Komponenten/Hilfsgeräte im Produktumfeld sind es in der Regel nicht.

- **Richtlinie (EU) 2022/2555 („Network and Information Security“, NIS2):**

Sie verlangt von „wesentlichen“ und „wichtigen“ Einrichtungen - darunter typischerweise auch größere Krankenhäuser - ein Informations-sicherheits-Management (z. B. Risikomanagement, Lieferkettenkontrollen, Meldepflichten). National wird das in Deutschland u. a. über das NIS2UmsuCG und branchenspezifische Standards (B3S) konkretisiert.

Zusammenfassung

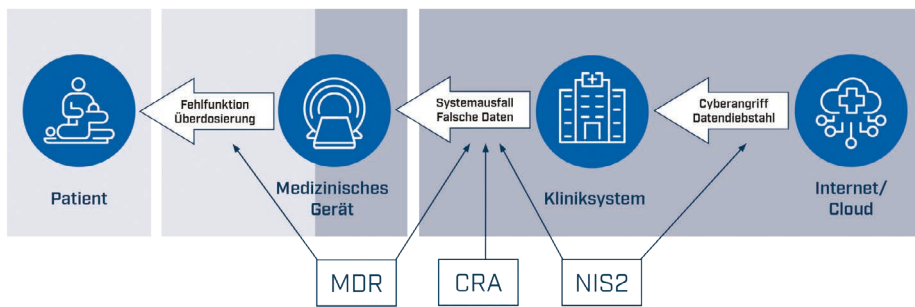
Die MDR regelt die Produkt-Safety und -Security, der CRA regelt Security-Pflichten für digitale Komponenten und die NIS2-Richtlinie regelt Security-Pflichten bei Betreibern (z. B. Krankenhäusern).

MSDR – Anforderungen an Geräte und Komponenten

Die europäische Verordnung (EU) 2017/745 über Medizinprodukte (MDR) stellt klare Forderungen an Sicherheit, Leistungsfähigkeit und klinische Eignung von Medizinprodukten. Auch wenn sich die MDR primär an Hersteller richtet, betrifft sie zunehmend auch Zulieferer – insbesondere dann, wenn ihre Komponenten Bestandteil eines zertifizierungspflichtigen Endprodukts werden.

Safety

Security



Safety & Security in der Praxis © HMS

Bereits im **Geltungsbereich (Artikel 1&2)** wird deutlich: Die MDR erfasst nicht nur das Endgerät, sondern auch deren Bestandteile wie Softwaremodule oder Zubehörteile, sofern sie funktional in das Medizinprodukt integriert sind. Besonders relevant ist dabei **Anhang I der MDR** („Allgemeine Sicherheits- und Leistungsanforderungen“), welcher zahlreiche technische Anforderungen beschreibt, die auch von Zulieferern beachtet werden müssen. Konkrete Abschnitte mit Auswirkung auf Embedded-Komponenten (Auszug):

- **Abschnitt 14.2(d):** Risiken in Zusammenhang mit möglichen Wechselwirkungen zwischen Software und der IT-Umgebung sollen ausgeschlossen werden.
- **Abschnitt 17.4:** Der Hersteller muss Mindestanforderungen an Hardware, IT-Netze und Cybersicherheitsmaßnahmen (Schutz vor unbefugtem Zugriff) für den bestimmungsgemäßen Betrieb festlegen.
- **Abschnitt 23(ab):** Anforderungen an Gebrauchsanweisungen und technische Unterlagen zu o. g. Mindestanforderungen.

Typische Anforderungen an Komponentenhersteller sind daher:

- Bereitstellung technischer Dokumentation mit sicherheitsrelevanten Informationen
- Nachweise zur Kompatibilität mit regulatorischen Anforderungen
- Unterstützung bei Risikobewertung
- Absicherung von Lebenszyklen und Updatefähigkeit

CRA – Cybersecurity für vernetzte Produkte

Der Cyber Resilience Act (CRA) ist eine EU-Verordnung für „Produkte mit digitalen Elementen“ (Hardware, Firmware, Software), die direkt oder indirekt vernetzt sind. Er gilt sektorübergreifend – also auch für eingebettete Standardkomponenten, Softwarebibliotheken, Module und IPCs, die später in Medizingeräten verwendet werden.

Wichtig für die Medizintechnik:

Medizinprodukte und deren Komponenten fallen nicht unter den CRA, wenn sie bereits den sektorspezifischen Regelungen wie MDR oder IVDR unterliegen (vgl. CRA Art. 2 Abs. 2(a)+(b)). Komponenten, die als eigenständige „Produkte mit digitalen Elementen“ in Verkehr gebracht werden (z. B. Netzwerkmodule, IPCs), also nicht explizit für den Gebrauch in Medizinprodukten, können aber CRA-pflichtig sein.

Aber: Wenn Komponenten, die später in Medizinprodukten eingesetzt werden, bereits CRA-konform sind, vereinfacht das die Integration und Konformität des Endprodukts für den OEM.

Anforderungen an Produkte aus dem CRA Anhang I:

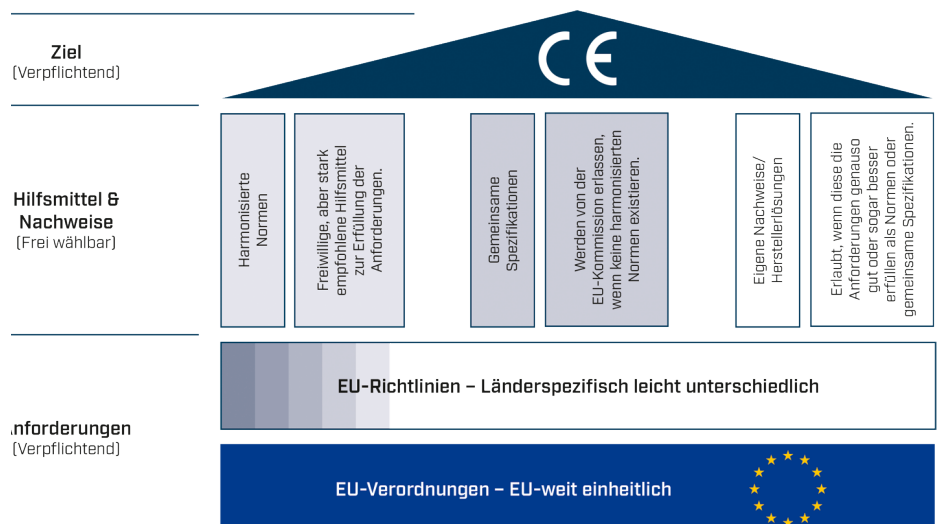
Teil 1: Hersteller von Produkten mit digitalen Elementen müssen ... (Auszug)

- ... diese ohne bekannte, ausnutzbare Schwachstellen in Verkehr bringen. (Anhang I, Teil I, Nr. 2 a)
- ... sichere Standardkonfiguration und Werks-Reset ermöglichen. (Nr. 2 b)

- ... die Patch-/Updatefähigkeit mit Sicherheitsupdates (ggf. automatisch) sicherstellen. Updates müssen innerhalb eines angemessenen Zeitrahmens installiert werden; Opt-out nur nutzerfreundlich und temporär. (Nr. 2 c)
- ... Schutz vor unbefugtem Zugriff durch geeignete Kontrollen bieten. Mindestens Authentifizierung, Identitäts-/Zugriffsverwaltung; unbefugten Zugriff detektieren/melden. (Nr. 2 d)
- ... so konzipiert, entwickelt und hergestellt werden, dass sie – auch bei externen Schnittstellen – möglichst geringe Angriffsflächen bieten.

Teil 2: Zur Behandlung von Schwachstellen/Vorfällen müssen Hersteller ...

- ... Software-Stücklisten (SBOM) in gängigem, maschinenlesbarem Format bereitstellen; mindestens Top-Level-Abhängigkeiten. (Anhang I, Teil II, Nr. 1)
- ... Schwachstellen zügig beheben und Sicherheitsupdates getrennt von Funktionsupdates ausliefern. „Unverzüglich“, risikobasiert. (Nr. 2)
- ... regelmäßig Sicherheit testen und überprüfen. Wirksame Security-Tests über den Lebenszyklus. (Nr. 3)
- ... koordinierte Offenlegung von Schwachstellen etablieren und Anlaufstelle veröffentlichen. CVD-Policy + Kontaktadresse für Meldungen; Informationsaustausch fördern. (Nr. 5 und Nr. 6)
- ... sichere Update-Lieferketten und kostenfreie, zeitnahe Sicherheitsupdates bereitstellen. Mechanismen für eine sichere Verteilung, ggf. automatische Installation; inkl. Hinweise/Handlungsempfehlungen. (Nr. 7 und Nr. 8)



Produktsicherheit in Europa: Gesetzliche Basis und Nachweiswege

Auch wenn es nicht gesetzlich gefordert ist, stärkt die Einhaltung der CRA-Pflichten (Secure-by-Design, Patchfähigkeit, SBOM, Vulnerability-Handling) die Sicherheit von Subsystemen und liefert dem OEM belastbare Nachweise für MDR-Anforderungen (z. B. Risikomanagement, IT-Sicherheitsmaßnahmen). Im Ergebnis führt dies zu einem geringeren Integrations- und Zulassungsrisiko, einer schnelleren CE-Kennzeichnung, weniger Feldmaßnahmen – und besserer Akzeptanz bei NIS2-pflichtigen Kunden.

NIS2 – Betreiberanforderungen und Auswirkungen auf Zulieferer

Die EU-Richtlinie NIS2 (Network and Information Security Directive) verfolgt das Ziel, die Cyberresilienz kritischer Infrastrukturen aus 18 verschiedenen Bereichen (unter anderem dem Gesundheitswesen) europaweit zu verbessern. Die Anforderungen richten sich zwar formal an Betreiber sogenannter „wesentlicher“ und „wichtiger Einrichtungen“ – darunter auch viele Krankenhäuser (bzw. Gesundheitsdienstleister), Labore und Hersteller von Medizingeräten – wirken mittelbar aber auch auf Zulieferer zurück.

Sicherheit der Lieferkette

Unter anderem wird als Risikomanagementmaßnahme im Bereich der Cybersicherheit (Art. 21) von den betroffenen Einrichtungen verlangt, die Sicherheit ihrer Lieferkette zu gewährleisten. Zusätzlich haben die Mitgliedsstaaten sicherzustellen, dass ein Austausch von Informationen zum Thema Cybersicherheit nicht nur mit den Einrichtungen selbst sondern ggf. auch deren Lieferanten oder Dienstleistern möglich ist (Art. 29).

Entscheidend dabei: Betreiber müssen Lieferkettenrisiken systematisch adressieren; dadurch steigen die Erwartungen an Zulieferer messbar.

Hinweis zur Einordnung von NIS2

NIS2 ist eine EU-Richtlinie (EU 2022/2555), keine Verordnung. Sie entfaltet ihre Wirkung erst nach Umsetzung in nationales Recht. In Deutschland geschieht dies über ein NIS2-Umsetzungsgesetz (inkl. KRITIS-Neuregelungen). Dadurch kann die nationale Ausgestaltung über die EU-Mindestvorgaben hinausgehen (vgl. NIS2 Art. 5 „Mindestharmonisierung“). Verordnungen (wie z. B. MDR und CRA) gelten dagegen ab einem benannten Stichtag in identischem Wortlaut in der kompletten EU.

Pflichten der Technischen Zulieferer

Die regulatorischen Anforderungen machen deutlich: Technische Zulieferer müssen heute mehr leisten als reine Funktionalität. Sie müssen belegen können, dass ihre Produkte sicher, dokumentiert und wartbar sind.

Typische Anforderungen:

- Security by Design
- Schwachstellenmanagement
- SBOM
- Patchfähigkeit
- Technische Dokumentation

Zulieferer, die ihren Kunden aktiv zuarbeiten – etwa mit Risikobewertungen, Cybersicherheitsdaten oder Supportprozessen – werden in Auswahlverfahren bevorzugt.

Fiktives Praxisbeispiel: Sicherheitskritischer Vorfall in einem NIS2-pflichtigen Krankenhaus

Die Ausgangslage: Ein Krankenhaus (NIS2-relevant) betreibt ein vernetztes Diagnosesystem (MDR-Produkt) mit integriertem IPC eines Zulieferers. Während einer Untersuchung friert das System ein; der Fail-Safe greift, die Untersuchung wird abgebrochen – Verfügbarkeit und potenziell Patientensicherheit sind betroffen.

Ablauf (verkürzt): Innerhalb von 24 h erfolgt die Early-Warning-Meldung gemäß NIS2; OEM und Zulieferer analysieren Logdaten und SBOM. Ursache ist eine bekannte Schwachstelle (CVE) in einer Netzwerkbibliothek des IPC; ein Patch des Zulieferers existiert, dem OEM war aber nicht kommuniziert worden, dass es sich hierbei um eine kritische Sicherheitslücke handelt, weswegen dieser geplant hatte, diesen erst beim nächsten Major-Update einzupflegen und nicht umgehend. Nach 72 h wird die Incident-Notification mit Details versendet. Binnen 14 Tagen liefert der OEM einen qualifizierten Hotfix, nach 30 Tagen folgt der Abschlussbericht mit Root-Cause und Maßnahmen.

Wer trägt in diesem Beispiel welche Verantwortung?

1. Krankenhaus (Betreiber, NIS2-pflichtig)

Pflichten:

- Betriebssicherheit sicherstellen (z. B. Fail-Safe, Patienten evakuieren, Dokumentation des Vorfalls).
- Meldepflichten: Early Warning binnen 24 h, Incident Notification binnen 72 h, Abschlussbericht binnen 30 Tagen.
- Zusammenarbeit mit OEM und Zulieferer, indem Logs, SBOM und Nutzungskontext bereitgestellt werden.

Risiko: Das Krankenhaus ist NIS2-Verpflichteter und steht in der direkten Haftung, falls Fristen oder Maßnahmen nicht eingehalten werden.

2. OEM (Hersteller des MDR-Produkts)

Pflichten:

- Qualifiziert den Patch und integriert ihn in den Systembuild.
- Erstellt und pflegt SBOM/VEX (zeigt, welche Komponenten betroffen sind und wie kritisch die Lücke ist).
- Trägt die Verantwortung für die klinische Sicherheit und MDR-Compliance des Gesamtsystems.
- Kommuniziert an das Krankenhaus: Schweregrad der Schwachstelle, Workarounds, verfügbare Hotfixes, Sicherheitsadvisories.

Risiko: Verzögerungen bei Qualifizierung und Kommunikation können Patientensicherheit gefährden und zu MDR-/NIS2-Verstößen führen.

3. Zulieferer (IPC-Hersteller/Komponentenlieferant)

Pflichten:

- Security-Monitoring: Schwachstellen (CVEs) in eigenen Komponenten verfolgen und bewerten.
- Patch-Bereitstellung: zeitnah Fixes liefern, inkl. Security-Advisory und Einordnung (z. B. CVSS-Score, Exploitbarkeit).
- Kommunikation: OEM muss aktiv informiert werden, warum der Patch sicherheitskritisch ist und welche Risiken bei Verzögerung bestehen.
- CVD-Prozess (Coordinated Vulnerability Disclosure): Security-Kontakt, Triage und Advisory an alle relevanten Kunden.

Risiko:

- Auch wenn das Krankenhaus nicht direkt Vertragspartner ist, kann NIS2 über die Supply-Chain-Pflichten den Zulieferer indirekt verpflichten.

Fazit

Regulatorische Anforderungen wie MDR, CRA und NIS2 betreffen längst nicht mehr nur Hersteller fertiger Medizingeräte. Auch Zulieferer geraten zunehmend in den Geltungsbereich – direkt oder indirekt. In einer vernetzten Systemlandschaft reicht technische Funktionalität nicht mehr aus. Produkte müssen regulatorisch nachvollziehbar sicher, kompatibel und dokumentiert sein.

Wer diese Anforderungen frühzeitig berücksichtigt, schafft Vertrauen – und Wettbewerbsvorteile. ◀

Mehr Informationen zum Thema finden Sie im kostenlosen Whitepaper. www.hms-networks.com/de/whitepapers/whitepaper/regulatorische-anforderungen-an-zulieferer-in-der-medizintechnik

