MedTech zwischen Innovation und Realität

Die Software-Hürde meistern

Software in Medizinprodukten stellt Hersteller vor neue Herausforderungen © Freepik/DC Studio

Die Medizintechnik befindet sich mitten in einer digitalen Transformation. Software wird zum entscheidenden Faktor für Innovation, Differenzierung und Anwendernutzen. Doch viele Hersteller tun sich schwer, digitale Lösungen sicher, zuverlässig und wirtschaftlich nachhaltig auf den Markt zu bringen.

Software und KI rücken ins Zentrum

Neue digitale Lösungen – von Softwareplattformen bis hin zu KI-gestützten Diagnoseverfahren – verändern grundlegend, wie Medizinprodukte und ihre Hersteller arbeiten. Die FDA [1] verzeichnete bis Juli 2025 insgesamt 1.250 zugelassene KI-gestützte Medizinprodukte. Nicht alle dieser Zulassungen stehen für bahnbrechende Neuentwicklungen. Vielfach handelt es sich um Software-Module, Updates oder spezialisierte Anwendungen. Der Trend bleibt dennoch eindeutig: Software und KI rücken ins Zentrum der Medizintechnik.

Herstellern fällt es jedoch oft schwer, die Brücke zwischen Innovation und Realität zu schlagen. Oder anders gesagt: Neue, smarte medizinische Produkte lassen sich nur schwer in marktfähige Lösungen und tragfähige Geschäftsmodelle übersetzen. Software in MedTech-Geräten stößt dabei schnell auf Hürden, die weit über die reine Entwicklung hinausreichen. Die regulatorischen Anforderungen – wie die Medical Device Regulations (MDR) - sind hoch und aufwendig.

Patientensicherheit im Vordergrund

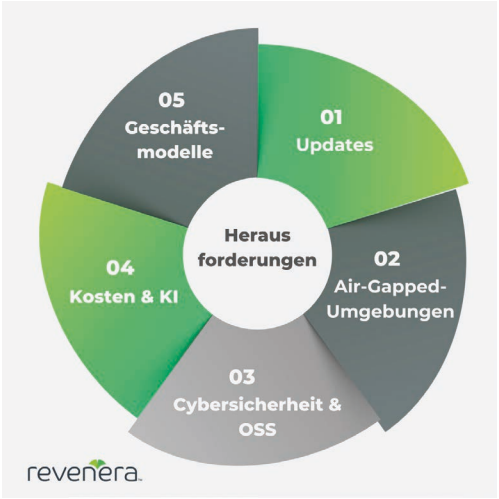
Anders als in vielen anderen Industrien steht die Patientensicherheit im Vordergrund. Gleichzeitig geraten Medizingeräte verstärkt ins Visier von Cyberangriffen. Laut IBM [2] lagen die durchschnittlichen Kosten eines Datenvorfalls im Gesundheitswesen 2024 bei 10,93 Millionen Dollar – der höchste Wert aller Branchen. Erfolgreiche MedTech-Software muss damit nicht nur innovativ, sondern auch robust, sicher und skalierbar sein.“

Fünf zentrale Herausforderungen

Ob digitale Innovation in der Praxis wirklich trägt, entscheidet sich an wenigen, aber zentralen Faktoren. Fünf Herausforderungen stehen dabei im Vordergrund:

1. Updates im „laufenden Betrieb“

Software-Aktualisierungen sind heute unverzichtbar für Sicherheit und Funktion. Dabei geht es längst um mehr, als Fehler im Code zu korrigieren. Moderne Releases erweitern den Feature-Umfang von bestehenden Hardware-Geräten, schalten Nutzer frei und verbessern die Kapazitäten oder Performance. Medizinische Geräte wie Anästhesiegeräte, Defibrillatoren oder Beatmungsgeräte sind oft mit hohen Investitionskosten verbunden und über einen langen Produktlebenszyklus hinweg im Einsatz. Updates stellen hier in erster Linie die Funktionsfähigkeit sicher, während regelmäßige Sicherheits-Patches gefährliche Schwachstellen und Sicherheitslücken schließen.



Herausforderungen steigen bei medizinischen Geräten in neue Dimensionen. © Revenera

Autorin:
Nicole Segerer
SVP & General Manager
Revenera
www.revenera.de

Zentrale Update-Plattformen

Für Hersteller ergibt sich daraus eine klare Konsequenz: Neue Updates müssen schnell, planbar und skalierbar bereitgestellt werden. Reparatur- und Wartungsprozesse sind im Klinik- und Praxiseinsatz schwer umzusetzen – wie die COVID-19-Pandemie gezeigt hat. Best Practices setzen auf zentrale Update-Plattformen, die es ermöglichen, Releases konsistent auszurollen. Manche Anbieter gehen noch einen Schritt weiter und bieten Self-Service-Funktionen an, über die Betreiber ihre Geräte eigenständig aktualisieren können. So bleiben Geräte aktuell und Hersteller reduzieren den Serviceaufwand wie auch Time-to-Market.

2. Air-Gapped-Umgebung bei KRITIS

Im KRITIS Bereich arbeiten viele Institutionen in isolierten Netzwerken ohne Internetzugang. Das kann mehrere Gründe haben. Zum einen lässt sich über das „Air-Gapped"-Prinzip die Angriffsfläche nach außen reduzieren und das Risiko von Cyberattacken, Ransomware-Angriffen und Datenleaks minimieren. Zum anderen spielen auch Interoperabilität und Integrationsrisiken eine Rolle: Manche Betreiber trennen Netzwerke, weil sie befürchten, dass Updates oder externe Verbindungen ungewollte Wechselwirkungen mit anderen Medizingeräten oder bestehenden IT-Systemen verursachen könnten. Hinzu kommen praktische Szenarien, in denen Geräte mobil (z. B. Rettungsfahrzeuge) oder in abgelegenen Regionen mit instabiler Netzabdeckung eingesetzt werden.

Lösungsmöglichkeiten

Fehlt der direkte Draht zur Cloud lassen sich Standardmechanismen wie Updates, Echtzeit-Lizenzprüfungen oder Telemetrie nicht mehr ohne weiters durchführen. Doch es gibt alternative Strategien, um Systeme auf dem neuesten Stand zu halten. Dazu gehören beispielsweise kryptografisch signierte Update-Pakete, die über geprüfte Datenträger oder abgesicherte Gateways verteilt werden. Zeitgebundene Lizenzschlüssel kommen ohne permanente Verbindung aus. Audit-Trails helfen darüber hinaus, die Erfüllung regulatorischer Anforderungen nachvollziehbar zu dokumentieren. So lassen sich selbst unter Air-Gapped-Bedingungen Sicherheit, Stabilität und Funktionsumfang der Geräte dauerhaft gewährleisten.

Open Source Software (OSS) bringt Sicherheits- und Compliance-Risiken mit sich. © Revenera

3. Das Open Source-Risiko

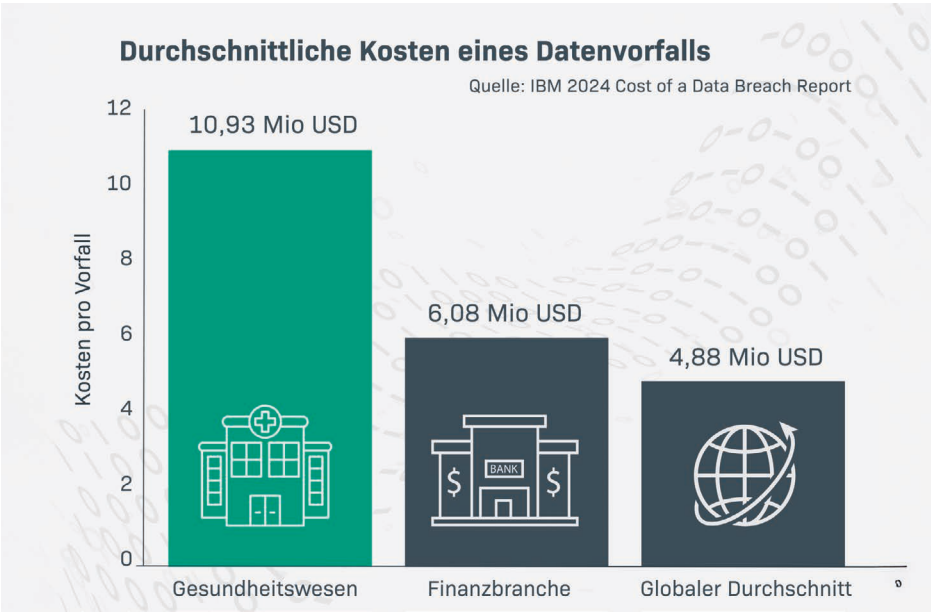
Open Source Software (OSS) macht in typischen Softwareanwendungen den Großteil des Codes aus. Das beschleunigt die Entwicklung, erhöht aber die Risiken durch fehlende Transparenz. Tatsächlich kennen viele Hersteller ihren eigenen Code nicht und können bei bekannt gewordenen Schwachstellen nicht einmal beurteilen, ob ihre Produkte betroffen sind. Dies zeigte sich jüngst bei der Log4j-Sicherheitslücke, die viele Organisationen über ihr tatsächliches Risiko im Unklaren ließ.

Lückenlose Software Bill of Materials

In der Medizintechnik ist das besonders kritisch: Hier verlangt die Regulierung nicht nur „Security by Design", sondern auch einen Nachweis über die eingesetzten Komponenten und deren Wartung. Der EU Cyber Resilience Act schreibt eine lückenlose Software Bill of Materials (SBOM) vor, die alle Module und Abhängigkeiten dokumentiert. Eine ähnliche Auflistung fordert auch das FDA im Premarket-Submission-Prozess.

Transparenz

über die gesamte Software-Supply-Chain sowie die kontinuierliche Prüfung auf Schwachstellen ist für Hersteller daher zentral. Best Practices setzen auf Software Composition Analysis (SCA), um automatisch SBOMs zu erzeugen und Abhängigkeiten mit Datenbanken für bekannte Schwachstellen abzugleichen. In modernen Entwicklungsumgebungen geschieht das früh im Prozess – nach dem Prinzip „Shift Left". Ergänzend lohnt sich der Aufbau eines Open Source Program Office (OSPO), das Richtlinien durchsetzt, Risiken bewertet und Entwicklerteams schult.



Kostspielige Cybervorfälle: Das Gesundheitswesen trifft es am stärksten. © IBM 2024 Cost of a Data Breach Report)

Die Integration von KI in Softwareprodukte braucht vernünftige Monetarisierungsstrategien.
© Revenera

4. Steigende Kosten – auch durch KI

MedTech-Unternehmen sind traditionell hardwaregetrieben. Viele Organisationen haben nur kleine Softwareteams, die oft nicht ausreichen, um komplexe Entwicklungs- und Compliance-Anforderungen abzudecken. Hinzu kommen hohe Aufwände für Dokumentation, Verifikation und Zertifizierung. Diese Fixkostenblöcke treiben die Entwicklungskosten in die Höhe und verlängern die Time-to-Market. Der Fachkräftemangel im Softwarebereich verstärkt das Problem zusätzlich.

Künstliche Intelligenz verschärft diese Lage erheblich. Modelltraining, Datenaufbereitung und Cloud-Infrastruktur verursachen hohe laufende Kosten, die sich nur schwer kalkulieren lassen. Laut einer MIT-Studie aus dem Jahr 2025 [3] erzielen 95 % der generativen KI-Pilotprojekte keinen messbaren finanziellen Return on Investment – die meisten bleiben in der Experimentierphase stecken und scheitern an der Wirtschaftlichkeit.

Regulatorische Unsicherheit

Hinzu kommt die regulatorische Unsicherheit. Mit dem EU AI Act und neuen Leitlinien der FDA entstehen zusätzliche Anforderungen an Dokumentation, Validierung und Überwachung von Algorithmen. Diese Vorgaben verlängern Entwicklungszyklen und erhöhen den Ressourcenbedarf weiter. Damit wird KI für viele Hersteller nicht nur eine technologische, sondern auch eine wirtschaftliche und regulatorische Bewährungsprobe.

5. Agile Geschäftsmodelle

Traditionell erzielen MedTech-Hersteller ihre Umsätze über einmalige Hardwareverkäufe. Mit Software- und KI-Funktionen verändert sich diese Logik. Laufende Betriebskosten, etwa für Cloud-Infrastruktur oder Modellinferenz, lassen sich mit klassischen CapEx-Modellen kaum abbilden. Gleichzeitig erwarten Kunden transparente und flexible Preisstrukturen. Starre Abonnements bergen Risiken: Sie decken die variablen Kosten oft nicht ab und gefährden Margen. Laut dem Revenera Monetization Monitor 2025 Outlook [4] sind nur rund ein Drittel der Softwareanbieter (36 %) überzeugt, dass ihr aktuelles Preismodell wirklich zum Markt passt. Diese Unsicherheit spüren auch MedTech-Hersteller, wenn es um die Einführung digitaler Funktionen geht.

Hybride Modelle

aus Abonnement und nutzungsabhängigen Credits bieten die Chance, Fixkosten abzusichern und variable Lasten fair zu verteilen. Besonders bei KI-Features eignet sich dieser Ansatz: Basisfunktionen laufen im Abo, Premium-Analysen oder zusätzliche Nutzungsstunden werden über Credits abgerechnet. Ein weiterer Ansatz ist Feature-on-Demand: Eine Hardwarebasis, deren Funktionsumfang sich per Softwarelizenz gezielt freischalten lässt. So lassen sich Produktvarianten reduzieren und Upgrades flexibel gestalten.

Outcome-basierte Modelle

Ergänzend gewinnen Outcome-basierte Modelle an Bedeutung, bei denen der Preis an erzielte Ergebnisse geknüpft ist – etwa erfolgreich abgeschlossene Analysen oder Workflow-Automatisierungen. Entscheidend bleibt eine zentrale Plattform für Lizenz- und Update-Management, die auch Offline-Szenarien unterstützt und gleichzeitig Transparenz über Nutzungsmuster liefert.

Fazit

Am Ende geht es für Hersteller nicht darum, das nächste intelligente Superprodukt für den Medizinsektor oder die vermeintliche Killer-App im Gesundheitswesen zu entwickeln. Viel wichtiger ist es, Kundenerwartungen zuverlässig zu erfüllen und die Anforderungen des Marktes realistisch abzubilden. Entscheidend bleibt – auch im Zeitalter von KI, Cloud und Cyberschutz – die wirtschaftliche Tragfähigkeit. Nur so lässt sich Wettbewerbsfähigkeit langfristig sichern.

Quellenangaben:

[1] FDA AI-Enabled Medical Devices List
https://www.fda.gov/medical-devices/software-medical-device-samd/artificial-intelligence-enabled-medical-devices

[2] IBM 2024 Cost of a Data Breach Report
https://www.ibm.com/think/insights/cost-of-a-data-breach-healthcare-industry

[3] MIT/NANDA Initiative The GenAI Divide: State of AI in Business 2025

[4] Revenera Monetization Monitor 2025 Outlook: Software Monetization Models and Strategies
https://info.revenera.com/SWM-RPT-monetization-monitor-models-and-strategies

Wer schreibt:

Nicole Segerer ist General Manager von Revenera, Anbieter von Lösungen für Softwaremonetarisierung, Compliance und Nutzungsanalyse. Sie ist Experte für Monetarisierungsmodelle für Software, SaaS und IoT-Unternehmen. Mit ihrem Team unterstützt sie Softwareanbieter und IoT-Hersteller bei der Umstellung auf neue Geschäftsmodelle und der Optimierung der Softwaremonetarisierung und Compliance. ◄