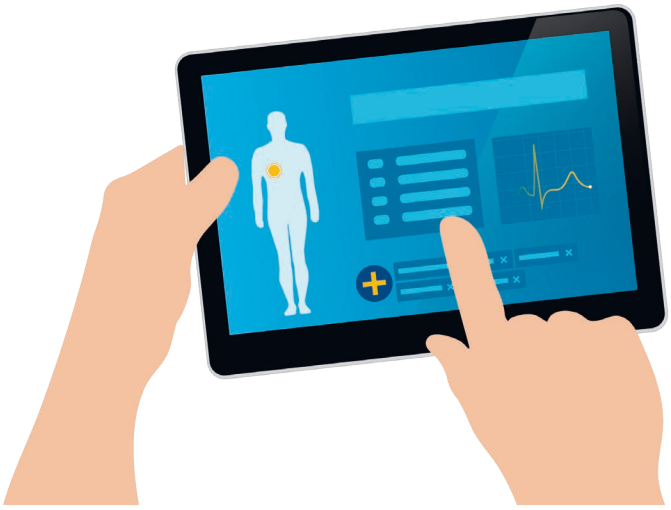
IT-Sicherheit wird zweite Säule neben der Produktsicherheit

Sicherheit von Medizinprodukten gemäß BfArM



© Pixabay

Die neue Medical Devices Regulations (MDR) ersetzt bestehende Richtlinien bei der Zulassung von Medizinprodukten. Sie bildet damit die Entwicklung von immer stärker vernetzter Technologie und die daraus resultierenden Risiken ab: Die IT-Sicherheit in BfArM (Bundesinstitut für Arzneimittel und Medizinprodukte) relevanten Produkten oder Anwendungen rückt in den Fokus, bei der Entwicklung, Herstellung und im Betrieb. Für die Hersteller bedeutet das eine Umstellung und den Aufbau neuer Kompetenzen.

Der Zulassungsprozess für Medizinprodukte ist komplex und folgt definierten Kriterien. Bisher stand dabei nur die Produktsicherheit im Mittelpunkt. Das ändert sich nun. Die europäische Verordnung über Medizinprodukte, (EU) 2017/745 (MDR), ersetzt die Richtlinien über Medizinprodukte (93/42/EWG, MDD) und aktive implantierbare Medizinprodukte (90/385/EWG, AIMDD). Die MDR ist bereits gültig und muss für erstmalig zugelassene Produkte auch angewandt werden. Für bereits zugelassene Produkte gibt es Übergangsregelungen, die spätestens 2025 auslaufen.

Potenzielle Risiken ausschalten bzw. minimieren

Die MDR umfasst sämtliche Aspekte eines Medizinprodukts. Ihre Novellierung wurde durch die zunehmende Digitalisierung im Medizinsektor notwendig – Medizintechnik und -produkte funktionieren nicht mehr autonom, sondern innerhalb vernetzter Systeme, was sie prinzipiell angreifbar macht. Damit sind das Risiko von Personenschäden und die IT-Sicherheit von Medizinprodukten in den Fokus gerückt: Der Behandlungsprozess mit analoger Arbeit des Mediziners und digitaler Arbeit durch Geräte kann nicht mehr entkoppelt werden. Medizinprodukte nehmen fortan direkten Einfluss auf den Körper des Patienten – seien es etwa Infusionspumpen oder bildgebende Verfahren wie Röntgen oder Computertomographien. Hier entsteht mit Blick auf die Patientensicherheit das Risiko einer ungewollten Manipulation: Etwa, wenn der 14-Jährige mit gebrochenem Bein im Krankenhaus aus Langeweile ein Röntgengerät hackt und mit der Dosierung spielt. Hersteller sind nun in der Pflicht, potenzielle Risiken auszuschalten bzw. zu minimieren. Hinzu kommt, dass sich das Sicherheitsniveau eines auf den Markt gebrachten, vernetzten Medizinprodukts im Laufe der Zeit verändert – etwa, wenn neue Schwachstellen und Sicherheitslücken entstehen. Auch dies bringt neue Anforderungen an den Zulassungsprozess mit sich.

Herausforderungen für die Hersteller

Für die Hersteller sind die Neuausrichtung und der dafür notwendige Perspektivwechsel hin zu Cybersicherheit bedeutende Herausforderungen: Denn bisher lag ihr Fokus darauf gewünschte Funktionen zu gewährleisten und sicherzustellen. Dabei ging man oft vom Best Case aus. Die IT-Sicherheit nimmt aber die gegenteilige Perspektive ein: Die Verhinderung unerwünschter Funktionen und damit die Fragestellung, wie Technologie manipuliert werden kann und welche Ereignisse zu Schäden führen können. Für Hersteller bedeutet das eine Umstellung – sie müssen daher neue Kompetenzen aufbauen.

Digitale Gesundheitsanwendungen

Hinzu kommt, dass zu Medizinprodukten nun auch digitale Gesundheitsanwendungen (DiGA), bspw. Apps auf Rezept, gehören. Auch diese wirken sich indirekt auf die Gesundheit der Nutzer aus – sei es bei Erinnerungsfunktionen zur Einnahme von Medikamenten, durch einen Ernährungsplan oder beim Vorhalten von Blutdruckangaben. Der Nutzer verlässt sich auf die Korrektheit der Informationen – und der Hersteller muss diese gewährleisten können. Software ist damit nicht mehr nur Bestandteil eines Medizinprodukts, sondern wird selbst zu einem Medizinprodukt. Die MDR deckt diese neue Realität nun ab – die Regulatorik muss also die technologische Entwicklung abbilden und auf die Entstehung neuer Produkte auf dem Markt reagieren.

Die Neuerungen im Detail

Folgende Neuerungen wurden durch die MDR im Detail erlassen:

- Der Anwendungsbereich wurde vergrößert. Die MDR umfasst nun ausdrücklich alle Produkte zur Reinigung, Sterilisation oder Desinfektion anderer Medizinprodukte, wiederaufbereitete Einmal-Medizinprodukte und bestimmte Produkte ohne medizinischen Zweck.
- Sie fordert einen Sicherheitsansatz, der sich am gesamten Produktlebenszyklus orientiert und durch klinische Daten untermauert wird.
- Die MDR stellt außerdem höhere Anforderungen an Benannte Stellen und führt eine Konsultation durch ein unabhängiges Expertengremium bei der klinischen Bewertung bestimmter Hochrisiko-Produkte ein.
- Darüber hinaus wird ein System zur Identifizierung und Rückverfolgung von Produkten (UDI – Unique Device Identifier) eingeführt.

© SRC GmbH

Autor:
Randolf Skerka, Business Development Manager Healthcare
SRC Security Research & Consulting GmbH
https://src-gmbh.de/

- Die MDR fordert außerdem die Eingabe umfangreicher Daten in die Eudamed-Datenbank und sie stellt Anforderungen an den Vertrieb von Medizinprodukten über das Internet bzw. an deren Fernabsatz.

Cybersicherheit

Die Anforderungen der Medical Devices Regulations an die Cybersicherheit sind im Anhang I der MDR, sowie in der „Guidance on Cybersecurity for medical devices“ formuliert. Während sie in den USA von der FDA herausgegeben und aktualisiert werden, besteht die Schwierigkeit in der EU darin, sie in nationale Gesetze umzusetzen. Die Anforderungen sind, wie üblich, nicht konkret. Unter anderem ist es die Aufgabe der für die Prüfung der Produkte zuständigen Benannten Stellen - i. d. R. privatwirtschaftliche Unternehmen wie TÜV oder Dekra - diese zu konkretisieren. Zudem besteht ein Nationaler Arbeitskreis (NAKI), der sich mit der Implementierung der EU-Verordnungen über Medizinprodukte (MDR) und In-vitro-Diagnostika (IVDR) beschäftigt und Konkretisierungen erarbeitet. Anders als bei der Zulassung von Arzneimitteln ist das Bundesinstitut für Arzneimittel und Medizinprodukte (BfArM) nicht in das Inverkehrbringen von Medizinprodukten involviert. Es ist aber für die zentrale Erfassung, Auswertung und Bewertung der bei Anwendung oder Verwendung auftretenden Risiken und für die Koordinierung der zu ergreifenden Maßnahmen zuständig.

Ein IT-Sicherheitskonzept wird notwendig

Hersteller von Medizinprodukten sehen sich künftig also mit der Aufgabe konfrontiert, gemäß dem Questionnaire IT Security for Medical Devices ein IT-Sicherheitskonzept für ihre Medizinprodukte zu erstellen. Zunächst erfolgt dabei die Schutzbedarfs-Feststellung. Dem schließt sich eine Bedrohungsanalyse an – damit wird die Frage beantwortet, was passieren kann, wenn das erforderliche Schutzniveau nicht erreicht wird. Eine Risikoanalyse zeigt die Auswirkungen des nicht vorhandenen Schutzes sowie geeignete Maßnahmen zur Vermeidung von Gefährdungen für Patienten, Anwender und Dritte. Sie beantwortet Fragen wie:

- Wie relevant ist eine Schwachstelle?
- Wie leicht ist sie auszunutzen?
- Und welches Schadpotenzial birgt sie?

Kontinuierliche Aktualisierung

Da eine Anforderung der MDR darin besteht, den gesamten Lebenszyklus eines Produkts abzudecken, muss das Sicherheitskonzept dauerhaft in einer kontinuierlichen Auseinandersetzung bzw. ereignisbasiert aktualisiert werden – etwa, um neu entstandene Schwachstellen zu berücksichtigen. In den isolierten Systemen früherer Zeit war die IT nach der Markteinführung keinen Änderungen mehr unterworfen. Heute muss der Hersteller für den Zulassungszeitraum seines Produkts gewährleisten, dass es sicher eingesetzt werden kann. Es ist üblich, dass die Zulassung eine Unveränderlichkeit bedingt, der Betreiber darf deswegen nur in eingeschränktem Bereich Änderungen wie die Aktualisierung eines Betriebssystems vornehmen. Die Hoheit liegt hier stets beim Hersteller. Gefordert ist unterm Strich ein sicheres Produkt, dass von einer sicheren Organisation entwickelt wird. Letztere wird durch die Prüfung des Produkts mitabgedeckt, da diese konkrete Anforderungen an die Organisation stellt, die erfüllt werden müssen.

Best Practices in der Zertifizierung

Hersteller müssen wissen, welche Kriterien im Prüfungsprozess der Zulassung zugrunde gelegt werden. Da die Produkte eine Prüfung bei den Benannten Stellen durchlaufen, ist es außerdem wichtig deren Veröffentlichungen zu diesem Thema zu kennen. Zentral ist hier der „Questionnaire IT Security for Medical Devices” der IG-NB. Insbesondere Hersteller, die neu auf dem Markt sind, müssen den Zulassungsprozess und seine Rahmenbedingungen verstehen.

Neue Herausforderungen durch die MDR

Insgesamt stellt die MDR Hersteller an drei Stellen vor (neue) Herausforderungen:

- Die Sicherheit im Entwicklungsprozess - Hersteller müssen nachweisen, dass sie in der Lage sind sichere Produkte zu entwickeln. IT-Risikoanalysen sind Teil davon, aber nicht die Kernkompetenz der Hersteller. Hier kann ein Partner wie bspw. die SRC GmbH unterstützen.
- Die zweite Herausforderung ist die Sicherheit des Produktes bis zur Markteinführung: Hier stellt vor allem Secure Coding, die Sicherheit in der Softwareentwicklung, viele Hersteller vor Herausforderungen. Denn Medizinprodukte werden heute durch Software gesteuert – Hersteller müssen deswegen die Anforderungen für ein sicheres Softwareprodukt kennen.
- Die dritte Herausforderung betrifft die Sicherheit des Produktes im Anwendungsfeld. Das umfasst vor allem das Schwachstellenmanagement. Neue Prozesse müssen dafür etabliert werden – auch hier benötigen Hersteller externe Unterstützung im Zulassungsprozess.

Fazit

Mit der Neufassung der MDR rückt bei der Zulassung von Medizinprodukten die IT-Sicherheit in den Fokus. Hersteller müssen diese während der Entwicklung und später dauerhaft beim Einsatz im Feld sicherstellen können und damit die Patientensicherheit gewährleisten. Notwendig wird dafür ein IT-Sicherheitskonzept mit Bestandteilen wie Risiko- und Schwachstellenmanagement – eine Daueraufgabe, da neue Risiken kontinuierlich bewertet werden müssen. Für Hersteller ist das mit dem Aufbau neuer Kompetenzen verbunden – hier kann ein externer Partner unterstützen. ◄