Cybersicherheits-Anforderungen gemäß der Verordnung (EU) MDR 2017/745 über Medizinprodukte

In einer zunehmend vernetzten Welt spielt Cybersicherheit dank technologischer Fortschritte bei der Entwicklung elektronischer Geräte eine zentrale Rolle. Cybersicherheit schützt vor Angriffen, die deren Zuverlässigkeit beeinträchtigen würden.

Wie lässt sich das Konzept Cybersicherheit definieren?

Cybersicherheit wird von der CISA (America's Cyber Defense Agency) definiert als „die Kunst, Netzwerke, Geräte und Informationen vor unbefugtem Zugriff oder krimineller Nutzung zu schützen, sowie die Praxis, die Vertraulichkeit, Integrität und Verfügbarkeit von Informationen sicherzustellen" („The art of protecting networks, devices, and information from unauthorized access or criminal use, and the practice of ensuring the confidentiality, integrity, and availability of information") [1]. Cybersicherheit umfasst in diesem Zusammenhang eine Reihe von Praktiken, die den Schutz elektronischer Geräte gewährleisten und sich dadurch auszeichnen, dass sie in verschiedenen Anwendungsbereichen eingesetzt werden können.

Im Bereich der Medizintechnik sind die Spezifikationen zur Cybersicherheit in Europa im Anhang I der Verordnung (EU) MDR 2017/745 [2] aufgeführt. Diese definieren die Mindestanforderungen an die Sicherheit, die sowohl bei der Entwicklung als auch bei der Vermarktung von Medizinprodukten, einschließlich IVDs („In-vitro-Diagnostika"), erfüllt werden müssen.

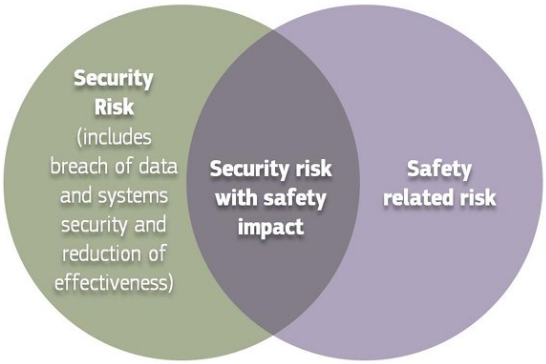
Was sind die Hauptaspekte, wenn es um Cybersicherheit für Medizinprodukte geht?

IT-Sicherheit für Medizinprodukte bezieht sich in erster Linie auf die folgenden Aspekte:

- Vertraulichkeit von Informationen, sowohl im Ruhezustand als auch während der Übertragung;
- Integrität, um die Authentizität und Genauigkeit von Daten zu gewährleisten;
- Verfügbarkeit von Prozessen, Geräten, Daten und verbundenen Systemen.

Diese drei Hauptaspekte werden durch das englische Akronym CIA zusammengefasst: „Confidentiality, Integrity, and Availability" (Vertraulichkeit, Integrität und Verfügbarkeit). Die

Hersteller sind demnach verpflichtet, Medizinprodukte nach dem neuesten Stand der Technik zu entwickeln und dabei den Grundsatz der Risikominderung im Bereich der Informationssicherheit umzusetzen. Darüber hinaus wirken sich Risiken im Zusammenhang mit der Sicherheit von IT-Systemen nur auf die technologischen Aspekte dieser Geräte aus, sondern können auch generell die Sicherheit beeinträchtigen. Daher ist es von entscheidender Bedeutung, durch entsprechende Cybersicherheits-Maßnahmen während des gesamten Lebenszyklus des Medizingeräts eine maximale Risikominderung zu gewährleisten, dies durch einen iterativen Prozess, der regelmäßige Systemaktualisierungen erfordert [3].



Cybersicherheitsmaßnahmen können laut MDCG 2019-16 [3] Auswirkungen auf die Sicherheit haben.

Ein Sicherheitsrisiko kann wie folgt aussehen: Ein Beatmungsgerät wird durch physischen Zugriff auf das Gerät über eine USB-Schnittstelle mit Malware angegriffen. Der Angriff führt dazu, dass das Gerät nicht mehr funktioniert, was die Sicherheit des Patienten während der Behandlung gefährden kann. Der Schutz der Zugangs-Ports zum Medizinprodukt ist daher von entscheidender Bedeutung, da ein mangelnder Schutz nicht nur ein Risiko für das Gerät selbst darstellt, sondern auch für dessen ordnungsgemäße Funktion und damit für die Gesundheit des Patienten während der bestimmungsgemäßen Verwendung. Cybersicherheitstechniken sollen das Gerät vor unerwünschtem Zugriff schützen und seine Funktionalität gewährleisten.

Gibt es Arbeitsgruppen, die sich mit der Harmonisierung von Cybersicherheitsansätzen für Medizinprodukte befassen?

Die Harmonisierung des Ansatzes zur Cybersicherheit von Medizinprodukten ist das Ziel einer internationalen Arbeitsgruppe des International Medical Device Regulators Forum (IMDRF), die derzeit den Leitfaden zur Cybersicherheit von Medizinprodukten [4] erarbeitet. Dieses Dokument

klärt die grundlegenden Aspekte der Gerätesicherheit und bietet Leitlinien für die Konstruktion von Geräten unter Berücksichtigung von Innovation, Leistung und Sicherheit.

Zusammenfassend lässt sich sagen, dass Mindestanforderungen an Cybersicherheit während des gesamten Lebenszyklus eines Medizinprodukts, vom Entwurf über den Vertrieb bis hin zur Wartung, berücksichtigt werden müssen, um eine maximale Leistung zu gewährleisten und die Gesundheit und Sicherheit der verschiedenen beteiligten Akteure zu schützen.

Referenzen:

- [1] „Was ist Cybersicherheit?“, www.cisa.gov
- [2] Verordnung (EU) 2017/745 des Europäischen Parlaments und des Rates
- [3] MDCG 2019-16 Rev.1, Guidance on Cybersecurity for medical devices (Leitlinien zur Cybersicherheit für Medizinprodukte)
- [4] Medical Device Cybersecurity Guide (Leitfaden zur Cybersicherheit für Medizinprodukte), www.imdrf.org

Stichworte: Cybersicherheit, Medizinprodukte, MDR 2017/745, MDCG 2019-16, Sicherheit

Autor: Gaia Di Federico, F&E-Elektroingenieur