zvei
electrifying ideas

Positionspapier

Medizintechnik braucht Cybersicherheit

Verband der Elektro- und Digitalindustrie

Vernetzte Medizintechnik

Medizintechnische Geräte und Anlagen in medizinischen Einrichtungen sind vielfach in IT-Netzwerke eingebunden, um Daten zu senden oder zu empfangen und IT-gestützte Arbeitsabläufe zu ermöglichen. Zahlreiche Geräte sind darüber hinaus permanent mit dem Internet verbunden, weil dies für den Betrieb oder für Wartungsmaßnahmen notwendig ist. Damit ist es erforderlich, Cybersicherheits-Anforderungen durchgängig zu berücksichtigen.

Die Vernetzung und Digitalisierung innerhalb der Gesundheitswirtschaft werden in den nächsten Jahren weiter fortschreiten. Dabei muss auch die Cybersicherheit medizintechnischer Geräte und Anlagen kontinuierlich beobachtet und weiterentwickelt werden. Zusätzlich ist zu erwarten, dass durch die Digitalisierung der Software-Anteil in den Geräten und Systemen steigt. Dieses wird zu weiteren Anforderungen hinsichtlich der Programmierung, Prüfung, Implementierung und After-Sales-Pflege der Software führen. Hersteller können das jedoch nur in der vorgesehenen Betriebsumgebung und unter Beachtung der Zweckbestimmung leisten.

Sowohl der europäische als auch der nationale Gesetzgeber fördern die Digitalisierung und haben in diesem Zusammenhang die Bedeutung von Cybersicherheit erkannt. Die damit steigenden Anforderungen an Medizintechnik und Betreiber spiegeln sich auch in den gesetzlichen Vorgaben.

Entsprechend dieser dynamischen Voraussetzungen stehen die folgenden fünf Punkte im Fokus:

1 Cybersicherheit als gemeinsame Aufgabe

Cybersicherheit von Medizinprodukten ist die gemeinsame Aufgabe der Hersteller und Betreiber. Für den Hersteller gehören dazu neben der Absicherung der Medizinprodukte auch angemessene Vorgaben für einen Einsatz dieser Medizinprodukte in der jeweiligen, vorgesehenen Betriebs- und Netzwerkumgebung. Die Betreiber müssen aufgrund ihrer originären Verantwortung für diese Umgebung sicherheitsbewusst handeln und die Hersteller-Empfehlung beachten. Die Hersteller unterstützen die Betreiber in Bezug auf die vom Hersteller zugelieferten, zweckbestimmen Produkte und Leistungen.

Hersteller, Betreiber, professionelle medizinische Anwender – und zunehmend auch Patienten – müssen gemeinsam dazu beitragen, einen sicheren Betrieb zu ermöglichen.

2 Cybersicherheit als integrale Anforderung an Medizintechnik

Cybersicherheit umfasst alle technischen (Hard- und Software) sowie organisatorischen Maßnahmen zur Gewährleistung des Angriffs- und Zugriffsschutzes bei medizintechnischen Geräten und Systemen. Diese gilt es sowohl für die Integration des Geräts in eine bestehende Netzwerkumgebung als auch hinsichtlich der funktionalen Eigenschaften des Geräts an sich umzusetzen. Zu bedenken ist dabei, dass z. B. durch einen unberechtigten Zugriff Daten, Dienste und Software des Medizingeräts derart manipuliert, beschädigt oder gelöscht werden können, dass das Medizingerät seine zweckbestimmte Funktion nicht mehr erfüllen kann oder Daten offengelegt werden.

Um dem entgegenzuwirken, sind risikobasiert abgestufte Cybersicherheits-Maßnahmen zu treffen, die die Vertraulichkeit, Integrität und Verfügbarkeit der Daten, Kommunikation und Funktionen im Medizingerät gewährleisten.

3 Cybersicherheit im gesamten Produktlebenszyklus

Die Cybersicherheit von Medizinprodukten muss während des gesamten Produktlebenszyklus gewährleistet werden. Die Organisationsreife eines Herstellers sowie des Betreibers im Hinblick auf Cybersicherheit ist daher maßgeblich für die durchgängige Verlässlichkeit eines Produkts. Im Rahmen der CE-Kennzeichnung von Medizinprodukten ist der Aspekt der Cybersicherheit schon

bei der Entwicklung, der Produktion und der Installation beim Kunden zu beachten. Dabei wird der aktuelle Stand der Technik berücksichtigt. Dieses schließt z. B. Cybersicherheits-Spezifikationen und -Verifikation im Entwicklungs- und Produktionsprozess mit ein. Erkenntnisse über neue Bedrohungen und Risiken und der sich stetig entwickelnde Stand der Technik müssen im Rahmen der Produktpflege mit einbezogen werden.

Hersteller und Betreiber berücksichtigen im Rahmen der Marktüberwachung auftretende Cybersicherheits-Risiken. Die daraus vom Hersteller abgeleiteten Maßnahmen und Vorgaben unterstützen den Betreiber bei einer möglichen Integration und in seiner Verantwortung zum sicheren Betrieb.

Industrieverbände, Wissenschaft und Behörden müssen gemeinsam einen fortlaufenden Dialog dazu führen. Verbände sind aufgefordert, über Branchenempfehlungen dessen Ergebnisse in die Breite zu bringen.

Der ZVEI unterstützt das Bundesamt für Sicherheit in der Informationstechnik (BSI) aktiv bei der Aufstellung von Empfehlungen für Maßnahmen der Hersteller und Betreiber bezüglich Cybersicherheit im Produktlebenszyklus.

Maßnahmen zur Verbesserung des Sicherheitsniveaus und insbesondere zur Schließung von Cybersicherheitslücken sollten allen Nutzern der Geräte und Systeme so schnell wie möglich aktiv angeboten werden. Die Verbesserung des Sicherheitsniveaus bereits installierter Geräte durch Nachrüstung sollte als eigenständige Aufgabe betrachtet werden.

4 Strukturierter Informationsaustausch

Hersteller und Betreiber entwickeln Prozesse, mit denen sie Hinweise auf Sicherheitslücken oder neue Gefährdungen von Anwendern, Forschern oder anderen Kreisen erhalten und verarbeiten. Ein gemeinsamer Informationspool kann dazu beitragen, dass entsprechende Hinweise schnell verbreitet werden und alle Betroffenen zügig geeignete Gegenmaßnahmen ergreifen können.

Durch einen strukturierten Austausch mit Behörden und allen Beteiligten der Gesundheitswirtschaft, z. B. über den UP KRITIS (Öffentlich-private Partnerschaft zum Schutz Kritischer Infrastrukturen in Deutschland), kann das Sicherheitsniveau weiter verbessert werden. Eine gemeinsame Analyse der Sicherheitsrisiken und der zugrundeliegenden Hard- und Softwaresysteme ist auch die Basis für die gemeinsame Entwicklung von Normen und Standards als Teil einer Sicherheitsarchitektur.

Hersteller von Medizinprodukten sollten deshalb den regelmäßigen Austausch mit Anwendern zum Thema Cybersicherheit suchen. Diese Erkenntnisse sollten sukzessive in die Produktentwicklung und die Produktpflege zurückfließen.

5 Benennung von Restrisiken im Betrieb

Im Rahmen der CE-Kennzeichnung wird für Medizinprodukte eine Risikoanalyse einschließlich Cybersicherheits-Aspekten durchgeführt, bei der die Zweckbestimmung des Geräts und seine wahrscheinliche Verwendung in der Praxis zugrunde gelegt werden. Soweit dabei Risiken für den Betrieb erkennbar werden, die nicht durch konstruktive Maßnahmen am Gerät selbst ausgeschlossen werden können, muss der Hersteller diese gegenüber dem Betreiber benennen.

In der Produktdokumentation und bei der Einweisung in den sicheren Betrieb des Geräts muss der Hersteller außerdem Vorschläge machen, wie Risiken vorgebeugt oder reduziert werden können.

Kontakt
Andreas Bätzel • Senior Manager Medizintechnik und Gesundheitsmarkt • Bereich Gesundheit •
Tel.: +49 69 63 02 388 • Mobil: +49 162 26 64 929 • E-Mail: andreas.baetzel@zvei.org

ZVEI e. V. • Verband der Elektro- und Digitalindustrie • Lyoner Straße 9 • 60528 Frankfurt am Main
Lobbyregister-Nr.: R002101 • EU-Transparenzregister ID: 94770746469-09 • www.zvei.org

Datum: 16.05.2023