ZVEI: Die Elektroindustrie

Positionspapier

Medizintechnik braucht Cybersicherheit

August 2017

Zentralverband Elektrotechnik- und Elektronikindustrie

Vernetzte Medizintechnik

Medizintechnische Geräte und Anlagen in Krankenhäusern und Arztpraxen sind vielfach in IT-Netzwerke eingebunden, um Daten zu senden oder zu empfangen und IT-gestützte Arbeitsabläufe zu unterstützen. Zahlreiche Geräte sind außerdem 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 innerhalb der Gesundheitswirtschaft wird in den nächsten Jahren noch weiter fortschreiten. Zusätzlich ist zu erwarten, dass durch die Digitalisierung der Software-Anteil in den Geräten und Systemen steigt. Dies wird zu weiteren Anforderungen hinsichtlich der Programmierung, Prüfung, Implementierung und After-Sales-Pflege der Software führen. Im Zuge dieser fortschreitenden Vernetzung und Digitalisierung muss auch die Cybersicherheit medizintechnischer Geräte und Anlagen kontinuierlich beobachtet und weiterentwickelt werden. Dies können Hersteller leisten – jedoch nur in der vorgesehenen Betriebsumgebung und unter Beachtung der Zweckbestimmung. Entsprechend stehen die folgenden Punkte im Fokus.

1. 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. Diese gilt es sowohl für die Integration des Geräts in ein bestehendes Krankenhaus-IT-Netz als auch hinsichtlich der funktionalen Eigenschaften des Geräts an sich umzusetzen. Zu bedenken ist dabei, dass durch einen unberechtigten Zugriff oder unbeabsichtigte Bedienung Daten, Dienste und Software des Medizingeräts derart offengelegt, manipuliert, beschädigt oder gelöscht werden können, dass das Medizingerät seine zweckbestimmte Funktion nicht mehr erfüllen kann.

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

2. Cybersicherheit während des gesamten Produktlebenszyklusses

Die Cybersicherheit von Medizinprodukten muss während des gesamten Produktlebenszyklusses gewährleistet werden. Dies schließt z. B. routinemäßige Cybersicherheits-Spezifikationen und -Testings im Entwicklungs- und Produktionsprozess mit ein. Die Organisationsreife eines Unternehmens im Hinblick auf Cybersicherheit ist daher maßgeblich für die durchgängige, umfassende Cybersicherheit und 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 und die Medizinprodukte stets daraufhin angepasst. Notwendigerweise entwickelt sich der Stand der Technik kontinuierlich weiter. Ebenfalls müssen Erkenntnisse über neue Bedrohungen und Risiken im Rahmen der Produktpflege einbezogen werden.

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

Der ZVEI unterstützt das Bundesamt für Sicherheit in der Informationstechnik (BSI) aktiv bei der Aufstellung von Empfehlungen für Maßnahmen der Hersteller 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.

3. Cybersicherheit als systemweite Aufgabe

Cybersicherheit von Medizinprodukten kann nicht die alleinige Aufgabe der Hersteller sein. Neben der Absicherung der Medizinprodukte gehören dazu auch angemessene Sicherheitsmaßnahmen für die Betriebs- und Netzwerkumgebung, in der die Medizinprodukte eingesetzt werden. Außerdem sollten die Anwender sicherheitsbewusst handeln und die Empfehlungen der Hersteller der Medizinprodukte beachten. Die Hersteller unterstützen die Anwender in dieser Aufgabe.

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

4. Informationsaustausch und Wissensvermittlung

Hersteller sollten Prozesse entwickeln, mit denen sie Hinweise auf Sicherheitslücken oder neue Gefährdungen von Anwendern, Forschern oder anderen Kreisen erhalten und verarbeiten. Ein gemeinsamer Informationspool der Hersteller von Medizinprodukten 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. Die Erkenntnisse sollten in die Produktentwicklung und die Produktpflege zurückfließen.

5. Unvermeidbare Risiken kenntlich machen

Im Rahmen der CE-Kennzeichnung wird für Medizinprodukte eine Risikoanalyse inklusive 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 selber ausgeschlossen werden können, muss der Hersteller diese gegenüber dem Anwender offenlegen.

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

ZVEI - Zentralverband Elektrotechnik-
und Elektronikindustrie e. V.
Fachverband Elektromedizinische Technik
Lyoner Straße 9
60528 Frankfurt am Main

Ansprechpartner:
Hans-Peter Bursig
Telefon +49 69 6302-206
E-Mail: bursig@zvei.org
www.zvei.org

Januar 2017