Angriffsszenarien durchzuspielen wird immer wichtiger

Medizintechnik rüstet sich für den Kampf gegen Cyberkriminelle

Es gibt auch bei vernetzten Medizinprodukten kein System ohne Sicherheitslücken. Diese ernüchternde Bilanz zogen Experten bei einer Veranstaltung des Verbands der Elektrotechnik (VDE) zur Cybersecurity in der Medizin. Die gesamte Medizintechnikbranche ist ein potenzielles Ziel von Cyberkriminellen.

Hacker sind eine Gefahr auch in der zunehmend digitalisierten Welt der Medizin.

© Thomasz Zajda/Fotolia.com

dabei auf den Gesundheitsbereich entfallen. Laut Molsen ist es für Medizintechnikanbieter bei der Entwicklung ihrer Produkte zur Risikominimierung für Cyberkriminalität unabdingbar, externe Experte einzubinden. Professionelle, unabhängige Penetrationstests von entsprechend qualifizierten Hackern zeigten schonungslos jede Sicherheitslücke auf, die dann noch vor der Marktreife des Produkts geschlossen werden kann.

Hohe rechtliche Auflagen

Medizintechnikanbieter bewegen sich in einem engen Regelungskorsett, wie die Juristin Dr. Julia Vorländer betonte. So müssten sie umfangreichen Pflichten genügen, die sich aus dem Medizinproduktegesetz und der Europäischen Medizinprodukteverordnung, der Medizinproduktebetriebsverordnung, dem Bundesdatenschutzgesetz und der im Mai nächsten Jahres greifenden EU-Datenschutz-Grundverordnung sowie dem Gesetz über das Bundesamt für Sicherheit in der Informationstechnik ergeben. Letzteres regelt die Sicherungs-, Melde- und Mitwirkungspflichten der Hersteller. Klärungsbedarf in puncto Verantwortlichkeit und Haftungsfragen im Zusammenhang mit gehackten Produkten mahnte Diplom-Ingenieur Hans Christian Wenner an, der sich auf die CE-Kennzeichnung und FDA-Zulassung von aktiven Medizinprodukten spezialisiert. Für ihn befindet sich die Welt längst im Zeitalter des Internet of Medical Things: „Dinge, auch Medizingeräte, sind permanent online, ohne dass der Benutzer direkt interagiert.“ Damit seien sie ein potenzielles Einfallstor für Cyberkriminelle – und das rund um die Uhr, das ganze Jahr über. Ein angepasstes und zeitgemäßes Risikomanagement werde im Internet of Medical Things von zentraler Bedeutung sein. *Matthias Wallenfels*

Gesundheitsdaten rücken immer mehr in den Fokus von Hackern. Für Aufregung bei Patienten hatte zum Beispiel der Fall eines großen US-amerikanischen Medizintechnikalters gesorgt, der seine Kunden in den USA und Kanada im vergangenen Jahr gewarnt hatte, dass eine seiner Insulinpumpen gehackt werden könnte. Wie Hannes Molsen, Web-Entwickler eines Lübecker Medizin- und Sicherheitstechnikkonzerns, aus der Praxis berichtete, könnten bei vernetzten Medizinprodukten in jeder Phase der Produktion Sicherheitslücken auftreten – vom Design über Entwicklung, Installation und Konfiguration bis hin zum Betrieb. Die kritischste Phase sei jedoch die erste. „Entstehen während des Aufsetzens der Architektur und des Designs eines Medizinprodukts Fehler, so lassen sich diese im Laufe der weiteren Entwicklung in der Regel nicht

mehr ausbügeln“, verdeutlichte Molsen. In dieser Konzeptphase müssten die Medizintechnikunternehmen nicht nur die Sicherheit des künftigen Produkts bedenken, sondern auch die Faktoren Verwendbarkeit, Wartbarkeit, Kosteneffizienz, Einfachheit und Funktionalität – angesichts gedeckelter Budgets oft mehr als ein Spagat. Allerdings, so Molsen, sei die Cybersicherheit kein Zufallsergebnis, sondern resultiere aus einem umfassenden Risikomanagement. Teil dieses Risikomanagements sei es, sich die verschiedenen Bedrohungsszenarien durch Cyberkriminelle vor Augen zu führen.

Dass sich Cyberkriminelle längst nicht nur auf den Gesundheitsmarkt in den USA konzentrieren, belegt eine Studie, wonach Cyberkriminelle allein 2015 weltweit 707 Millionen Datensätze erbeuteten. 23 % der Angriffe und nahezu ein Fünftel aller erbeuteten Daten seien