Cyber-Einbrecher – eine Gefahr auch in der zunehmend digitalisierten Welt der Medizin.

© Thomas Zajda/Fotolia.com

Optimiertes Risikomanagement wird immer wichtiger

Medizintechnik ist längst im Visier von Cyberkriminellen

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.

Für Aufregung bei Patienten gesorgt hatte zum Beispiel der Fall eines großen US-amerikanischen Medizintechnikbieters, der im vergangenen Jahr seine Kunden in den USA und Kanada gewarnt hat, dass eine seiner Insulinpumpen gehackt werden könnte.

Wie Hannes Molsen, Web-Entwickler bei einem Lübecker Medizin- und Sicherheitstechnikkonzern, aus der Praxis berichtete, könnten bei vernetzten Medizinprodukten in jeder Phase der Produktion Sicherheitslücken auftreten – vom Design über die Entwicklung, Installation und Konfiguration bis hin zum Betrieb. Die kritischste Phase sei allerdings die erste. „Entstehen während des Aufsetzens der Architektur und des Designs eines Medizinproduktes Fehler, so lassen sich diese im Laufe der weiteren Entwicklung in der Regel nicht mehr ausbügeln“, verdeutlichte Molsen. Cybersicherheit, so Molsen weiter, sei kein Zufallsergebnis, sondern resultiere aus einem umfassenden Risikomanagement.

Teil dieses Risikomanagements sei es wiederum, sich die verschiedenen Be-

drohungsszenarien durch Cyberkriminelle vor Augen zu führen. Wichtig für die Branche: Gesundheitsdaten rücken immer mehr in den Fokus von Hackern. Dass sich Cyberkriminelle längst nicht nur auf den Gesundheitsmarkt in den USA konzentrieren, belegt eine Studie, wonach Cyberkriminelle allein im Jahr 2015 weltweit 707 Millionen Datensätze erbeuteten. 23 % der Angriffe und nahezu ein Fünftel aller erbeuteten Daten seien dabei auf den Gesundheitsbereich entfallen.

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

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 über die Bestimmungen des Bundesamts für Sicherheit in der Informationstechnik ergeben. Letztere regeln die Sicherungs-, Melde- und Mitwirkungspflichten der Hersteller.

Neue Risiken durch „das Internet der Dinge“

Klärungsbedarf in puncto Verantwortlichkeit und Haftungsfragen im Zusammenhang mit gehackten Produkten mahnte Hans Christian Wenner aus Rüsselsheim an. Der Diplom-Ingenieur hat 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. Ein angepasstes und zeitgemäßes Risikomanagement werde daher im Internet der Medizin-Dinge von zentraler Bedeutung sein.

Matthias Wallenfels