CYBERSECURITY IN DER MEDIZIN

Wie können Hersteller und Betreiber von vernetzten Medizingeräten und IT-Netzwerken im Gesundheitssektor die Sicherheit erhöhen? Dies war die zentrale Frage bei der Veranstaltung „Cybersecurity in der Medizin" – organisiert von der DGBMT im VDE.

Es gibt kein System ohne Sicherheitslücken", so das Eingangsstatement von Hannes Molsen, Product Security Manager bei der Drägerwerk AG. Deshalb müssen Hersteller Cybersecurity-Strategien bereits bei der Produktentwicklung und für den gesamten Produktlebenszyklus etablieren. Neben der Sicherheit spielen bei der Wahl eines Produkts im Gesundheitssektor auch die Parameter Wirtschaftlichkeit und Einfachheit in der Bedienung eine wichtige Rolle. Hier müsse der Betreiber eines Medizinprodukts abwägen, ob auf Kosten der Security die genannten Faktoren im Vordergrund stehen sollen.

VON DER HERSTELLER- ZUR ANWENDERSEITE

Für die Anwenderseite ergriff Jochen Kaiser aus dem Servicecenter IT am Klinikum Stuttgart das Wort: Aus der Praxis schilderte er den „Clash of Cultures" zwischen IT- und Medizintechnik-Abteilungen in Kliniken: „Eine rein organisatorische Lösung hilft hier nicht weiter. Vielmehr müssen standardisierte Sicherheitsvorgaben definiert werden", betonte Kaiser. Wichtig sei auch ein neues Rollenverständnis für Medizingeräte: „Nicht mehr die Exzellenz in der Diagnostik sollte im Vordergrund stehen, sondern die Gesamtmischung aus Diagnostik, Service, Integration und Schnittstellenkosten beziehungsweise -qualität."

PENETRATIONSTESTS FÜR MEHR SICHERHEIT

Die Bedrohung im Gesundheitssektor sei real, so der IT-Forensiker Martin Wundram. Ihm und seinem Team sei es bei Penetrationstests gelungen, mit wenigen Klicks die Sicherheitsmaßnahmen von Kliniken zu überwinden: „Wir konnten Ärzten, Laboren und Apothekern bei ihrer Arbeit über die Schulter schauen. Nicht immer resultieren Gefahren aus einer unerlaubten privaten Nutzung des Internets durch die Mitarbeiter: In einem medizinischen Großlabor bestellte ein Mitarbeiter Berufskleidung über die manipulierte Seite eines deutschen Online-Shops und infizierte in der Folge das Netzwerk mit Schadsoftware. „Die zentrale Stellschraube ist häufig Komfort versus Sicherheit", so Wundram.

René Salamon, Verantwortlicher für den Sektor Gesundheit beim Bundesamt für Sicherheit in der Informationstechnik (BSI), bei der DGBMT-Veranstaltung „Cybersecurity in der Medizin" in Frankfurt/M.

© UWE NÖLKE

DGBMT

DGBMT im VDE

Ansprechpartner: Dr. Cord Schlötelburg
Geschäftsführer der Deutschen Gesellschaft für Biomedizinische Technik im VDE

Stresemannallee 15, 60596 Frankfurt

Tel.: +49-(0)69-6308-208

E-Mail: cord.schloetelburg@vde.com
www.vde.com/dgbmt

Seine Empfehlung lautet deshalb, das Netzwerk in durch Firewalls getrennte Teilbereiche aufzuteilen.

BALANCE ZWISCHEN INNOVATION UND HÄRTUNG SCHAFFEN

„Die Daten sind die Kronjuwelen ihrer Patienten. Die Queen stellt ihre zwar aus, aber nicht für jedermann zugänglich in die Cloud", brachte es René Salamon vom Bundesamt für Sicherheit in der Informationstechnik (BSI) auf den Punkt. Die Herausforderung bei Medizinprodukten: eine Balance zwischen Innovation und Härtung schaffen. Krankenhäuser würden in der Praxis häufiger angegriffen als etwa der Finanzsektor – weil es im Gesundheitssektor einfacher sei, an Daten zu kommen. Dem will der für Mai 2017 geplante zweite Teil der KRITIS-Verordnung – der auch den Gesundheitssektor betrifft – zum Schutz Kritischer Infrastrukturen Rechnung tragen. Im Zentrum stehe laut Salamon die Frage: „Wie kann es gelingen, dass IT-Sicherheit nicht den Fortschritt in der Medizintechnik behindert?"