DER ZUNAHME VON CYBERATTACKEN ENTGEGENWIRKEN

Und wieder ist es passiert: Elf Krankenhäuser und weitere vier Einrichtungen in Rheinland-Pfalz und im Saarland waren von einem Cyberangriff betroffen. Da stellt sich die Frage, was Betreiber, Hersteller und Politik tun können, um Angriffen aus dem Netz bestmöglich entgegenzuwirken.

Aktuell müssen nur diejenigen Krankenhäuser ein IT-Sicherheitskonzept auf dem Stand der Technik implementieren und regelmäßig aktualisieren, die nach dem IT-Sicherheitsgesetz zur Gruppe der Kritischen Infrastrukturen zählen. Durch die zunehmende Anzahl an Cyberangriffen muss die Absicherung des IT-Netzes aber in Zukunft nicht nur bei einzelnen Häusern, sondern generell bei allen Leistungserbringern höchste Priorität genießen. Ein umfassendes Sicherheitskonzept für das eigene Netzwerk und die darin betriebenen IT-Systeme und Medizingeräte sollten der zukünftige Standard in allen ambulanten oder stationären Einrichtungen sein.

Dazu zählt auch ein klar definiertes System von Zugriffs- und Nutzungsrechten. Nicht jeder Mitarbeiter benötigt uneingeschränkte Nutzungsrechte für alle Patientendaten, die während des Behandlungsverlaufs erhoben werden. Durch LogControl-Prozesse und deren Überwachungen wird jeder Zugang überprüfbar und auf jeden unberechtigten Zugriff kann schnell und konsequent reagiert werden.

Ebenso ist aufseiten der Medizinproduktehersteller die zunehmende Gefährdungslage umfassend zu berücksichtigen. Die gesetzlichen Anforderungen an Medizinprodukte müssen auch im Hinblick auf die Informationssicherheit angewendet werden. Dazu zählen unter anderem zusätzlich implementierte Sicherheitsfunktionen, wie z. B. Verschlüsselung, Zugriffsschutz und die elektronische Signatur. Solche und andere Maßnahmen müssen bereits im Entwicklungs- und Produktionsprozess eine noch größere Rolle spielen.

Für mehr IT-Sicherheit sind zudem ein breiter Dialog und eine praktische anwendbare Gesetzgebung notwendig. Der Expertenkreis „CyberMed“ innerhalb der „Allianz für Cyber-Sicherheit“ initiiert bereits einen regelmäßigen Austausch zwischen Vertretern der Industrie und Anwendern sowie Behörden. Ziel ist es, dass Betreiber künftig frühzeitig im Beschaffungsprozess produktbegleitende Informationen über die implementierten Cybersicherheitsmaßnahmen in Medizingeräten in standardisierter Form erhalten. Ziel muss es sein, solcher Guidance mehr politisches Gewicht zu verleihen. Der Ausbau des Expertenkreises zum Referenzgremium für die Cybersicherheit von Medizintechnik ist daher sinnvoll.

Nicht zuletzt bedeuten mehr Investitionen in eine sichere IT-Infrastruktur auch mehr personelle und finanzielle Kapazitäten. Gerade in der deutschen Krankenhauslandschaft bestehen schon heute große Finanzierungslücken, weil die Länder ihrer Investitionsverantwortung nicht nachkommen. In den nächsten fünf Jahren sind bundesweit mindestens elf Milliarden Euro zur Sicherstellung eines stabilen und sicheren Krankenhaus-IT-Betriebs notwendig. Das vom ZVEI und vielen weiteren Akteuren im Gesundheitssystem geforderte Investitionsprogramm des Bundes und der Länder darf zum Schutz der Patienten nicht länger auf sich warten lassen.

ZVEI: Die Elektroindustrie

ZVEI – Zentralverband Elektrotechnik- und Elektronikindustrie e. V.

Lyoner Straße 9, 60528 Frankfurt am Main

Tel.: +49-(0)69-6302-206
Fax: +49-(0)69-6302-390
E-Mail: medtech@zvei.org

www.zvei.org/gesundheit

Weitere Informationen, FAQs und Positionspapiere finden Sie auf der ZVEI-Internetseite im Themenbereich Gesundheit.

Hans-Peter Bursig
Geschäftsführer des ZVEI-Fachverbands Elektromedizinische Technik

BILD: © ZVEI