CYBERSICHERHEIT BRAUCHT STÄNDIGE AUFMERKSAMKEIT UND KLARE FÜHRUNG

Die digitale Transformation der Gesundheitsversorgung und damit die Vernetzung von Medizintechnik und IT nimmt Fahrt auf. Die positiven Effekte liegen auf der Hand: Eine vernetzte integrierte Gesundheitsinfrastruktur ist die Grundlage für optimierte Versorgungsabläufe und die individualisierte Versorgung von Patient:innen.

Gleichzeitig macht die zunehmende Digitalisierung die Einrichtungen der Gesundheitsversorgung in ihren alltäglichen Abläufen auch verwundbarer. Während die Vernetzung von Medizintechnik und IT voranschreitet, entwickeln sich auch die Arten von Cyberattacken weiter und erfordern eine kontinuierliche Aktualisierung der Cybersicherheitsmaßnahmen.

Für die Medizintechnik hat der Schutz medizintechnischer Geräte gegen Cyberangriffe in den vergangenen Jahren zunehmend an Bedeutung gewonnen. Die gesetzlichen Regelungen für Sicherheit von Medizinprodukten nach der Medical Device Regulation wie auch die spezielle Einsatzumgebung der Medizintechnik müssen hierbei berücksichtigt werden. Doch ein sicheres Medizinprodukt allein bietet noch keinen umfassenden Schutz: Cybersicherheit ist immer Teamarbeit!

Damit medizintechnische Geräte und Software innerhalb des Krankenhauses sicher Daten austauschen und ihre Funktion erfüllen können, muss die Absicherung des IT-Netzes im Krankenhaus höchste Priorität haben. Die wichtigste Voraussetzung für alle Maßnahmen ist außerdem ein grundlegendes Bewusstsein der Beschäftigten für diese Thematik.

Seitens der Politik braucht es eine klare Vorgabe, dass Cybersicherheit in der Gesundheitsversorgung zentral ist. Für alle muss klar sein, welchen Beitrag sie zur Cybersicherheit leisten können. Dafür ist der regelmäßige und strukturierte Austausch zwischen Herstellern und Anwendern notwendig. Der Gesetzgeber muss sicherstellen, dass alle Beteiligten im Gesundheitssystem, insbesondere Hersteller und Betreiber, Klarheit bezüglich ihrer jeweiligen Verantwortlichkeit für einen sicheren Betrieb haben. Die KRITIS-Gesetzgebung und das weiter gewachsene Bewusstsein für den Datenschutz nach Verabschiedung der EU-DSGVO haben bereits einen wichtigen Beitrag zum Sicherheitsbewusstsein geleistet. Durch die rasante Weiterentwicklung der IT-Landschaften in Kliniken, immer neue Cyberbedrohungen und entsprechende Gegenmaßnahmen im Bereich der IT-Sicherheit, kann ein dauerhafter und strukturierter Austausch zu mehr Sicherheit führen. Diesen Austausch sollte die Politik fördern. In den vergangenen Jahren hat die Anzahl von Cyberangriffen deutlich zugenommen. Das zeigt, dass das Thema Cybersicherheit kein Zukunftsthema ist, sondern sich rasant entwickelt und derzeit so akut ist wie wohl noch nie.

Die geplante Digitalisierungsstrategie im Koalitionsvertrag sollte das Thema Cybersicherheit deshalb unbedingt beinhalten, gerade auch für die Gesundheitswirtschaft.

ZVEI
Elektromedizinische Technik

ZVEI e. V.
Verband der Elektro- und Digitalindustrie
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

Pia Graß
Managerin Public Affairs Medizintechnik, ZVEI-Fachverband Elektromedizinische Technik

BILD: © ZVEI