CYBERSICHERHEIT: KOMPLEXE HERAUSFORDERUNG

Die Gesundheitswirtschaft steht beim Thema Cybersicherheit immer vor der Herausforderung, die Ziele für den Schutz und den Betrieb von IT-Systemen und Netzwerken in Einklang zu bringen.

Eine medizinische Versorgung auf aktuellem Niveau ist auf Online-Verbindungen angewiesen. Gleichzeitig nimmt die Bedrohung durch Cyberangriffe zu: In den vergangenen Jahren sind auch in Deutschland Krankenhäuser angegriffen worden und mussten den Betrieb unterbrechen. Das Krankenhauszukunftsgesetz (KHZG) sieht auch deshalb vor, dass geförderte Projekte einen bestimmten Anteil der Projektmittel für die Cybersicherheit verwenden müssen.

Für Krankenhäuser, die in Deutschland zur „kritischen Infrastruktur Gesundheit“ (KRITIS) gehören, gibt es schon länger die gesetzliche Verpflichtung, ein umfassendes Konzept für die Cybersicherheit umzusetzen. Der KRITIS-Branchenarbeitskreis „Medizinische Versorgung“ hat dafür einen branchenspezifischen Sicherheitsstandard (B3S) entwickelt. Seit 1. Januar 2022 sind alle Krankenhäuser in Deutschland durch § 75 c SGB V dazu verpflichtet, nach dem Stand der Technik angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen ihrer informationstechnischen Systeme zu treffen. Die Sicherheitskonzepte der Krankenhäuser müssen inzwischen auch die Anbindung der Krankenhäuser an die Telematikinfrastruktur berücksichtigen. Der B3S wird deshalb jetzt aktualisiert.

Die Interessen für den Schutz und den bestimmungsgemäßen Gebrauch von IT-Systemen und Medizinprodukten sind aber nicht immer gleichgerichtet. Cybersicherheit ist Teil der gesetzlich geforderten Maßnahmen zur Risikominimierung bei Medizinprodukten. Die Hersteller machen deshalb Vorgaben für die Netzwerkumgebung, damit der Betreiber die Produkte bestimmungsgemäß verwenden und für die medizinische Versorgung von Patientinnen und Patienten sicher nutzen kann. Allerdings sind in einem Krankenhaus oder einer Arztpraxis unterschiedliche Medizinprodukte und IT-Systeme im Einsatz. Die Absicherung des Netzwerks der Gesundheitseinrichtung gegen Cyberangriffe muss deshalb die Vorgaben der verschiedenen Hersteller berücksichtigen und dabei eine möglichst starke Absicherung gegen Cyberangriffe erreichen. Dies ist am besten über ein umfassendes Sicherheitskonzept für die gesamte Gesundheitseinrichtung zu erreichen. Zwei Leitfäden des ZVEI bieten hierfür eine erste Orientierung und verweisen auf internationale Normen.

In dieser komplexen Situation müssen Betreiber und Hersteller zusätzlich darauf reagieren, dass sich die Bedrohung durch Cyberangriffe ständig verändert. Für beide Seiten ist ein regelmäßiger Austausch deshalb wichtig, damit die verschiedenen Sicherheitsmaßnahmen ihre Aufgabe erfüllen können. Der ZVEI und seine Mitgliedsunternehmen beteiligen sich deshalb in der Allianz für Cybersicherheit am „Expertenkreis CyberMed“. Er bietet Betreibern und Herstellern eine übergreifende Plattform zum Austausch und gemeinsamen Arbeiten.

zvei
electrifying ideas

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

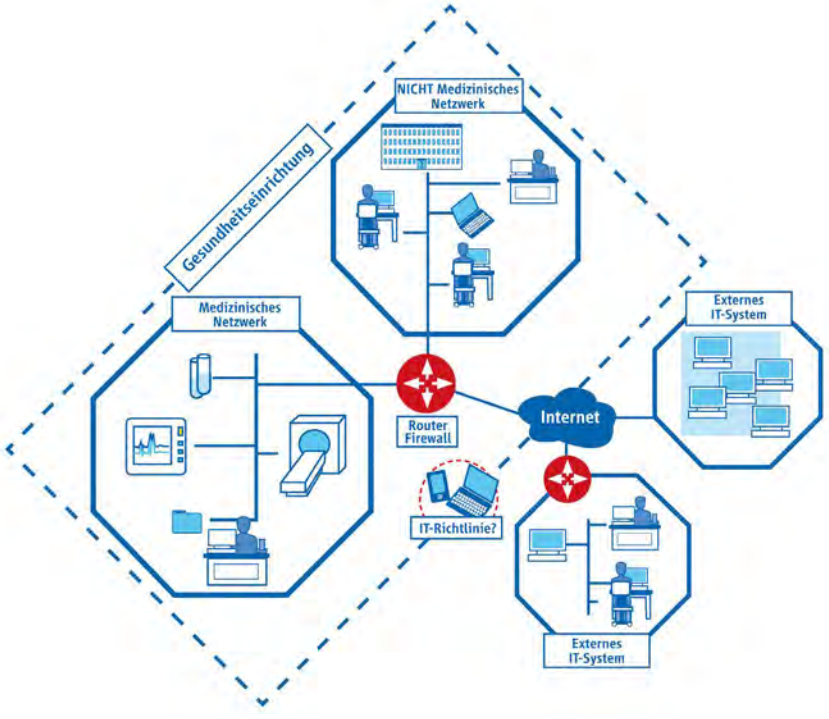

BILD: © ZVEI