Digitalisierung im Gesundheitswesen: ein zweischneidiges Schwert

Der zunehmende Umfang digital erfasster Patientendaten ist auch eine Quelle erhöhter Cyberrisiken, mit denen proaktiv umgegangen werden muss.

Der Datenschutz und die Absicherung der immer stärker vernetzten Informationssysteme sind bei Gesundheitseinrichtungen jeder Art ein Dauerthema, besonders nach der Einführung der Datenschutz-Grundverordnung (DSGVO) und der erfolgten Einordnung der im Gesundheitswesen tätigen Organisationen zu den kritischen Infrastrukturen (KRITIS).

Das wachsende Interesse der Cyberkriminellen

Dies konfrontiert die Gesundheitsbranche aufgrund erhöhter Risiken mit strengeren Normen und Auflagen als andere Marktsegmente, insbesondere bei der „Privacy by Design“ und der Informationssicherheit: Nicht nur die Wahrung der Vertraulichkeit der Patientendaten, sondern auch deren Integrität und Verfügbarkeit zu jedem Zeitpunkt werden klar vorgeschrieben. Das neue Regelwerk kommt zu einer Zeit, in der Gesundheitseinrichtungen einen großen Spagat zu bewältigen haben: Einerseits setzt man immer öfter auf neue Technologien (Fernsprechstunde, Fernuntersuchung, medizinische Fernüberwachung durch Apps, Fernhilfe und medizinische Regulierung), um einen verbesserten Zugang zur Gesundheitsversorgung zu garantieren. Andererseits werden in kritischen Bereichen viel zu oft Geräte genutzt, die noch veraltete Betriebssysteme und Anwendungen aufweisen und sich dadurch leichter von Cyberkriminellen ausbeuten lassen. „Nicht nur Patientendaten, sondern auch medizinische Geräte sind mittlerweile zur Zielscheibe geworden“, bestätigt Uwe Gries, Country-Manager DACH bei Stormshield. So identifizierten z. B. israelische Forscher bereits im April des letzten Jahres eine Malware, die auf MRT-Bilder Tumore hinzufügen oder entfernen konnte.

Uwe Gries, Country Manager DACH bei Stormshield

Wichtig: Auf kleine Details achten

Zusätzlich zum erwähnten Spagat zwischen Digitalisierung und Obsoleszenz vieler für die Betriebskontinuität der Gesundheitseinrichtungen unerlässlicher Systeme entspringt die Anfälligkeit dieser Organisationen ebenfalls der Notwendigkeit, mit zahlreichen externen medizinischen Fachkräften (anderen Einrichtungen, unabhängigen Ärzten usw.) zusammenzuarbeiten. Das Ergebnis: ein immer größeres Aufkommen an abzusichernder Kommunikation zur Vermeidung von Datenlecks oder Datenverfälschung. „Oft scheitert‘s an den kleinen Details. Es kommt beispielsweise immer wieder vor, dass in Gesundheitseinrichtungen zwar modernste Firewalls und ausgefeilte Infrastrukturen für den externen Datenaustausch Einsatz finden, der interne Datenfluss allerdings nicht verschlüsselt und das interne WLAN-Netz mit zu schwachen Passwörtern versehen wird“, erwähnt Gries.

Als europäische Referenz für Cybersecurity im Bereich IT- und OT-Systeme, kritischer Infrastrukturen und sensibler Daten ist Stormshield der Meinung, dass die mit der unaufhaltsamen Vernetzung und Digitalisierung im Gesundheitswesen verbundenen Fragen der Cybersicherheit nicht länger als rein technische Anliegen betrachtet werden dürfen: Sie sind die Grundpfeiler der geschäftlichen Belastbarkeit der in dieser Branche tätigen Organisationen und deren Fähigkeit, trotz möglicher Krisensituationen lebenswichtige Dienste zu erbringen. Die Absicherung von Daten, Maschinen und Infrastrukturen im Gesundheitswesen müsste auf das Prinzip der umfassenden Verteidigung unter Einsatz verschiedener Technologien setzen und eine von Anfang bis Ende konsistente Überlagerung von Sicherheitsebenen vorsehen, die keine Arbeitsbereiche und -werkzeuge vernachlässigt. Da bekannterweise das Personal die erste Verteidigungslinie darstellt, ist eine weitreichende Sensibilisierung der Mitarbeiter für das Thema Cybersicherheit und digitale Hygiene genauso entscheidend.

Stormshield
dach@stormshield.eu
www.stormshield.com/de/loesungen/