IT-SICHERHEIT: DAS „SMARTE“ KRANKENHAUS RICHTIG ABSICHERN

ROHDE & SCHWARZ CYBERSECURITY Die Digitalisierung bietet der Gesundheitsbranche enorme Chancen. Damit sensible Daten sicher sind und es nicht zu Störungen der Abläufe kommt, sind neue IT-Sicherheitskonzepte und der Einsatz innovativer IT-Sicherheitslösungen erforderlich.

Vernetzte medizinische Geräte erleichtern die Zusammenarbeit von Ärzten. Gleichzeitig machen sie das „smarte Krankenhaus“ attraktiv für Hacker. Eine Studie von Roland Berger ermittelte, dass 2017 bereits 64 Prozent der deutschen Kliniken Opfer von Cyberattacken waren. Einer der letzten größeren Angriffe war der auf das Klinikum Fürth: Ein Virus war via Phishing-E-Mail eingeschleust worden. Die Folgen: OP-Ausfälle, Aufnahmestopp von Patienten.

Weitere Angriffsflächen bieten „Webapplikationen“. Sie sind über den Browser zugänglich und machen die Arbeit in der Gesundheitsbranche flexibler. Aber: Diese Anwendungen sind für Hacker leicht zu knacken. Datenbanken zählen zu den beliebtesten Angriffszielen, da sie große Datenmengen bereithalten.

Dabei ist der Schutz solcher Daten durch die EU-Datenschutz-Grundverordnung (EU-DSGVO) streng geregelt. Das „E-Health-Gesetz“ legt zusätzlich den Aufbau einer sicheren Telematikinfrastruktur fest. Zudem müssen Kliniken ab 30 000 vollstationären Fällen im Jahr ein Mindestniveau an Informationssicherheit nachweisen. Bei Verstößen drohen Sanktionen.

INDIVIDUELLE IT-SICHERHEITS-TECHNOLOGIEN

Neben rechtlichen und wirtschaftlichen Folgen können Angriffe zu Vertrauensverlusten bei Patienten führen. Um das zu verhindern, sind geeignete IT-Sicherheitskonzepte entscheidend: Spezialisten prüfen vorhandene Strukturen, die bei Bedarf mit individuellen Sicherheitstechnologien nachgebessert werden. Dabei sollten Kliniken auf Hersteller wie Rohde & Schwarz Cybersecurity setzen, die innovative BSI-zertifizierte Lösungen anbieten:

- Um Webapplikationen zu schützen, brauchen Krankenhäuser eine „Web Application Firewall“. Diese verhindert den Zugriff verdächtiger Inhalte und vermeidet, dass Webanwendungen zum Einfallstor für Schadsoftware werden.
- Daten werden vermehrt in der Cloud gespeichert. Selbst wenn Firewalls aktiv sind, können Cloud-Provider auf die Daten zugreifen. Deshalb sollten Kliniken auf Lösungen setzen, die Daten unabhängig von ihrem Speicherort und EU-DSGVO-konform schützen.
- Im Gesundheitsweisen ist die Absicherung digitaler Übertragungswege wichtig – etwa zwischen Krankenhäusern und Hausärzten von Patienten. Um die Übertragung trotz Verschlüsselung effizient zu halten, gibt es spezielle Produkte.
- Da 70 Prozent der Angriffe über das Internet erfolgen, muss auch der Browser abgesichert werden. Am gezieltesten ist das möglich mit einem virtuellen Browser: Dieser isoliert Attacken und vermeidet den Zugriff auf das eigene Netzwerk.

Auf Basis dieser Maßnahmen ermöglichen Gesundheitseinrichtungen weitere digitale Entwicklungen und stärken das Vertrauen der Patienten in das „smarte“ Krankenhaus.

Dr. Falk Herrmann
CEO bei Rohde & Schwarz Cybersecurity

ROHDE&SCHWARZ

Rohde & Schwarz Cybersecurity GmbH
Tel.: +49-(0)30 65 884 222
E-Mail: cybersecurity@rohde-schwarz.com
www.rohde-schwarz.com/cybersecurity