Liebe Leserinnen, liebe Leser

Wenn die IT ausfällt, ist das keine IT-Frage mehr

Was passiert in einem Krankenhaus, wenn zentrale IT-Systeme plötzlich nicht mehr verfügbar sind? Wenn Befunde nicht abgerufen werden können, die Kommunikation zwischen Stationen und Funktionsbereichen ausfällt oder vernetzte Medizingeräte nicht mehr wie vorgesehen arbeiten? Die Antwort darauf ist längst keine reine IT-Frage mehr. Mit zunehmender Digitalisierung werden Verfügbarkeit und Sicherheit digitaler Systeme zu einer Voraussetzung für den Krankenhausbetrieb – und damit auch für die Patientensicherheit.

Wie real die Bedrohung ist, zeigen aktuelle Zahlen. Eine Befragung unter 165 Gesundheitseinrichtungen kommt zu dem Ergebnis, dass mehr als die Hälfte der 58 befragten Krankenhäuser innerhalb der vergangenen zwölf Monate von einem Cyberangriff betroffen war – was bei jedem fünften Krankenhaus zu einer Betriebsunterbrechung führte. Zugleich bauen die Häuser ihre Schutzmaßnahmen aus: Rund vier von fünf Krankenhäusern verfügen über einen Notfallplan für schwere Cyberangriffe, mehr als 85 Prozent wollen Lösungen zur Angriffserkennung und -abwehr einführen oder ausbauen.

Auch die Politik reagiert. Das Bundesministerium für Gesundheit (BMG) bereitet ein ‚Sofortprogramm Cybersicherheit' vor, mit dem Krankenhäuser und weitere versorgungskritische Einrichtungen ihre IT- und Cybersicherheit stärken sollen. Geplant ist unter anderem ein Cybersicherheits-Hub, der Förderaufrufe durchführen, Anträge prüfen und Projekte begleiten soll. Die konkreten Förderbedingungen stehen noch aus, laut aktuellen Informationen sollen bis 2029 insgesamt rund zwei Milliarden Euro bereitgestellt werden, um Kliniken und medizinische Einrichtungen gegen Cyberangriffe abzusichern.

Cybersicherheit wird zur Betriebsfrage

Damit verschiebt sich die Frage, was ein Krankenhaus unter IT-Sicherheit verstehen muss. Firewall, Virenschutz und Multifaktor-Authentifizierung bleiben wichtige Grundlagen. Sie reichen jedoch nicht aus, wenn eine zunehmend vernetzte technische Infrastruktur geschützt werden soll. So ist zum Beispiel ein Medizingerät heute nicht mehr zwingend ein isoliertes technisches System. Es kommuniziert mit anderen Geräten, Informationssystemen oder externen Diensten und kann damit Teil der digitalen Angriffsfläche eines Krankenhauses werden.

Für die Sicherheitsstrategie bedeutet das einen Perspektivwechsel: Es genügt nicht, Schwachstellen zu verwalten und auf einen Angriff zu reagieren, wenn bereits Schaden entstanden ist. Krankenhäuser müssen erkennen können, was in ihren Netzen und an ihren vernetzten Geräten passiert. Dazu gehören eine möglichst vollständige Übersicht über die Systeme, eine Bewertung ihrer Kritikalität und Verfahren, mit denen ungewöhnliche Aktivitäten früh erkannt werden. Genau hier setzt die Titelstory dieser Ausgabe an.

Bild: Kai Gebel

Julia Rondot,
Verlegerin medhochzwei Verlag

Bild: Silke Weinsheimer

Sven Preusker,
Redakteur

Von der Aufgabe zur gemeinsamen Verantwortung

Hinzu kommt die regulatorische Entwicklung. NIS2 erweitert den europäischen Cybersicherheitsrahmen und stärkt die Verantwortung der Leitungsebene für das Risikomanagement. Informationssicherheit wird damit noch stärker zu einer Frage der Unternehmens- und Betriebsorganisation. Die eigentliche Herausforderung liegt deshalb nicht darin, möglichst viele Sicherheitsprodukte zu beschaffen. Es geht darum, die digitale Infrastruktur des Krankenhauses als Teil seiner kritischen Betriebsinfrastruktur zu verstehen. Dazu gehören Server und Netzwerke ebenso wie Patientenakten, Kommunikationssysteme, Gebäudetechnik und Medizingeräte.

Wenn ein digitales System ausfällt, darf die Frage nicht erst dann gestellt werden, welche Folgen das für die Versorgung hat. Sie muss bereits bei der Planung, Beschaffung, Vernetzung und Überwachung der Systeme beantwortet werden. Cybersicherheit ist damit eine gemeinsame Aufgabe von IT, Technik, Medizintechnik, Management und klinischen Bereichen. Daran wird sich künftig auch messen lassen, wie resilient ein Krankenhaus tatsächlich ist.

Wir wünschen Ihnen eine aufschlussreiche Lektüre!