EINE PUBLIKATION DES REFLEX VERLAGES ZUM THEMA

JULI 2021

IT-Sicherheit

www.it-sicherheit-info.de

REFLEX Verlag

GRUSSWORT

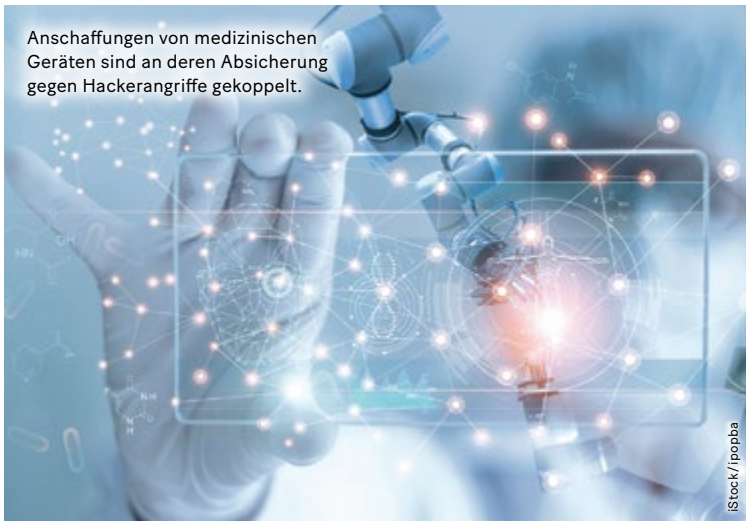
Sprung an die Weltspitze

In der Wirtschaft gibt es ein Umdenken. Zu viele sahen in kriminellen Hackern eine eher sekundäre Bedrohung. Doch im Jahr 2020 hatten digitale Verwüstungen mit geschätzten 72.000 Euro Schaden pro Attacke ein Ausmaß erreicht, das neue Gesetze und neues Bewusstsein erforderte. Dieses Umdenken ist verbunden mit dem Engagement und Wissen der Sicherheitsmitarbeiter:innen, die Fundamente für immer neue und ausgereiftere IT-Systemlandschaften aufbauen und so den digitalen Wandel mitgestalten. Deren Visionen, wie IT-Sicherheit gestaltet und weiter verfeinert werden kann, tragen den erwarteten wirtschaftlichen Aufschwung mit. Denn IT-Sicherheit ist mehr als Kämpfe gegen Bedrohungen aus den Netzen, als Schutz vor Spionage und Diebstahl. Es ist eine neue, aufstrebende Industrie, deren Hersteller aus Deutschland die Spitze der weltweiten IT-Expertise erobern werden.

Christian Raum
Chefredakteur

Milliarden Euro für den digitalen Wandel

KRANKENHAUSZUKUNFTSFONDS | VON CHRISTIN HOHMEIER



Anschaffungen von medizinischen Geräten sind an deren Absicherung gegen Hackerangriffe gekoppelt.

iStock/ipopba

Viele Krankenhäuser klagen, dass sie während der Corona-Pandemie in eine schwierige wirtschaftliche Lage gerutscht seien. Operationen und Behandlungen seien verschoben worden oder ganz ausgefallen, viele Häuser und Einrichtungen in die roten Zahlen gerutscht. Mit dem Milliardenfonds möchte die Regierung den Verantwortlichen Mittel bereitstellen, um wichtige Teile deren Infrastrukturen auf den Stand der Zeit zu bringen.

Schon lange hatten Politiker:innen einen Investitionsstau im Gesundheitswesen beklagt. Mit der Covid-19-Pandemie kamen dann scheinbar auch die wenigen verbliebenen Bemühungen für den digitalen Wandel nahezu zum Erliegen. Weil die Bundesregierung die Digitalisierung im Gesundheitswesen gefährdet sah – und auch erkannte, wie schlecht im Jahr 2020 viele Häuser für Epidemien wie Covid-19 ausgestattet waren – diskutierten die Gesundheitspolitiker:innen und Ministerien über die Einrichtung eines „Krankenhauszukunftsfonds". Im Oktober 2020 beschloss der Bundestag diesen Fonds mit drei Milliarden Euro auszustatten, verbunden mit der Verpflichtung der Bundesländer, noch einmal 1,3 Milliarden beizusteuern.

Finanzierung von Telemedizin, Robotik und IT-Monitoring

15 Prozent für IT-Sicherheit

Zur Vergabe der Mittel und der Förderung der Krankenhäuser und deren Infrastrukturen verabschiedete das Parlament im Oktober 2020 das „Gesetz für ein Zukunftsprogramm Krankenhäuser". Am 31. Dezember 2020 ist das Gesetz in Kraft getreten, seit dem ersten Januar stehen die Milliarden bereit. Ein wichtiger Aspekt innerhalb des Gesetzes sind die Bestimmungen rund um die IT-Sicherheit, den sicheren Datenaustausch und die Absicherung der internen Infrastrukturen sowie der Systeme zum Versenden und Empfangen von Daten – beispielsweise für Robotikanwendungen – oder Dokumente wie Patientenakten und Arztbriefe. Um diese Anforderungen abzusichern, sind die Mittel für die Digitalisierung an Investitionen in die IT-Systemsicherheit gebunden. ❑

Krankenhauszukunftsfonds

Wichtige Eckpunkte sind:

- In jedem geförderten Projekt müssen fünfzehn Prozent der Förderung in die IT-Sicherheit investiert werden.
- Ein Bestandteil des Fonds enthält Fördermittel speziell für die IT-Sicherheitsprojekte in den Krankenhäusern.
- Die Förderung fokussiert nicht nur auf die Investitionen für die Anschaffung neuer Produkte, sondern umfasst auch Beratungsleistungen und den Betrieb der IT-Systeme.
- Die Förderung ist auf drei Jahre beschränkt.

Fokusinterview

„IT-Sicherheitsüberwachung für Krankenhäuser"

Siego Kreiter, Geschäftsführer und CTO der IS4IT KRITIS GmbH erklärt, wie eine intelligente Security-Monitoring-Lösung wie IBM QRadar Sicherheitsbedrohungen frühzeitig erkennt und so der Entscheidungsfindung in Sicherheitsteams und im Management für Gegenmaßnahmen dient.

Welche Rolle spielt das Krankenhauszukunftsgesetz bei der Absicherung der digitalen Systeme? Über das Krankenhauszukunftsgesetz werden für Krankenhäuser zusätzliche Mittel für die Weiterentwicklung der Digitalisierung bereitgestellt. Mindestens 15 Prozent dieser Mittel müssen dabei in die IT-Sicherheit fließen. Ein weiterer Teil des Fonds ist explizit für IT-Sicherheitslösungen vorgesehen. Das wird auf jeden Fall einen positiven Einfluss auf die Gesamtsicherheit der IT-Landschaft der Krankenhäuser haben.

Welches sind aus der Sicht eines Krankenhauses wichtige Kriterien bei der Auswahl einer IT-Sicherheitslösung? Im Vergleich zu anderen kritischen Infrastrukturen haben Krankenhäuser spezifische Kriterien bei der Auswahl von IT-Sicherheitslösungen. Natürlich fordert der Gesetzgeber für die Gesundheitsdaten der Patienten einen besonderen Schutz. Andererseits stellt die Vielzahl unterschiedlichster medizinischer Geräte ein hohes Risiko dar. Weil diese Geräte eine lange Nutzungsdauer haben, arbeiten viele mit veralteter Software und haben deshalb keine optimale Absicherung gegen Angriffe. Eine umfassende Sicherheitslösung muss also alle IT-Systeme und alle operationalen Systeme im Krankenhaus überwachen.

Welche Rolle spielt dabei eine intelligente Software als Kern eines Sicherheitssystems? Eine Security-Monitoring-Lösung dient zur Überwachung und frühzeitigen Erkennung von Bedrohungen der gesamten IT-Infrastruktur eines Krankenhauses. In der Anfangsphase „lernt" die Software das normale Verhalten der IT-Systeme und der Anwender durch Beobachtung von Aktivitäten und Analyse des Datenverkehrs kennen. Später kann das System Abweichungen vom normalen Zustand erkennen und Alarme erzeugen. Ein Team von Security-Analysten kann diese Alarme auswerten, die Ergebnisse mit dem Management und der IT-Abteilung diskutieren und zum Beispiel bei Angriffen entsprechende Gegenmaßnahmen vorschlagen.

Welche Argumente sprechen für die Zusammenarbeit mit einem Dienstleister? Der Betrieb von IT-Sicherheitslösungen ist sicherlich nicht Teil des Geschäftszwecks eines Krankenhauses. Die hohe Komplexität solcher Systeme und der notwendige Aufwand für den Betrieb – insbesondere, wenn eine Rund-um-die-Uhr-Beobachtung notwendig ist – sind Argumente, die für die Zusammenarbeit mit einem spezialisierten Dienstleister sprechen. Dieser verfügt über das notwendige Know-how und auch die personellen Kapazitäten, um unabhängig von den alltäglichen Betriebsaufgaben der IT-Verantwortlichen im Krankenhaus die Sicherheitssituation im Blick zu behalten.