Sicher, mobil, zukunftsfähig: Trends im Gesundheitswesen 2025

Wie machen sichere Zugangsstrategien und moderne Technologien das Gesundheitswesen zukunftsfähig und schaffen ein Gleichgewicht zwischen Effizienz und Sicherheit?

Carmen Teutsch, Weinheim

Besonders das Thema Cybersicherheit stellt das Gesundheitswesen vor große Herausforderungen. Welche Trends und Technologien entscheidend sind, um Sicherheitsrisiken zu reduzieren und die Effizienz zu steigern, erläutert Fran Rosch, CEO von Imprivata im Interview.

Fran Rosch

M&K: Das Gesundheitswesen steht weltweit vor großen Herausforderungen, insbesondere im Bereich der Cybersicherheit. Welche Trends sehen Sie für 2025?

Fran Rosch: Eine der größten Herausforderungen für das Gesundheitswesen im Jahr 2025 wird die gleichzeitige Verbesserung der Cybersicherheit und der Effizienz klinischer Arbeitsabläufe sein. Komplexe Passwörter und umständliche Multi-Faktor-Authentifizierung (MFA)-Lösungen zur Erhöhung der Datensicherheit können die Arbeit des Klinikpersonals erheblich verlangsamen und zu Problemen bei der Patientenversorgung und Frustration führen. Gleichzeitig stellt die zunehmende Abhängigkeit von Drittanbietern ein wachsendes Risiko dar, das durch strenge Prüfungs- und Beschaffungsprozesse sowie eine umfassende Strategie zur Verwaltung des Zugriffs durch Dritte minimiert werden muss. Die Einhaltung gesetzlicher Vorschriften und die Gewährleistung der Compliance erfordern eine kontinuierliche Überwachung und ein konsequentes Zugriffsmanagement.

Zu den bedeutendsten Trends gehört der Einsatz passwortloser Authentifizierung, die nicht nur den Zugang rationalisiert, sondern auch die Sicherheit verbessert. Tools, die künstliche Intelligenz (KI) und maschinelles Lernen (ML) nutzen, ermöglichen es Organisationen, durch die Analyse von Benutzerverhalten und Systemnutzung fundierte Entscheidungen zur Optimierung von Workflows zu treffen, was gleichzeitig Sicherheitsrisiken reduziert und IT-Kosten senkt. Außerdem wird die Konsolidierung von Anbietern als Ansatz zur Risikominimierung immer wichtiger. Ein entscheidender Faktor bleibt die funktionsübergreifende Zusammenarbeit zwischen IT-, Sicherheits- und klinischen Teams, um Technologien so zu gestalten, dass sie optimal auf die klinischen Arbeitsabläufe abgestimmt sind. Durch diese Maßnahmen kann das Gesundheitswesen eine widerstandsfähige Umgebung schaffen, die nicht nur Patientendaten schützt, sondern auch das Vertrauen stärkt, Vorschriften einhält und die Effizienz der Patientenversorgung steigert.

Was zeichnet den DACH-Markt aus und wie können seine spezifischen Bedürfnisse adressiert werden?

Rosch: Der DACH-Markt hat einzigartige Anforderungen, insbesondere im Gesundheitswesen durch eine besonders hohe Sensibilität für Datenschutz und strenge regulatorische Vorgaben wie NIS2. Die Herausforderung besteht darin, sensible Patientendaten zu schützen, ohne die Arbeitsabläufe zu behindern. Hier sind Lösungen gefragt, die Sicherheit bieten, ohne den Klinikalltag zu verkomplizieren, wie beispielsweise die Kombination von Single Sign On und Multi-Faktor-Authentifizierung, die einen schnellen und sicheren Zugriff auf Patientendaten ermöglichen.

Zur Person

Fran Rosch, President und CEO von Imprivata, bringt über 25 Jahre Erfahrung im Bereich Sicherheit und Identitätsmanagement mit. Vor seinem Start bei Imprivata war er als CEO von ForgeRock tätig. Unter seiner Führung wuchs ForgeRock um über 400%, führte einen SaaS-Umstieg durch und etablierte sich als Marktführer in den Märkten Consumer Identity and Access und Workforce Identity.

Welche Herausforderungen sehen Sie bei der Integration von mobilen Geräten in die Arbeitsabläufe des Gesundheitswesens?

Rosch: Mobile Technologien sind der Schlüssel zur Weiterentwicklung des Gesundheitswesens. Sie ermöglichen es Klinikern, jederzeit und überall auf Patientendaten zuzugreifen, was die Effizienz und die Patientenversorgung deutlich verbessern kann. Doch hier liegt auch eine große Herausforderung: Eine vom Ponemon Institute in unserem Auftrag durchgeführte Studie zeigt, dass nur 28 % der IT- und Sicherheitsexperten glauben, dass ihre Strategien mobile Geräte und sensible Daten effektiv schützen.

Ein weiteres Problem ist die Benutzerfreundlichkeit. Nur 31 % der Mitarbeiter empfinden den Zugriff auf gemeinsam genutzte Geräte als einfach, und wiederholte manuelle Authentifizierungen führen zu Produktivitätsverlusten von bis zu 872 Stunden pro Woche. Mit unseren Enterprise Asset Management-Lösungen setzen wir auf passwortlose Authentifizierung und optimierte Workflows, um genau diese Herausforderungen zu lösen.

Welche Auswirkungen haben regulatorische Anforderungen wie NIS2 und wie unterstützt Technologie Krankenhäuser bei der Einhaltung dieser Vorgaben?

Rosch: NIS2 stellt hohe Anforderungen an die Cybersicherheit im Gesundheitswesen. Organisationen müssen nachweisen, dass sie angemessene Sicherheitsmaßnahmen implementiert haben, um den Zugang zu sensiblen Daten zu kontrollieren und Bedrohungen abzuwehren.

Unsere Technologien helfen Krankenhäusern, diese Anforderungen zu erfüllen. Mit MFA stellen wir sicher, dass nur autorisierte Personen Zugriff auf geschützte Gesundheitsinformationen erhalten. SSO wiederum reduziert die Komplexität und ermöglicht Klinikern schnellen Zugriff, ohne Abstriche bei der Sicherheit. Darüber hinaus unterstützen wir unsere Kunden mit Auditing-Funktionen, die eine kontinuierliche Überwachung und Anpassung der Sicherheitsstrategie ermöglichen.

Welche Vision verfolgen Sie für die Zukunft des Gesundheitswesens, insbesondere im Hinblick auf den Einsatz von KI und Mobilität?

Rosch: Ich bin davon überzeugt, dass KI und Mobilität das Gesundheitswesen revolutionieren werden. KI kann nicht nur dabei helfen, Bedrohungen zu erkennen und darauf zu reagieren, sondern auch die klinische Entscheidungsfindung und die Patientenversorgung verbessern. Wir müssen uns jedoch darüber im Klaren sein, dass KI-Anwendungen große Mengen sensibler Daten erfordern, was neue Herausforderungen für den Datenschutz und die Cybersicherheit mit sich bringt.

Unser Ziel bei Imprivata ist es, Sicherheit, Produktivität und Benutzerfreundlichkeit gleichzeitig zu verbessern. Wir wollen ein Ökosystem schaffen, in dem klinische Arbeitsabläufe durch mobile und KI-basierte Technologien effizienter werden, ohne die Sicherheit zu beeinträchtigen. Unsere Lösungen sind so konzipiert, dass sie Krankenhäuser dabei unterstützen, sich nicht nur an die aktuellen Anforderungen anzupassen, sondern auch für die Zukunft gerüstet zu sein. ■

| www.imprivata.com/de |

Standhinweis

DMEA
8. – 10. April, Berlin
www.dmea.de
Halle 4.2 | Stand B-107