Ganzheitliche IT-Sicherheit mit dem Cerner-Ecosystem

Managed Services – Cerner, übernehmen Sie!

Gemeinsam auf digitaler Reise

Cerner

Gerüstet für die Zukunft

Ganzheitliche IT-Sicherheit mit dem Cerner-Ecosystem

„Wir haben Ihre Patientendaten!“, ist so ziemlich das Letzte, was ein Krankenhausbetreiber in einer E-Mail lesen will. Und doch ist es bitterer Ernst. Laut der Roland Berger Krankenhausstudie 2017 wurden 64 Prozent der deutschen Krankenhäuser schon einmal Opfer eines Hackerangriffs. Ziel diverser globaler Angriffe mit Erpressungstrojanern, wie beispielweise „WannaCry“, waren Computer in branchenübergreifenden Unternehmen, unter anderem bei Maersk und der Deutschen Bahn. Während sich Reisende über die Fehlermeldungen auf den Anzeigetafeln eher ärgerten, führte der Cyberangriff in britischen Krankenhäusern teilweise zum Stillstand der medizinischen Versorgung. Mit der zunehmenden Digitalisierung vieler Krankenhäuser steigt, neben dem Bedarf an Notfallkonzepten und der Aufklärung der Mitarbeiter, auch der Bedarf an adäquaten IT-Security-Lösungen.

IT-Sicherheit aus einer Hand

„IT-Security ist ein sehr komplexer Bereich mit vielen Ebenen“, erklärt Stefan Ruch, Solution Leader bei Cerner Deutschland. „Die fortschreitende Digitalisierung in den Krankenhäusern stellt auch neue Anforderungen an die IT. Wer kann heute noch auf WLAN verzichten? Wie stelle ich meinen Patienten Inhalte zur Verfügung, wie tausche ich Daten mit anderen Krankenhäusern aus und schütze mich gleichzeitig vor unberechtigten Zugriffen? Es gibt viele Produkte, die zwar vereinzelte Probleme lösen, aber eine strategische Problemlösung hinsichtlich der IT-Sicherheit ausblenden. – Unser Ansatz ist ein anderer: Wir arbeiten mit den weltweit führenden Anbietern zusammen und bieten mit dem Cerner-Ecosystem ganzheitliche Lösungen aus einer Hand an“, erklärt Stefan Ruch. „Dazu kooperieren wir eng mit unseren Partnern zusammen, die zu Recht als Experten auf ihrem Gebiet gelten.“

Unter Druck durch KRITIS und DSGVO

„Vor dem Hintergrund des IT-Sicherheitsgesetzes für Kritische Infrastruktur (KRITIS) und der neuen Datenschutzgrundverordnung (DSGVO) steigt der Druck für Krankenhäuser, das Thema IT-Security noch stärker in den Fokus zu stellen“, sagt Carsten Emmerling, Program Manager, Managed Services bei Cerner Deutschland. „Auch wenn die KRITIS-Maßnahmen in erster Linie die ca. 100 systemrelevanten Krankenhäuser betreffen, müssen sich alle anderen Häuser ebenfalls daran orientieren und entsprechende Maßnahmen einleiten.“ Für alle Gesundheitseinrichtungen aber gilt ab Mai 2018 die verpflichtende Anwendung der neuen DSGVO und der nationalen Datenschutzvorschriften, sofern relevant, mit Öffnungsklauseln. „Für die Krankenhäuser bedeutet das vor allem viele zusätzliche Prozesse mit strengerer Rechenschafts- und Dokumentationspflicht sowie eines einheitlichen Datenschutzlevels in der gesamten EU und eingeschränkt über seine Grenzen hinaus“, erklärt Emmerling. Bei fehlenden Anforderungen drohen künftig empfindliche Strafen. So kann das Bußgeld pro Fall auf bis zu 4 Prozent des Jahresumsatzes festgesetzt werden. „Bei einem Umsatz von 100 Millionen Euro sind das also 4 Millionen Euro Bußgeld“, rechnet Carsten Emmerling vor. „Umsatzeinbußen können aber nicht nur eine Betriebsweiterführung gefährden. Hinzu kommen ein Reputationsverlust für die Einrichtung und möglicherweise Strafverfahren gegen verantwortliche Mitarbeiter.“ Besser ist also auf jeden Fall, es gar nicht erst dazu kommen zu lassen.

Managed Services – Cerner, übernehmen Sie!

„Gerade im Bereich IT-Security gibt es so viele Aufgaben, dass kleine IT-Abteilungen schnell an ihre Leistungsgrenzen stoßen“, weiß Emmerling. „Da müssen Updates und Patches zeitnah installiert, regelmäßige Backups durchgeführt und alles akribisch dokumentiert werden.“ Laut DSGVO müssen außerdem alle Systeme und Tools auf dem aktuellen technischen Stand sein. Allein das Expertenwissen in allen diesen Bereichen vorzuhalten, ist eine immense Herausforderung. Die Lösung: standardisierte Betriebsaufgaben an Cerner Managed Services abgeben.

„Mit unseren flexiblen Managed-Service-Angeboten können wir die IT-Fachleute im Krankenhaus bedarfsgerecht entlasten“, erklärt Emmerling. Kunden profitieren dabei von vielen Vorteilen:

- **Reduzierung des Betriebsrisikos**
  Cerner bietet die bestmögliche System-Verfügbarkeit, Performance sowie Betreuung, z. B. beim Hosting im Cerner-Rechenzentrum. IT-Abteilungen müssen sich keine Gedanken mehr um Einstellung, Training und Erhalt von eigenen Spezialisten machen.

- **Höchste IT-Sicherheit**
  Das Cerner-Rechenzentrum verfügt seit vielen Jahren über eine ISO 27001 Informationssicherheits-Managementsystem-Zertifizierung. Die Cerner-Datenschutzrichtlinie dient als Betriebsgrundlage. Mit der teilautomatisierten, proaktiven Überwachung inklusive Meldung und Analyse rund um die Uhr bietet Cerner ein vollständiges IT-Monitoring durch Experten. Außerdem unterstützt Cerner seine Kunden bei einer rechtskonformen, auditierfähigen Dokumentation nach DSGVO- und KRITIS-Maßgaben.

- **Von Erfahrungen aus aller Welt profitieren**
  Krankenhäuser profitieren von Cerner „Best Practices" und Skaleneffekten als KIS-Hersteller sowie vom globalen Betrieb und dem Hosting von mehr als 600 klinischen Systemen. Cerner unterstützt Projekte mit einem breiten IT-Know-how aus der Kundenbasis: Was ist wo wie möglich und praktikabel.

„Es geht hier um kritische Systeme mit hochsensiblen Daten. Ich kann nachvollziehen, dass es einem mulmig wird, wenn man daran denkt, eine komplette Systemlandschaft umzustellen", sagt Emmerling. „Aber wenn wir uns um Routineaufgaben auf höchstem IT-Security-Niveau kümmern, kann sich das IT-Personal auf das Wesentliche konzentrieren: sich um die internen Kunden kümmern, klinische Prozesse verbessern, den Ausbau der Systemlandschaft planen und Projekte umsetzen, die die Effizienz im Krankenhaus erhöhen."

Mit smarten Authentifizierungslösungen Zeit und Nerven sparen

Sich in unterschiedlichen Anwendungen mehrmals täglich immer wieder neu anmelden zu müssen, ist lästig und zeitaufwendig. „Studien haben ergeben, dass Ärzte und Pflegekräfte jeden Tag bis zu 45 Minuten allein für die Eingabe von Benutzernamen und Passwort verschwenden", sagt Stefan Ruch. „Dazu kommen weitere Sicherheitsvorkehrungen, etwa ein Passwortwechsel alle 90 Tage oder Zwangsabmeldungen nach Inaktivität. Das kostet nicht nur Zeit und Nerven, sondern reduziert auch die IT-Sicherheit, weil als Folge viele Nutzer ein einfaches Passwort für alle Anwendungen wählen. Sammel- und Stationsaccounts sind trotz DSGVO immer noch üblich. Sicherer und schneller ist die Authentifizierungslösung von Imprivata: Single Sign-on.

„Imprivatas Lösung ist ein wirksamer Baustein im Komplex IT-Sicherheit", erklärt Ruch. „Imprivata OneSign automatisiert den Anmeldevorgang und bietet u. a. passive und aktive Möglichkeiten zur Sicherung

Carsten Emmerling, Program Manager, Managed Services bei Cerner Deutschland

unbeaufsichtigter Arbeitsstationen und dient damit dem Schutz der Patientendaten vor unberechtigten Zugriffen." Ein Highlight ist sicherlich die dreidimensionale Gesichts- und Präsenzerkennung: Entfernt sich der Anwender vom Arbeitsplatz, wird der Bildschirm gesperrt. Kehrt der Anwender zurück, entsperrt sich der Monitor wieder. Außerdem zeichnet die Lösung sämtliche lokale und Remote-Zugriffsereignisse auf Anwendungen und Medizingeräte in einer zentralen Datenbank auf. Das bietet Administratoren eine hohe Transparenz in Bezug auf System- oder Anwendungszugriffe und ermöglicht eine schnelle Reaktion auf Audit-Anfragen. „Single Sign-on erhöht damit nicht nur die Sicherheit, sondern unterstützt auch Compliance- und Dokumentationsanforderungen."

Der Faktor Mensch

IT-Sicherheit ist aber nicht nur eine Frage der Technologie. Auch Mitarbeiterinnen und Mitarbeiter müssen für das Thema sensibilisiert werden. Gesetze und Verordnungen helfen da nur bedingt. Ein Bewusstseinswandel kann vor allem auch durch Aufklärung, Fortbildungen und Schulungen erreicht werden. „Und durch einen regelmäßigen Austausch", ergänzt Ruch: „Der *medico*®-Anwenderkreis Süd hat dazu eine Arbeitsgruppe ‚IT-Security' ins Leben gerufen. Dort tauschen sich Anwender und Cerner-Kolleginnen und Kollegen zum Thema aus. Außerdem bekommen wir auch immer wieder Feedback von unseren Kunden, was sehr hilfreich ist. So können wir kundenseitige Vorschläge in unsere eigenen Ideen und Entwicklungen einfließen lassen. Von diesem dialogischen Austausch profitieren also letztlich alle."

Info/Kontakt:
www.cerner.de
carsten.emmerling@cerner.com

GesundheIT im Wandel
Gemeinsam auf digitaler Reise

Über Cerner

Seit mehr als 35 Jahren entwickeln wir bei Cerner zusammen mit unseren Partnern IT-Lösungen, die als Ecosystem dazu beitragen, die Gesundheitsversorgung von heute zum Positiven zu verändern und die von morgen zu gestalten. Weltweit arbeiten in unserem Unternehmen über 26.000 Mitarbeiter an der Vision durch unsere Lösungen das Gesundheitswesen, und damit die Gesundheit von Menschen, stetig zu verbessern.

Die Nähe zu unseren Kunden ist dabei ein wesentlicher Faktor. Denn um weltweit gesammelte Erfahrungen und Ideen in lokale Gesundheitssysteme einfließen zu lassen, muss man diese auch wirklich verstehen.

Deswegen unterhalten wir im deutschsprachigen Raum zahlreiche Standorte – zum Beispiel in Berlin, Erlangen, St. Wolfgang, Idstein, Wien und Gmünd – an denen über 650 Kolleginnen und Kollegen leben und eng mit lokalen Partnern und Kunden zusammenarbeiten.

Mit unseren Lösungen tragen wir dazu bei, Prozesse zu optimieren, die medizinische Dokumentation und Kommunikation zu verbessern, Zeit und Ressourcen besser zu nutzen und Risiken oder Fehler zu reduzieren. Auf diese Weise können nicht nur eine größere Patientenzufriedenheit und höhere Behandlungsqualität erreicht werden, sondern auch eine gesteigerte Rentabilität – und damit ein finanzierbares Gesundheitswesen auf hohem Niveau.

Dabei ist unser Blick stets in die Zukunft gerichtet: Bereits heute arbeiten wir auch an Zukunftsthemen wie „Population Health Management“ und Big Data. Über 27.000 Gesundheitsorganisationen weltweit, davon rund 550 in Deutschland und Österreich, gehen bereits mit uns den Weg hin zum digitalen Krankenhaus und letztlich zu neuen Versorgungskonzepten.

Cerner Health Services Deutschland GmbH

Cunoweg 1
65510 Idstein, Germany
www.cerner.de
informationen@cerner.com

www.cerner.de