Foto: Zenzeta – stock.adobe.comm

Kliniknetze und der Schutz sensibler Daten im Cloud-Zeitalter

Das Krankenhauszukunftsgesetz als Chance für eine sichere und datenschutzkonforme Infrastruktur

Von Thorsten Ramm

Dass deutsche Krankenhäuser bei digitalen Infrastrukturen aufholen müssen ist unbestritten. Ebenso der Nutzen, den die Digitalisierung bringt: Sie optimiert Prozesse, erleichtert den Klinik- und Pflegealltag, reduziert den administrativen Aufwand. So bleibt mehr Zeit für die Pflege und die Patienten. Mit dem Krankenhauszukunftsgesetz (KHZG) stehen seit Anfang des Jahres 4,3 Milliarden Euro für die Einführung und Modernisierung digitaler Prozesse in Kliniken und Gesundheitseinrichtungen zur Verfügung. Ziel ist es unter anderem, leistungsfähige und sichere digitale Infrastrukturen aufzubauen. Darunter auch WLAN-Netze, die heute immer mehr über die Cloud verwaltet werden. Dies birgt Chancen, Risiken und Nebenwirkungen.

Keywords*: Digitalisierung, IT, Datenschutz*

Während in anderen europäischen Ländern digitale Technologien längst zum medizinischen Alltag gehören, hinkt Deutschland hinterher. Laut einer Studie des Deutschen Krankenhaus Instituts DKI von Ende 2019 haben nur elf Prozent krankenhausweit die elektronische Patientenakte vollständig umgesetzt, beim flächendeckenden WLAN sind es immerhin 36 Prozent.

Mit einem umfangreichen Förderprogram will der Bund die Digitalisierung nun vorantreiben und den Investitionsstau auflösen. Ein Teil der Mittel aus dem Krankenhauszukunftsgesetz wird in den Infrastrukturausbau fließen. Dazu gehört auch der Auf- bzw. Ausbau leistungsfähiger WLAN-Netze, da WLAN heute in vielen Kliniken nicht flächendeckend zur Verfügung steht. WLAN ist die Grundvoraussetzung für eine Vielzahl der digitalen Klinikprozesse – vom digitalen Patientenmanagement über Ortungslösungen bis zur WLAN-gestützten Telefonie und Alarmierung. Erst wenn eine leistungsfähige WLAN-Infrastruktur vorhanden ist, wird eine durchgängige Klinik-Digitalisierung überhaupt möglich.

WLAN als Grundlage für alle digitalen Prozesse

Eine professionelle WLAN-Infrastruktur ist die Grundlage für eine lückenlose digitale Behandlungsdokumentation. Per Tablet können Ärzte von überall aus sicher auf Befunde im KIS, PACS oder RIS zugreifen und Untersuchungsergebnisse direkt und digital am Patientenbett erfassen – die Daten müssen nicht mehr aufwändig per Hand übertragen werden. Über WLAN-Infrastrukturen werden auch mobile Patientenmonitore eingebunden und eine lückenlose Überwachung der Vitaldaten von Patienten sichergestellt.

Für die schnelle interne Krankenhauskommunikation sind Mobiltelefone die erste Wahl. Diese werden per WLAN mit der Klinikinfrastruktur vernetzt, sodass das Pflegepersonal jederzeit unabhängig von einer separaten DECT-Infrastruktur telefonieren oder Alarme auslösen kann.

Die Netzwerkinfrastruktur bildet aber auch die Basis für digitale Pa- ▶

tienten-Services: Diese reichen von WLAN-Hotspots über Patienten-Self-Service-Terminals bis zu multimedialen Anwendungen wie TV, Streaming, Musik oder Telefonie. Diese Patienten-Systeme werden – sicher separiert – in die Infrastruktur des Krankenhauses eingebunden.

„Der Europäische Gerichtshof kippte Mitte Juli 2020 das Datenschutzabkommen zwischen der EU und den USA. Damit wurde dem legalen Transfer personenbezogener Daten in die USA bzw. zu US-Unternehmen ein weitgehender Riegel vorgeschoben."

Integriertes Bluetooth als Basis für Ortungsdienste

Über eine simple Erweiterung der WLAN-Infrastruktur legen Kliniken die Basis für hocheffiziente Ortungsdienste. Voraussetzung ist, dass die eingesetzten WLAN Access Points als zusätzlichen Funkstandard Bluetooth unterstützen. Ob medizintechnische Geräte, Betten, Rollstühle – sie alle werden punktgenau per RTLS geortet. Es ist kein zeitaufwändiges Suchen mehr erforderlich, Mehrfachanschaffungen werden vermieden. Selbst eine App-gestützte Patienten-Wegeführung oder Sensor-basierte IoT-Anwendungen wie die Überwachung von Medikamentenschränken inklusive einer Temperaturüberwachung werden möglich. Für mehr Transparenz und Effizienz bei Raum- und Gerätereservierungen können Mobile Wireless ePaper Displays eingesetzt werden, die aktuelle Belegungs- und Buchungsinformationen automatisiert anzeigen.

Patienten können darüber hinaus mit Armbändern mit integrierten Funkmodulen zur Identifikation, Ortung und dem Auslösen von Alarmen ausgestattet werden. Das sorgt für mehr Sicherheit und Bewegungsfreiheit in der Pflege.

Netzwerkverwaltung aus der Cloud

Mit einem leistungsstarken WLAN wird in Gesundheitseinrichtungen der Grundstein für moderne digitale Prozesse gelegt. Doch die IT-Infrastruktur muss auch gepflegt und instandgehalten werden. Eine komplexe Aufgabe, die Experten-Know-how und Ressourcen erfordert und die mit der verpflichtenden Umsetzung des Sicherheitsstandards B3S Krankenhaus ab Januar 2022 noch einmal massiv an Bedeutung gewinnt.

Für den laufenden Betrieb, für Wartung und Management der WLAN-Netze bieten sich daher auch für Kliniken Cloud-Lösungen an: dabei wird das WLAN über eine Software in der Cloud verwaltet (im Fachjargon: Software-defined Networking) und muss nicht mehr zeitaufwändig vor Ort in der Klinik gemanagt werden.

IT-Verantwortliche oder Systemhauspartner rollen digitale Netze wie das Klinik-WLAN – und, je nach Lösung, auch alle weiteren, aktiven Netzwerkkomponenten wie Router und Switches – hochautomatisiert aus der Ferne aus, verwalten sie und sorgen für durchgängige Sicherheits-Policies. Bis zu 80 Prozent Zeitersparnis bei Wartung und Pflege sind mit einem Cloud-gemanagten Netzwerk möglich. Vom Cloud-gestützten Netzwerkmanagement profitieren Häuser aller Größen. Klinikverbunde mit mehreren Häusern können ihre Netze aufeinander abstimmen und nach einem einheitlichen Schema aufbauen und betreiben. Auf diese Weise werden sie auch zentral mit wichtigen Sicherheitsupdates versorgt.

Risiken und Nebenwirkungen: Beim Datenschutz auf Nummer sicher gehen

Die Digitalisierung und der Cloud-Einsatz bergen aber auch Risiken. Bei der Auslagerung der Netzwerkverwaltung in die Cloud verlassen laufend Daten die Kliniknetze, über die Rückschlüsse auf Patienten möglich sein könnten. Das Missbrauchspotenzial dieser Daten ist groß. Gerade im Gesundheitsbereich werden Unmengen sensibler Daten verarbeitet. Patienten, ihre Gesundheit und ihre Daten verdienen höchste Sorgfalt und größtmöglichen Schutz. Es muss sichergestellt werden, dass sie die Hoheit über ihre Daten behalten und die Patientendatensouveränität gewahrt bleibt.

Die Daten dürfen deshalb nicht ohne Weiteres in einer Cloud verarbeitet werden. Denn auch hier gilt es, Risiken und Nebenwirkungen abzuwägen. Nicht alle Anbieter erfüllen die strengen hiesigen Datenschutzvorgaben. Oftmals kommen die Cloud-Dienste von Lösungsanbietern aus dem Nicht-EU-Raum und unterliegen ausländischer Jurisdik-

Das Privacy Shield-Abkommen

Das Privacy Shield-Abkommen war ein Mechanismus für US-Unternehmen, mit dem sie sich mittels Selbstzertifizierung zur europäischen Datenschutzgrundverordnung (EU-DSGVO) konform erklären konnten. Unternehmen, Organisationen und Einrichtungen konnten sensible personenbezogene Daten an die Unternehmen übermitteln, ohne einen DSGVO-Verstoß zu riskieren. Der EuGH hat im Juli entschieden, dass das Privacy Shield-Abkommen zwischen der EU und den USA nicht mit der europäischen Datenschutzgrundverordnung (EU-DSGVO) vereinbar ist. Die Daten von EU-Bürgern werden nicht ausreichend vor dem unbegründeten Zugriff der US-Behörden geschützt. In anderen Worten: Wer personenbezogene Daten bei Cloud-Diensten von US-Anbietern verarbeitet, begeht in den meisten Fällen einen datenschutzrechtlichen Verstoß. Denn US-Unternehmen sind gezwungen, Daten an die US-Behörden herauszugeben, selbst dann, wenn sie Rechenzentren in der EU betreiben. Kein Vertrag, den sie mit Dritten abschließen, kann dies verhindern.

tion. In vielen Fällen handelt es sich dabei gemäß EU-Recht sogar um sogenannte „unsichere Drittstaaten". Jede Klinik muss sich deshalb die Frage stellen, welcher nationalen Gesetzgebung der Cloud-Anbieter unterliegt und ob dessen Lösung die strengen EU-Datenschutzvorgaben erfüllt.

Diese Herausforderung ist mit dem Ende des Privacy Shield-Abkommens noch größer geworden. Der Europäische Gerichtshof kippte Mitte Juli 2020 das Datenschutzabkommen zwischen der EU und den USA. Damit wurde dem legalen Transfer personenbezogener Daten in die USA bzw. zu US-Unternehmen ein weitgehender Riegel vorgeschoben. Die Nutzung vieler US-Cloud-Lösungen, darunter auch die Netzwerkverwaltung, wurde damit rechtswidrig – selbst wenn diese aus einem europäischen Rechenzentrum des Anbieters erfolgt.

Was jetzt zu tun ist: Datenschutzkonform investieren

Projekte im Rahmen des KHZG sind dann förderfähig, wenn sie mindestens 15 Prozent der Investitionen zur Erhöhung der Informationssicherheit vorsehen und nachweislich DSGVO-konform sind. Darin liegt eine große Chance: Kliniken, die bislang auf US-Lösungen setzen, sollten eine sorgfältige Risikoanalyse durchführen, datenschutzrechtlich kritische Anwendungen oder Prozesse identifizieren und Migrationsstrategien entwickeln. Das bedeutet auch, dass sie gegebenenfalls in eine neue Infrastruktur investieren müssen. Mit den Fördermitteln des KHZG können sie auf sichere, DSGVO-konforme Angebote umsteigen. Dann sind der DSGVO-konforme Umgang mit Patientendaten und die gebotene Patientendatensouveränität sichergestellt.

„Für die schnelle interne Krankenhauskommunikation sind Mobiltelefone die erste Wahl. Diese werden per WLAN mit der Klinikinfrastruktur vernetzt, sodass das Pflegepersonal jederzeit unabhängig von einer separaten DECT-Infrastruktur telefonieren oder Alarme auslösen kann."

Bislang wurden in diesem Kontext zwar noch keine Bußgelder verhängt, die Datenschutzkonferenz hat jedoch Ende Januar angekündigt, die Durchsetzung des EuGH-Urteils nun stärker in den Blick zu nehmen.

Fakt ist: Klinik-Verantwortliche, die Cloud-Computing einsetzen, sei es zur Verarbeitung von Klinik- oder Patientendaten oder zur Netzwerkverwaltung, stehen in der Verantwortung für die Compliance. Wer Datenschutzverstöße, Bußgelder und Reputationsverlust vermeiden möchte, muss also genau hinsehen – wie auch die Autoren eines umfangreichen wissenschaftlichen Gutachtens zum Einsatz Cloud-basierter KIS-Lösungen betonen, das im Auftrag des vom Bundesgesundheitsministerium gegründeten health innovation hub erstellt wurde.

Kliniken, die neu investieren, müssen sich intensiv mit den Herstellern befassen. Lösungen von Anbietern aus Deutschland und Europa unterliegen den europäischen Datenschutzstandards und bergen nicht die Gefahr eines möglichen Zugriffs durch Drittstaaten. Deutsche Netzwerkinfrastrukturausstatter sind nicht verpflichtet, sensible Daten in der Netzwerkmanagement-Cloud offenzulegen oder den Zugang zu solchen über verdeckte Zugänge, sogenannte Backdoors, zu ermöglichen. Ein DSGVO-konformer und rechtssicherer Betrieb ist damit zu jeder Zeit gewährleistet. Mit Datenschutz „Made in Germany" werden die hohen Compliance-Vorgaben aus DSGVO und Patientendaten-Schutz-Gesetz auch in Cloud-gemanagten Netzen erfüllt und die Gefahr von Datenschutzverstößen, Bußgeldern und Reputationsrisiken wird minimiert.

Fazit

Die Digitalisierung der Kliniken ist unverzichtbare Aufgabe für die Zukunft des Gesundheitswesens. Mit dem KHZG werden jetzt die Weichen für die Einführung und Modernisierung digitaler Prozesse und Infrastrukturen gestellt. Die Qualität der Gesundheitsfürsorge in Deutschland wird langfristig gesichert und das elementare Recht der Patienten auf Datensouveränität und informationelle Selbstbestimmung verankert. ■

Thorsten Ramm
Healthcare-Experte
LANCOM Systems

Thorsten Ramm