LANCOM Whitepaper

Cloud-gemanagte Netzwerke (SDN) für Behandlung und Pflege auf höchstem Niveau

Seit Oktober 2020 fördern Bund und Länder den Auf- und Ausbau digitaler Infrastrukturen in Kliniken und Krankenhäusern mit rund 4,3 Milliarden Euro. Dies ist eine bis dahin einmalige Chance für den Klinik-sektor. Anwendungen und Prozesse werden heutzutage zunehmend digitalisiert: Mehr und mehr Nutzer, Endgeräte und Dinge (IoT) sind miteinander vernetzt, was auch und gerade im Gesundheitswesen gilt und insbesondere Kliniken und Krankenhäuser betrifft. Bereits heute finden sich in US-amerikanischen Krankenhäusern mehr als 10 vernetzte Geräte in der Peripherie einzelner Krankenbetten. Ein funktionierendes Netzwerk ist daher das Herz jeder Klinik, es aufzubauen und zu steuern eine hochkomplexe Operation. Gleichzeitig mehren sich Berichte verheerender Cyber-Angriffe mit immensen Schäden für die betroffenen Einrichtungen. Hier stoßen traditionell gemanagte Netzwerke schnell an ihre Grenzen. Cloud-gemanagte Netzwerke hingegen sorgen für Automatisierung und höchste Betriebssicherheit. Denn nicht mehr nur die Hardware und eine einmal festgelegte Infrastruktur stehen im Vordergrund. Vielmehr geht es darum, den Istzustand der Netze und Einzelkomponenten stets transparent und den Datenverkehr sicher zu gestalten. Ein Paradigmenwechsel mit erheblichen Chancen, der für die ohnehin unter enormem Kostendruck stehenden Klinikbetreiber interessante Aussichten bietet.

IT – mehr als ein Wettbewerbsfaktor für Klinikbetreiber

IT-Abteilungen in Krankenhäusern stehen unter Druck: Sie müssen den Übergang von schriftlicher zu elektronischer Datenerfassung bewerkstelligen und dabei die Vertraulichkeit sensibler Gesundheits- und Patientendaten gewährleisten. Nicht nur Kliniken mit 30.000 und mehr vollstationären Patienten p. a., also Betreiber sog. Kritischer Infrastrukturen (KRITIS), müssen die gesetzlichen Forderungen zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) erfüllen. Ab dem 01.01.2022 sind alle und somit auch kleinere Kliniken angehalten, ein Informationssicherheitsmanagementsystem aufzubauen. Die erhöhten Sicherheitsanforderungen ergeben sich aus dem Gesetz zum Schutz elektronischer Patientendaten in der Telematikinfrastruktur, kurz Patientendatenschutzgesetz (PDSG), und stellen diese kleineren Häuser in Teilen den KRITIS-Umgebungen gleich. Dabei geht es um nichts Geringeres als den Schutz vor gestohlenen medizinischen Daten sowie die Aufrechterhaltung effizienter klinischer Prozesse und somit möglicherweise sogar um den Schutz des Lebens der Patienten. Beides muss im Sinne der Patienten und gleichermaßen zur Wahrung des Wirtschaftsbetriebes der Kliniken unbedingt gewährleistet sein. So müssen diensthabende Ärzte beispielsweise jederzeit schnellen Zugriff auf Patientenakten haben, wo bisher die Papierakte vielleicht erst vom Schreibtisch eines Kollegen beschafft werden musste. Daher wird auch die permanente Verfügbarkeit des Netzwerkes für mobile Endgeräte wie Laptops und Tablets zur Pflichtaufgabe

und zum kritischen Faktor. Werden Vitalzeichen nicht nur mit stationären Überwachungsgeräten, sondern auch über mobile Endgeräte aufgezeichnet, sind Mediziner und Pflegepersonal in Zukunft mobiler, flexibler und somit effizienter. Das spart Zeit, die den Patienten zugutekommt.

Patientenortung, Asset Management und Klinikkomfort

Der Einsatz einer modernen Netzwerkinfrastruktur in Kliniken eröffnet weitere Anwendungsfelder, die für effiziente Prozesse bis hin zu Vorteilen im Wettbewerb sorgen. So kann eine WLAN-Infrastruktur erweitert werden, um die Basis für hocheffiziente Real-Time Location Services (RTLS) zu schaffen, mittels derer medizintechnische Geräte, Betten oder auch Rollstühle punktgenau geortet werden. Hierdurch entfallen zeitaufwändige Suchen der entsprechenden Assets, Mehrfachanschaffungen entfallen, ihre Auslastung wird gesteigert und Diebstahl wird vermieden.

Ortsbezogene Dienste (Location-based Services, LBS) auf Basis von Bluetooth-Technologie können installiert werden, um demente oder desorientierte Patienten zu orten und zu identifizieren. Hierzu erhält der Patient ein Armband mit integriertem Funkmodul, wodurch er eine angemessene Bewegungsfreiheit und gleichzeitig mehr Sicherheit erlangt.

Über WLAN werden heute und künftig immer mehr Abläufe digital erfasst – Ergebnisse der Morgenvisite, Befunde der Notaufnahme, Asset Tracking, Patienten- und Besucher-Navigation oder individuelle Essenswünsche – fast jeder Handgriff wird digital begleitet.

Zusätzlich steigen die Ansprüche der Patienten an einen möglichst komfortablen Klinikaufenthalt: Sie möchten vom Krankenbett aus mit ihrem mobilen Endgerät sicher im WLAN surfen oder Entertainment-Angebote nutzen.

Cloud-Management hält Schritt mit dem technischen Fortschritt

So erfreulich die Digitalisierung ist, so weitreichend sind die Konsequenzen für das Netzwerk: Die unterschiedlichsten Klinik- und Aufgabenbereiche – medizinische Datenübertragung, Kommunikation, Multimedia-Unterhaltung und Verwaltung – bedürfen einer zuverlässigen Infrastruktur. Immer mehr Geräte benötigen einen stetigen und unterbrechungsfreien Zugriff auf sensible und/oder überlebenswichtige Informationen.

Die Folge: Die Netzwerke müssen immer mehr Daten verarbeiten. Bestehende Netze in Kliniken sind für derartige Anforderungen jedoch oft nicht ausgelegt, denn in der Regel handelt es sich um inflexible Systeme, die nicht schnell und bedarfsgerecht erweiterbar sind und damit das Gegenteil dessen, was ein moderner Krankenhausbetrieb benötigt: Eine flexible Infrastruktur, die nicht durch fest installierte Komponenten limitiert, sondern flexibel und skalierbar ist, sprich sich an verändernde Anforderungen anpassen lässt.

Die veränderten Rahmenbedingungen überlasten traditionelle Netzwerkstrukturen über kurz oder lang und zwingen die Verantwortlichen zum Umdenken. Um der steigenden Komplexität Herr zu werden, müssen Netzwerke „neu“ gedacht und durch flexible Cloud-gemanagte Infrastrukturen ersetzt werden. Eine tragende Rolle spielen dabei die folgenden Fragestellungen: Wie können vernetzte Services wie digitale Behandlungsdokumentation, Patienten-Monitoring oder Ortungslösungen etc. für medizinische Geräte Ärzten und Pflegekräften zur Verfügung gestellt werden? Wie können gleichzeitig IT-Sicherheit und Patientendatensouveränität gewährleistet

werden? Wie tragen moderne Services wie WLAN-Hotspots und Entertainmentsysteme zur Patientenzufriedenheit bei und wie schlagen sich letztlich diese Investitionen und Veränderungen möglichst positiv in den Gesamtbetriebskosten (TCO) nieder? Dieser Brückenschlag gelingt mit Cloud-gemanagten (W)LAN-Konzepten sowie modernen SD-WAN-Lösungen zur Echtzeit-Anbindung verteilter Klinikstandorte, externer Spezialisten und Reha-Zentren.

Die Idee dahinter: Netze werden automatisch aufgesetzt, überwacht und erweitert. Traditionelle digitale Strukturen, die verwaltungsintensiv und statisch sind, werden in dynamische Netze mit flexiblen Erweiterungsoptionen umgewandelt. Dazu werden Funktionsebenen des Netzwerks in Form virtueller Services von der Hardware entkoppelt, die Steuerungsebene also von der Datenebene getrennt. Eine Software-Anwendung steuert den Umgang mit Datenpaketen auf der Datenebene der Hardware – der Router, Firewalls, Switches oder Access Points. Während in traditionellen Architekturen Einstellungsänderungen an vorhandenen Netzwerkgeräten sowie neue Hardware individuell und manuell konfiguriert werden müssen, ermöglicht ein Cloud-Management das zentrale ortsunabhängige Design, Management und Monitoring von Netzen mit wenigen Mausklicks.

Unsicherheit gegenüber der Einführung des Cloud-Managements

Zwar ist die Rechtslage sehr komplex und die Bedenken bzgl. der Sicherheit vor Cyberbedrohungen der Patientendatensicherheit beim Einsatz neuer Technologien, insbesondere Clouddienste sind hoch. Doch können Anbieter von Netzwerkinfrastrukturlösungen hier punkten, Vertrauen schaffen und auf die Vorzüge europäischer Lösungen mit entsprechenden Sicherheitsstandards hinweisen. Insbesondere sei hier auf einen jüngst erschienenen Report der Agentur der Europäischen Union für Cybersicherheit (ENISA) hingewiesen (https://www.enisa.europa.eu/publications/cloud-security-for-healthcare-services/). Dessen Ziel ist es, Cloud-Sicherheitspraktiken für das Gesundheitswesen bereitzustellen sowie Sicherheits- und Datenschutzaspekte herauszuarbeiten, die bei der Beschaffung von Cloud-Diensten für das Gesundheitswesen berücksichtigt werden sollten. Denn – so zeigt das Papier klar auf – Cloud-Lösungen verschaffen Gesundheitsanbietern die notwendige Flexibilität und ermöglichen eine schnelle Bereitstellung neuer Dienste einschließlich Angeboten „virtueller“ Gesundheit und der Telemedizin. Die Studie zeigt typische Anwendungsfälle für Cloudnutzung im klinischen Kontext auf, wie beispielsweise die elektronische Gesundheitsakte, Fernbetreuung und medizinische Geräte und erarbeitet 17 Sicherheits- und Datenschutzmaßnahmen, die die notwendige Cloud-Sicherheit gewährleisten. Ein ebenfalls bei er ENISA erschienenes Online-Tool (https://www.enisa.europa.eu/news/enisa-news/procurement-guidelines-for-cybersecurity-in-hospitals-new-online-tool-for-a-customised-experience) zur Umsetzung der Beschaffungsrichtlinie für Krankenhäuser zielt darauf ab, Beschaffungsverantwortlichen umfassende Informationen an die Hand zu geben, um den Beschaffungsprozess der Krankenhäuser an der Erreichung der gesetzlich geforderten Cybersicherheitsziele auszurichten. Dies führt Kliniken zur Auswahl eines vertrauenswürdigen Cloud-Dienst-Anbieters, mit dem sie angemessene organisatorische und technische Vorkehrungen zur Umsetzung

sämtlicher der Forderungen des Krankenhauszukunftsgesetzes (KHZG), des Gesetzes zum Schutz elektronischer Patientendaten in der Telematikinfrastruktur (PDSG), der EU-Datenschutz-Grundverordnung (DSGVO/GDPR) sowie des IT-Sicherheitsgesetzes treffen. Daher ist es wichtig, im Rahmen dieses Whitepapers auf die Vorzüge europäischer Anbieter und Lösungen mit entsprechenden Standards bei Sicherheit und insbesondere Datenschutzkonformität und Vertrauenswürdigkeit hinzuweisen. An dieser Stelle sei auf einen Leitfaden hingewiesen, der beschreibt, wie Compliance-Risiken in Unternehmensnetzen minimiert werden können. Das Dokument können Sie gerne hier anfordern.

Dies wurde insbesondere auch nochmals durch die Entscheidung des Europäischen Gerichtshofes (EuGH) vom 16. Juli 2020 unterstrichen. Damals kippte das Gericht das Privacy Shield, also die Datenschutz-Absprache zwischen der Europäischen Kommission und den USA. Auf Basis des Privacy Shields waren US-Unternehmen überhaupt nur in der Lage, personenbezogene Daten von EU-Bürgern zu verarbeiten. Die richterliche Entscheidung entzog dieser Praxis quasi über Nacht die rechtliche Grundlage, was einen klaren Sieg für den Schutz personenbezogener Daten von EU-Bürgerinnen und -Bürgern darstellt. Das Urteil zeigt einmal mehr, dass auch Kliniken zum Schutz der Patientendaten auf europäische Anbieter setzen sollten, um nicht in datenschutzrechtliche Schwierigkeiten zu geraten.

Cloud-basiertes Management des Kliniknetzes zahlt sich mehrfach aus

Ein Cloud-gemanagtes Klinik-Netzwerk ist auf lange Sicht wesentlich rentabler und wirtschaftlicher als traditionelle Netzwerke und das bei höherer Leistungsfähigkeit und zugleich geringerem Wartungsaufwand, insbesondere, da Vororteinsätze von Technikern nahezu gänzlich entfallen.

Kliniken profitieren daher von erheblichen Zeit- und Kosteneinsparungen, weil SD-WAN und Cloud-Management den Arbeitsalltag der Netzwerkadministratoren wesentlich erleichtern. Denn die Software übernimmt die Konfiguration und die frei werdenden Ressourcen können für Planung, Überwachung und konzeptionelle Weiterentwicklung der Netzwerke eingesetzt werden. Die gesamte Infrastruktur wird flexibler und kann sehr viel schneller als bisher an sich verändernde Anforderungen angepasst werden. Bandbreiten werden innerhalb von Minuten angepasst, Services online aktiviert oder beendet und der Zustand des gesamten Netzwerkes stets in Echtzeit überwacht. Selbst komplexe Vorgänge wie die Behebung von Störungen oder der Rollout neuer Netzwerkbereiche und Services, die früher mehrere Tage oder Wochen in Anspruch nehmen konnten, sind per Mausklick in Minuten oder zumindest in wenigen Stunden erledigt.

Im Ernstfall: Schnelles Eingreifen und automatische Priorisierung

Netzwerke in Klinikumgebungen müssen ausgesprochen zuverlässig sein, weil von ihrem reibungslosen Funktionieren unter Umständen Leben abhängen können. Kommt es im traditionellen Netzwerk zu einem Ausfall oder einer Störung, kann dies die stationären Abläufe empfindlich beeinträchtigen. Dies verursacht nicht nur Kosten, sondern kann zum ernsthaften Risiko für die Versorgungssicherheit der Patienten werden. Eine Cloud-basierte Infrastruktur bietet maximale Übersicht und Einflussmöglichkeit auf alle im Netzwerk eingesetzten Geräte und Anwendungen. Sie

stellt somit einen wichtigen Baustein für das klinische Informationssicherheitsmanagement dar weil es die Überwachung des aktuellen Zustandes sämtlicher Komponenten wie Router, Firewalls, Switches und Access Points erlaubt. Der IT-Admin erkennt Anomalien, auslaufende Lizenzen, Fehler oder Geräteausfälle sofort und kann darauf unmittelbar reagieren, meist noch bevor dies Auswirkungen auf die Anwender hat.

Individuelle Priorisierung verschiedener Netzwerkanwendungen

Dabei müssen Netzwerke in Zeiten hohen Verkehrsaufkommens nicht nur alle angeschlossenen Geräte unterstützen. Sie müssen auch unterscheiden können, ob eine Patientenakte für einen Routine-Checkup eingesehen oder auf der Intensivstation bzw. Notaufnahme benötigt wird und die Vorgänge entsprechend ihrer Dringlichkeit priorisieren. An erster Stelle stehen die kritischen Vorgänge und Geräte. IT-Administratoren können den Netzwerkverkehr für dringliche und somit zeitkritische Applikationen priorisieren und die Geschwindigkeit von Übertragungen gleichzeitig stattfindender Transfers weniger dringlicherer Anwendungen bremsen oder verhindern. Backoffice-Applikationen oder Anwendungen der Verwaltung müssen im Zweifel beispielsweise in der Bandbreite gegenüber zeitkritischen Transfers medizinisch relevanter Daten eingeschränkt werden.

Die Versprechen Cloud-gemanagter Kliniknetzwerke

Aufbau, Rollout und Management klinischer Netzwerke in Kombination mit modernster Cloud-Technologie sind wesentliche Treiber der digitalen Transformation. Mithilfe von Cloud-Technologien können alle Funktionen für Konfiguration, Management und Monitoring einfach, zentral und ortsunabhängig per Laptop, Tablet oder Smartphone ausgeführt werden. Ob Highspeed-Internetzugang, modernste Vernetzung der Klinikstandorte via SD-WAN, die Einrichtung von WLAN-Profilen, Priorisieren zeitkritischen Datenverkehrs oder die Integration neuer Geräte wie Router, Firewalls, Switches oder Access Points – eine moderne Cloud-Lösung passt sich den Bedürfnissen einer Klinik, egal welcher Größe, an. Die Investitionen bleiben überschaubar und der Aufwand ist monatlich kalkulierbar.

IT- und Investitionssicherheit inklusive – made in Germany

Werden Netze aus einer Public Cloud verwaltet, sind Vertrauen, Sicherheit und Datenschutz wesentliche Rahmenbedingungen. Deshalb ist die Wahl eines Anbieters, der mindestens europäischem oder besser noch deutschem Datenschutzrecht unterliegt und seine Dienste in hiesigen Rechenzentren gemäß DSGVO hostet, für Kliniken und Krankenhausbetriebe alternativlos.

Sichere Investition in die Zukunft

Ebenfalls sollte auch das Thema Investitionssicherheit bedacht werden! Viele Netzwerkhersteller setzen für ihre Cloud-gemanagten Netzwerklösungen spezielle Router oder Access Points ein. Sie können ausschließlich über die Cloud betrieben werden und sind teilweise fest an einzelne Netze oder Standorte gebunden. Ein „Ausbuchen“ aus

dem Cloud-Management mit dem Ziel, die Hardware traditionell, sprich als stand-alone Lösung zu verwalten oder eine Verschiebung von einem Standort zu einem anderen sind technisch oft gar nicht möglich. Dies schränkt die Flexibilität der Anwender deutlich ein und sorgt im Falle von Veränderungen für zusätzliche ungeplante Ausgaben. Optimalen Investitionsschutz bieten daher Netzwerk-Komponenten, die sowohl autark oder über die Cloud betrieben werden können und jederzeit eine Anpassung an geänderte betriebliche Erfordernisse ermöglichen.

Kliniknetzwerk-as-a-Service via Managed Service Provider

Gerade für kleine und mittelgroße Kliniken können die in einer Public-Cloud gehosteten Netzwerke, die durch einen auf das Gesundheitswesen spezialisierten Service-Provider (Managed Service Provider, MSP) zur Verfügung gestellt und verwaltet werden, besonders interessant und wirtschaftlich sein. Sie können nach dem Prinzip „pay as you grow“ flexibel und bedarfsgerecht gebucht werden. Bezahlt wird dabei nur die Leistung, die gebucht wurde (“pay what you get“). Kommen neue Anwender und Geräte hinzu, werden sie über das zentrale Administrations-Dashboard definiert und innerhalb weniger Minuten an das vorhandene Netz angebunden.

Private-Cloud-Ansatz für hohe Sicherheitsanforderungen

Für Kliniken, die aufgrund ihrer Größe als Betreiber Kritischer Infrastrukturen (KRITIS) mit erweiterten Sicherheitsbedürfnissen gelten, sind Self-Hosting-Modelle interessant, die den Betrieb der Management-Cloud im eigenen Rechenzentrum ermöglichen. Ebenfalls ist das Hosting des Systems auf einer eigenen dedizierten Hardware, einer sogenannten Private Appliance, möglich. Dies erlaubt den Betrieb eines Cloud-basierten Management-Systems „on premises“, ohne eine mit anderen Mandanten geteilte Infrastruktur.

Fazit: Innovation schafft Versorgungssicherheit

Klinikbetreiber stehen aufgrund der gestiegenen Anforderungen in den zuvor genannten Bereichen enorm unter Druck. Dieser geht unmittelbar auf ihre IT-Abteilungen über, denn sie sollen zum Wegbereiter einer umfassenden Digitalstrategie werden, die medizinische Ausrüstung, IT-Technologie und Datenvernetzung umfasst. Das Netzwerk spielt dabei eine Schlüsselrolle. Cloud-Management ist die Zukunft des Netzwerkmanagements und gibt Kliniken wesentlich mehr Flexibilität für künftige Digitalisierungsschritte und -initiativen, mit denen sie den Weg für ein zukunftsfähiges Krankenhaus erfolgreich beschreiten.