KTM Krankenhaus TECHNIK+MANAGEMENT
Auszug aus Juni 2021

Digitalisierung in Kliniken: Was die Basis-Infrastruktur können muss

Checkliste für die Digitalisierung

In deutschen Kliniken nimmt sie, befördert durch das Krankenhauszukunftsgesetz (KHZG), immer mehr Fahrt auf: die Digitalisierung. Gleichzeitig müssen vor allem kleinere Kliniken vor dem Hintergrund des Patientendaten-Schutz-Gesetzes (PDSG) künftig striktere Anforderungen an Informationssicherheit und Datenschutz erfüllen. Was müssen Kliniken dabei beachten?

Bund und Länder legen mit dem Krankenhauszukunftsgesetz (KHZG) und den damit verbundenen Fördermilliarden den Grundstein für eine nie gekannte Digitalisierungsoffensive im deutschen Gesundheitswesen. Und auch die Informations- sowie die Versorgungssicherheit und der Datenschutz stehen im Fokus wie nie. Das alles hat direkte Auswirkungen auf die klinische Netzwerkinfrastruktur, die die Basis für nahezu alle digitalisierten Prozesse in der stationären Pflege bildet. Eine Checkliste zeigt, worauf Klinikleitungen bei der Beschaffung von WLAN & Co., beim Netzwerkbetrieb (Stichwort: Cloud) und bei Cybersecurity-Lösungen achten müssen, um Compliance-Vorgaben und Fördervoraussetzungen zu erfüllen und einen reibungslosen Betrieb zu gewährleisten.

Eine professionelle WLAN-Infrastruktur ist die Grundlage einer lückenlosen digitalen Behandlungsdokumentation: Per Tablet und WLAN greifen Ärzte von überall sicher auf Befunde im KIS, PACS oder RIS zu und erfassen Untersuchungsergebnisse direkt digital am Patientenbett.

WLAN: Basis für alle mobilen und drahtlosen Klinikprozesse

Eine professionelle Ausleuchtung ist der erste Schritt zu einem flächendeckenden, hochverfügbaren WLAN (Wireless Local Area Network) mit ausreichend Bandbreite. Die Königsdisziplin ist die Ausleuchtung vor Ort (On-Site WLAN Survey), mit der sowohl Anzahl als auch Montageorte der WLAN-Access-Points sehr akkurat bestimmt und Zonen mit unzureichender Abdeckung oder Interferenzen durch Überlappung vermieden werden können. Die Alternative ist eine virtuelle Ausleuchtung (Off-Site) auf Basis von Grundrissen und Angaben zur Gebäudebeschaffung. Bei beiden Verfahren müssen die gewünschten Dienste – WLAN, Voice-over-WLAN oder Location-based Services (LBS, RTLS) – und die geschätzte Anzahl der WLAN-Nutzer mit in die Planung einbezogen werden. Daraus ergeben sich die benötigten Netzwerkports, Verkabelungsarbeiten und LAN-Switches.

Sodann werden die Anforderungen an die WLAN-Hardware definiert, mit einem K.-o.-Kriterium ganz zu Beginn: Access-Points, die im medizinischen Umfeld eingesetzt werden sollen, müssen die europäische Norm EN 60601-1-2 in Bezug auf Störfestigkeit und elektromagnetische Verträglichkeit erfüllen. Erst danach können im Auswahlprozess weitere technische Ausstattungsmerkmale herangezogen werden. Dabei gehören neben der Leistungsfähigkeit

vor allem Sicherheitsmerkmale auf die Checkliste, wie zum Beispiel Virtualisierungsfunktionen. Access-Points mit VLAN-Unterstützung (Virtual Local Area Network) ermöglichen den sicheren Betrieb mehrerer logisch voneinander getrennter Netze über eine einzige Geräteinfrastruktur. Typischerweise sind dies das medizinische Netz, das Verwaltungsnetz und der Internetzugang für die Patienten. Um die hohen Compliance-Vorgaben der DSGVO und des KHZG zu erfüllen, müssen ausnahmslos alle Geräte Sicherheit gemäß Stand der Technik bieten.
Konkret heißt das: Moderne Verschlüsselungsstandards wie WPA3 Enterprise (mit Zertifikaten) und eine Authentisierung der WLAN-Clients durch NAC-Systeme (Network Access Control) sind Pflicht. Je nach Systemumgebung kommen Validierungen für den Einsatz mit Patientenmonitoring-Lösungen (Dräger, Philips etc.), Alarmierung oder WLAN-Telefonie (Ascom, Spectralink o. Ä.) hinzu. In diesem Zusammenhang sind auch QoS-Funktionen (Quality of Service) elementar, über die wichtige Datenströme priorisiert werden. Damit das WLAN zukunftssicher ist und die nötigen Bandbreiten liefert, sollten Kliniken auf WiFi-6-Geräte (IEEE 802.11ax) setzen. Dieser Standard verbindet effiziente Energiesparmechanismen für Endgeräte (WLAN-Telefone, Pager etc.) mit der Fähigkeit, sehr viele Clients gleichzeitig zu versorgen (High Density). Hardwareseitig sollten die Access-Points Power over Ethernet (PoE) unterstützen, sodass die Energieversorgung über die Switches erfolgt und keine zusätzlichen Steckdosen benötigt werden. Kliniken, die Ortungsdienste nutzen möchten, benötigen Access-Points mit Bluetooth-Unterstützung. Dies ermöglicht eine einfache Erweiterung um Echtzeitdienste wie Location Based Services (LBS) oder Real Time Locating Systems (RTLS) (Hipross, Blukii o. Ä.).

LAN: Rückgrat für eine leistungsstarke Vernetzung

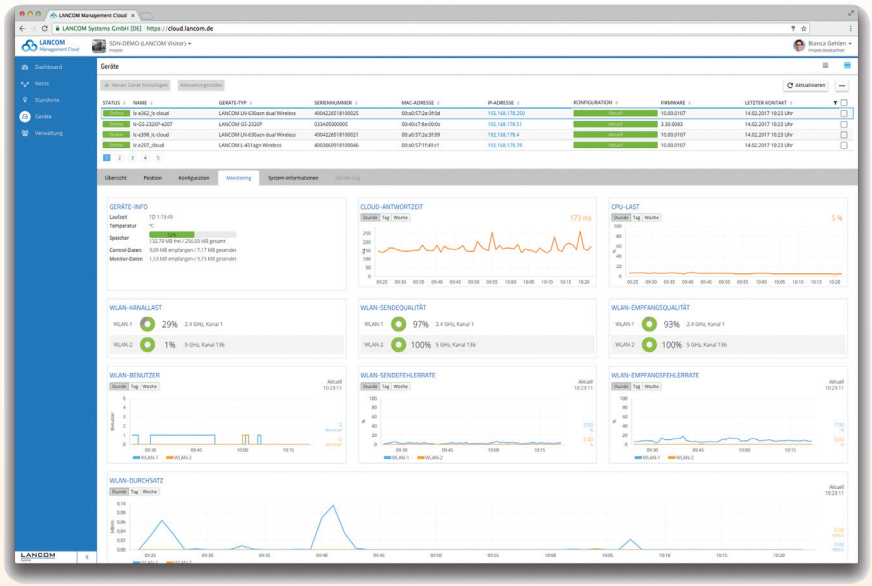
Den zweiten großen Infrastrukturblock in Kliniken bildet das LAN. Nur mit hochwertiger Verkabelung (Kupfer, Glasfaser), ausreichend Netzwerkports und sicheren, leistungsstarken Switches wird es den Anforderungen des Klinikalltags gerecht. Switch-Infrastrukturen sind meist über mehrere Ebenen organisiert. ‚Normale Nutzer' wie PCs, stationäre Medizingeräte oder WLAN-Access-Points werden an Access-Switches angeschlossen. Diese werden über die erste Ebene der Aggregation-Switches gebündelt, die wiederum in einer oder mehreren weiteren Aggregationsebenen untereinander bis zur Core-Ebene (Rechenzentrum) vernetzt sind. Daraus leiten sich zentrale Anforderungen ab. Um eine ausreichende Anzahl an Ports zur Verfügung zu stellen und/oder die Ausfallsicherheit zu gewährleisten, sollten sich mehrere Switches auf gleicher Ebene zu einem virtuellen Gerät verbinden lassen (Stacking). Entscheidend ist die interne Datendurchsatzrate der Geräte (Backplane-Durchsatz), die nicht zum Flaschenhals im Netzwerk werden darf. ‚Non-Blocking-Backplane Stacking' ist daher zwingende Voraussetzung für Aggregation-Switches.
Hardwareseitig müssen die Switches in der Lage sein, WLAN-Access-Points über PoE mit Strom zu versorgen, um aufwändige Erweiterungsarbeiten am Stromnetz zu vermeiden. Die Switch-Ports selbst sollten mindestens 2,5 (besser 5) GBit/s Datendurchsatz unterstützen, um die volle Bandbreite moderner WiFi-6-Access-Points ausschöpfen zu können. Nicht genutzte Ports sollten sich per IEEE 803.az deaktivieren lassen, um Energie zu sparen.
Aufgrund der hohen Anforderungen an Sicherheit und Konfiguration sollten in Kliniknetzen ausschließlich Fully-managed Switches zum Einsatz kommen. Ebenso auf die Checkliste gehören VLAN-Unterstützung, portbasierte Sicherheit nach 802.1x und Access-Control-Listen – möglichst mit Anbindung an NAC-Systeme. In größeren LANs sollten die Aggregation-Switches Funktionen bieten, die die Router entlasten. DHCP-Server-Funktionalität sowie statisches oder dynamisches Routing per RIP, OSPF oder BGP über ein oder mehrere Netzwerksegmente hinweg steigern die Effizienz des gesamten Netzwerks.

Eine professionelle Ausleuchtung ist der erste Schritt zu einem flächendeckenden, hochverfügbaren WLAN: Sowohl Anzahl als auch Montageorte der WLAN-Access-Points müssen sehr akkurat bestimmt sein.

Bilder: Lancom Systems

WAN: Kritische Schnittstelle zum Internet

Ob Vernetzung von Klinikverbünden, telemedizinische Anwendungen oder einfach der Zugang zum Netz: WAN-Router und -Gateways bilden



Ein gut funktionierendes Netzwerk aufzubauen und zu managen, ist eine hochkomplexe Angelegenheit. Managementsysteme, die die gesamte Netzwerkarchitektur (WAN, LAN, WLAN etc.) organisieren, optimieren und steuern, können hier helfen.

die neuralgische Schnittstelle zwischen dem lokalen internen Netz (LAN) und dem Internet. Zusammen mit Firewalls sichern sie Kliniknetze gegen Angriffe von außen ab, ermöglichen aber dennoch den Zugriff auf das Internet und verknüpfen verschiedene Standorte und Dienstleister sicher miteinander. Daraus ergibt sich eine Vielzahl an Sicherheits- und Performanceanforderungen, die auf die Checkliste eines jeden IT-Verantwortlichen gehören. Router mit mehreren, auch unterschiedlichen WAN-Schnittstellen (xDSL, Glasfaser, Mobilfunk, Ethernet für Provider-Modems) geben Kliniken die Möglichkeit, mehrere Anschlüsse für höhere Bandbreiten zu bündeln oder – im Falle einer Störung – durch intelligente Back-up-Mechanismen nahtlos auf eine andere Leitung oder LTE/5G umzuschalten. Sie sorgen so für höchste Verfügbarkeit. Ein zusätzliches Plus beim Durchsatz bringen dynamische Routingprotokolle wie RIP, BGP, OSPF oder LISP sowie Dynamic Path Selection in Verbindung mit applicationbased Routing.

Im Interesse der Informationssicherheit muss darauf geachtet werden, dass der Router einerseits eine integrierte Firewall besitzt, vor allem aber auch die Möglichkeit bietet, verschiedene IP-Kontexte mit eigenen Firewallregeln und VLANs zu konfigurieren. Darüber kann ein einzelnes Gerät mehrere sicher voneinander getrennte, virtuelle Router mit beliebig vielen Netzsegmenten zur Verfügung stellen. Ein möglicherweise infizierter Computer kann so nicht das gesamte Netzwerk kompromittieren. Ein deutliches Sicherheitsplus verspricht zudem ein integrierter Session Border Controller (SBC), der bei IP-Telefonie (VoIP) eine Trennung des (unsicheren) externen Netzes vom (sicheren) internen Netz gewährleistet. Anders als eine Firewall ist er in der Lage, an der Netzwerkgrenze Echtzeit-SIP-Kommunikation im Bereich der Signalisierungsdaten (Control Plane) sowie der Sprach- und Mediadaten (Data Plane) zu untersuchen und zu steuern.

Sollen mehrere Standorte miteinander vernetzt oder externe Gesundheitspartner und Dienstleister in das Kliniknetz eingebunden werden, geschieht dies am wirtschaftlichsten über virtuelle private Netzwerke (VPN). Je nach Leistungsfähigkeit des im Router integrierten VPN-Gateways können tausende verschlüsselte VPN-Tunnel aufgebaut werden, die die Authentizität, Integrität und Vertraulichkeit der übermittelten Daten sicherstellen. So können Befunde, Röntgen- und CT-Bilder sowie andere Gesundheitsinformationen standortübergreifend sicher ausgetauscht, Zweitmeinungen eingeholt und telemedizinische Dienste angeboten werden. Ebenso werden in der Notfallmedizin dank verschlüsselter Kommunikation bereits am Unfallort per Ferndiagnostik durch Fachärzte richtige Entscheidungen getroffen – und somit möglicherweise Leben gerettet.

Firewall und UTM: Schutz gegen Cyber-Angriffe

Optimalen Schutz klinischer Netze vor Angriffen von außen bieten hochmoderne Firewall-Lösungen, die mit einer Kombination aus Unified Threat Management (UTM), Machine Learning und Sandboxing auch neuartige oder bis dato unbekannte Viren und Malware (Zero-Day-Exploits) neutralisieren. Mit zunehmender Verschlüsselung des Datenverkehrs ist es darüber hinaus wichtig, dass die Firewalls SSL-Inspection unterstützen und dadurch auch bei verschlüsselten Datenpaketen Scans, Filterung und Anwendungserkennung durchführen und Sicherheitsvorgaben erfolgreich umsetzen können. Schutz vor komplexen APT-Cyberangriffen (Advanced Persistent Threat) wiederum bietet eine integrierte Deep Packet Inspection (DPI), die eine präzise Klassifizierung des Netzwerkverkehrs, der eingesetzten Protokolle und Anwendungen sowie Schutz vor Datenlecks (Data Loss Prevention) ermöglicht. Contentfilter bieten zusätzliche Sicherheit.

Netzwerkmanagement: Cloud und Datenschutz

Firewalls können wahlweise als Hardware Appliance oder virtuelle Maschine im Rechenzentrum betrieben werden. Das BSI empfiehlt im IT-Grundschutzhandbuch den Einsatz zweier getrennter Firewalls in Bereichen mit erhöhtem Schutzbedarf, wozu Kliniknetzwerke zweifelsfrei zählen. Dies kann auch über den kombinierten Betrieb eines Routers/Gateways mit integrierter Firewall und einer dedizierten Firewall erreicht werden. Für maximale Transparenz hinsichtlich der Umsetzung der Sicher-

heits- und Compliance-Vorgaben empfiehlt sich eine grafische Managementkonsole.
Neben klassischen Gerätemerkmalen gehört auch das Netzwerkmanagement auf die Checkliste der IT-Beschaffer. Aufgrund der hohen Komplexität klinischer Netze, der enormen Anzahl aktiver Komponenten und der strikten Anforderungen an Informationssicherheit und Versorgungssicherheit gemäß KHZG und PDSG stößt traditionelles Netzwerkmanagement mit seinen vielen manuellen Vorgängen und Fehlerquellen schnell an seine Grenzen. Stattdessen spielt eine cloudbasierte Netzwerkverwaltung auf Basis von softwaredefined Networking (SDN) hier ihre vollen Stärken aus. Sie sorgt für die nötige Transparenz, Stabilität und Automatisierung und kann Betriebskosten nachhaltig senken.
Allerdings muss die Netzwerk-Hardware (Router, Switches, Access-Points) das Management per SDN unterstützen, im Idealfall sogar beide Optionen (traditionell und Cloud) bieten. Zudem müssen die Anforderungen der DSGVO erfüllt sein, da beim Cloudmanagement personenbezogene Daten verarbeitet werden.
Auf der sicheren Seite sind Kliniken entweder mit Lösungen europäischer Anbieter oder mit Managementsystemen, die sich ‚On Premise' nutzen lassen – was jedoch eher für größere Häuser oder Klinikverbünde in Frage kommen dürfte. Keine rechtliche Basis gibt es für die meisten Cloudsysteme von Anbietern aus unsicheren Drittstaaten, wozu nach dem Aus des EU-US-Privacy-Shields durch das EuGH-Urteil vom Juli 2020 auch die USA zählen. Hier drohen im Zweifel hohe Bußgelder.
Kliniken und Krankenhäuser, die ihre Prozesse nachhaltig, rechtssicher und mit Hilfe der Fördermittel aus dem KHZG digitalisieren möchten, haben beim Auf- und Ausbau ihrer Netzwerkinfrastruktur also einiges zu beachten. Die lange Checkliste im Bereich Hardware, Software, Netzwerkbetrieb und Datenschutz wird abgerundet durch Fragestellungen zu Garantie, Service und Lifecycle-Management – und hier insbesondere zu Update-Garantien im Fall von Sicherheitslücken. Es lohnt sich, bei geplanten Investitionen und Ausschreibungen genau hinzusehen und im Zweifel Expertenrat einzuholen.

Thorsten Ramm

Digitalisierung vereinfacht Abläufe und schafft Transparenz: So kann etwa dank automatischem Abgleich mit der jeweiligen Datenbank die Belegung von Krankenhauszimmern auf digitalen Schildern immer aktuell angezeigt werden.

Kontakt

Lancom Systems GmbH
Adenauerstraße 20/B2
52146 Würselen
Tel.: +49 2405 49936-0
info@lancom.de
www.lancom.de