Warum IT-Sicherheit immer wichtiger wird und wie Cyberversicherungen helfen können

Mehr Bedrohung, mehr Schutzbedarf

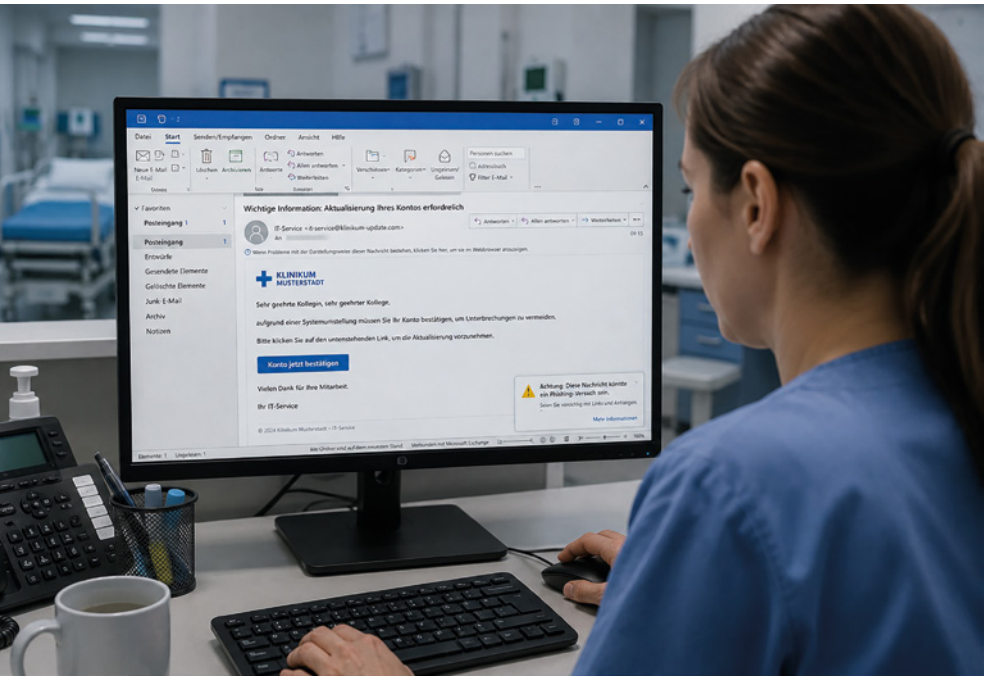
Cyberangriffe gehören inzwischen zu den größten Risiken für Unternehmen in Deutschland. Was früher vor allem große Konzerne betraf, wirkt sich zunehmend auch auf kleine und mittelständische Unternehmen sowie öffentliche Einrichtungen aus. KMU und Krankenhäusern fehlt oft die personelle und technische Infrastruktur, um schnell und professionell zu reagieren. Bei Krankenhäusern können Cybervorfälle darüber hinaus im Ernstfall Menschenleben gefährden, zu hohen finanziellen Einbußen führen und der Reputation schaden. Cyberversicherungen können die Schäden im Falle von Hackerangriffen abfedern.

Im Zuge der Digitalisierung sind Krankenhäuser effizienter geworden. Elektronische Patientenakten, digitale Bildgebung, Telemedizin und vernetzte Medizintechnik ermöglichen moderne Versorgungskonzepte. Damit steigt jedoch auch die Abhängigkeit von funktionierenden IT-Systemen.

Der jüngste Cyberangriff auf den externen Abrechnungsdienstleister Unimed zeigt außerdem, dass zugleich die digitalen Bedrohungen zunehmen. Laut Unimed konnte der Angriff nach kurzer Zeit abgewehrt werden, trotzdem gelangten personenbezogene Daten von Zehntausenden Patienten in die Hände von Cyberkriminellen. Betroffen waren unter anderem Abrechnungsinformationen, Stammdaten und in einzelnen Fällen auch sensible Gesundheitsdaten.
Für Krankenhäuser hat diese Entwicklung weitreichende Konsequenzen. Denn Cyberangriffe gefährden heute nicht nur wirtschaftliche Interessen oder den Datenschutz, sondern können im Ernstfall Auswirkungen auf die Patientenversorgung haben.

Krankenhäuser als gefragte Ziele

Cyberkriminalität zählt inzwischen zu den größten Geschäftsrisiken in allen Branchen. Das Gesundheitswesen nimmt dabei jedoch eine besondere Rolle ein. Krankenhäuser verarbeiten hochsensible Gesundheitsdaten und personenbezogene Informationen, sind rund um die Uhr auf funktionierende IT-Prozesse angewiesen und arbeiten mit einer Vielzahl externer Dienstleister zusammen. Diese Kombination macht sie zu attraktiven Zielen.
Während große Kliniken häufig über spezialisierte IT-Abteilungen verfügen, stehen viele kleinere und mittlere Krankenhäuser vor erheblichen Herausforderungen. Personalmangel, begrenzte IT-Budgets und historisch gewachsene Systemlandschaften erschweren die Umsetzung moderner Sicherheitskonzepte. Gleichzeitig steigt die Professionalität der Angreifer kontinuierlich.
Als besonders problematisch stellt sich dabei heraus, dass Cyberangriffe heute selten isolierte IT-Ereignisse sind. Sie betreffen oft mehrere Organisationen gleichzeitig – beispielsweise über Softwarelieferanten, Managed-Service-Provider oder spezialisierte Dienstleister wie Abrechnungsunternehmen. Der Unimed-Vorfall macht deutlich, dass Krankenhäuser ihre Sicherheitsstrategie deshalb auf die gesamte digitale Wertschöpfungskette ausweiten sollten.



Krankenhäuser verarbeiten hochsensible Daten. Das macht sie zum attraktiven Ziel für Cyberkriminelle. Über Phishing-Mails versuchen Hacker, Mitarbeiter zur Preisgabe sensibler Informationen zu bewegen.

Bilder: ProFina (KI-generiert)

Ransomware bleibt größte Bedrohung

Nach wie vor zählen Ransomware-Angriffe zu den am häufigsten genutzten Methoden von Cyberkriminellen. Dabei verschlüsseln die Angreifer geschäftskritische Systeme und verlangen Lösegeld für deren Freigabe. Im klinischen Umfeld können dadurch beispielsweise Informationssysteme, Bildarchivierung, Laboranwendungen oder Terminmanagement ausfallen – mit weitreichenden Folgen: Operationen müssen verschoben und Notfallpatienten umgeleitet werden. Außerdem kann der finanzielle Schaden erheblich sein.

Daneben gewinnen klassische Malware-Angriffe weiter an Bedeutung. Schadprogramme wie Trojaner, Spyware oder Keylogger werden dazu genutzt, Systeme auszuspionieren, Daten abzugreifen oder unbemerkt Zugriff auf Unternehmensnetzwerke zu erhalten. Über Phishing versuchen Hacker, Mitarbeiter durch täuschend echte E-Mails, SMS oder Anrufe zur Preisgabe sensibler Informationen wie Passwörter oder Zugangsdaten zu bewegen. Auch gefälschte Rechnungen oder manipulierte Zahlungsaufforderungen gehören dazu. Diese Form des Angriffs ist besonders häufig, weil sie gezielt menschliche Fehler ausnutzt. Gerade bei hohem Arbeitsdruck und zahlreichen digitalen Kommunikationswegen ist die Gefahr groß.

Die wirtschaftlichen Folgen solcher Angriffe gehen dabei weit über den eigentlichen IT-Schaden hinaus. Wenn keine Patienten behandelt werden, keine Operationen stattfinden können oder keine Diagnostik möglich ist, entstehen innerhalb kürzester Zeit erhebliche wirtschaftliche Schäden. Noch schwerer wiegt jedoch der Vertrauensverlust bei Patienten, Partnern und Mitarbeitern, wenn sensible Daten kompromittiert werden.

Kontinuierliches Risikomanagement entscheidend

Ziel ist deshalb nicht allein der Schutz von Daten, sondern die Sicherstellung der medizinischen Handlungsfähigkeit. Moderne Sicherheitsstrategien setzen daher auf einen ganzheitlichen Ansatz aus Prävention, Detektion, Reaktion und Wiederherstellung.

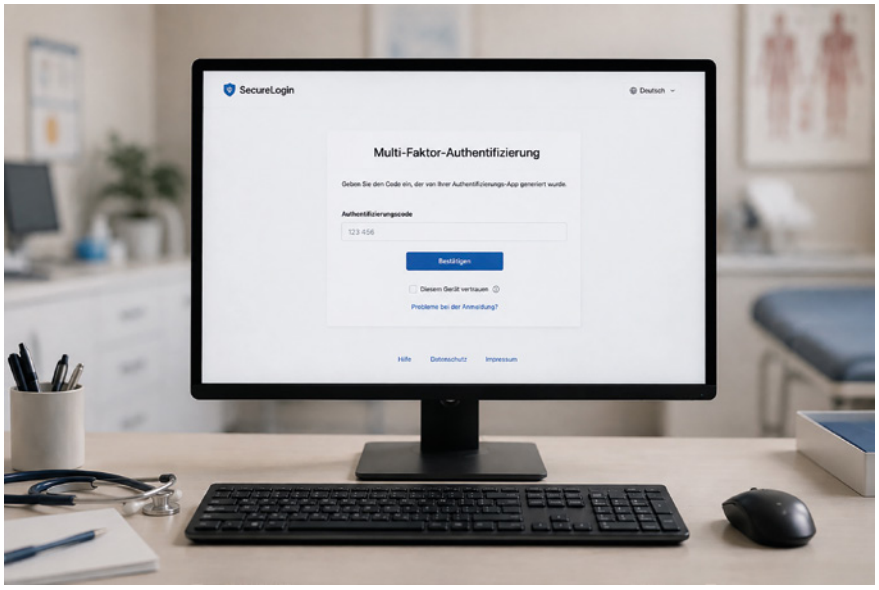
Moderne Sicherheitsstrategien setzen auf einen ganzheitlichen Ansatz aus Prävention, Detektion, Reaktion und Wiederherstellung.

Dazu gehören unter anderem konsequente Netzwerksegmentierung, Multi-Faktor-Authentifizierung, regelmäßige Sicherheitsupdates, kontinuierliches Schwachstellenmanagement und die Trennung kritischer Systeme von administrativen Netzwerken. Ebenso wichtig sind aktuelle Datensicherungen, getestete Notfallpläne und regelmäßige Krisenübungen. Nur wenn technische Maßnahmen mit klar definierten Prozessen kombiniert werden, lassen sich Ausfallzeiten im Ernstfall wirksam begrenzen.

Zudem sollten Informationssicherheitsstandards, Zertifizierungen, vertragliche Sicherheitsanforderungen und Notfallprozesse von externen Partnern überprüft werden. Regelmäßige Audits und ein kontinuierliches Risikomanagement helfen dabei, Schwachstellen frühzeitig zu erkennen.

Versicherungen ergänzen ganzheitliches Sicherheitskonzept

Trotz umfangreicher Schutzmaßnahmen lässt sich ein Restrisiko niemals vollständig ausschließen. Deshalb gewinnen Cyberversicherungen auch im Gesundheitswesen an Bedeutung. Sie dienen jedoch längst nicht mehr ausschließlich der finanziellen Entschädigung. Viele Versicherer stellen im Ernstfall spezialisierte Incident-Response-Teams bereit, koordinieren IT-Forensiker, unterstützen bei



Moderne Sicherheitsstrategien wie Multi-Faktor-Authentifizierung, Netzwerksegmentierung, Sicherheitsupdates, Schwachstellenmanagement und die Trennung kritischer Systeme sollten zur IT-Sicherheit gehören.

der Wiederherstellung kompromittierter Systeme und begleiten die Kommunikation mit Datenschutzbehörden. Darüber hinaus übernehmen sie – je nach Vertrag – Kosten für Datenrettung, Betriebsunterbrechungen und juristische Beratung.

Gerade Krankenhäuser profitieren von dieser schnellen externen Unterstützung. Da jede Stunde Systemausfall Auswirkungen auf den Klinikbetrieb haben kann, entscheidet die Reaktionsgeschwindigkeit häufig über das tatsächliche Schadensausmaß. Cyberversicherungen ersetzen dabei allerdings keine wirksame Informationssicherheit. Vielmehr ergänzen sie ein ganzheitliches Sicherheitskonzept und setzen häufig selbst ein bestimmtes Sicherheitsniveau für den Versicherungsschutz voraus.

Cyberresilienz als strategische Managementaufgabe

Cyberangriffe werden das Gesundheitswesen auch künftig begleiten. IT-Sicherheit ist heute deshalb eine Grundvoraussetzung für einen funktionierenden Krankenhausbetrieb und den Schutz sensibler Patientendaten. Für Klinikleitungen bedeutet das, Cyberresilienz als strategische Managementaufgabe zu verstehen. Technische Schutzmaßnahmen, qualifizierte Mitarbeiter, belastbare Notfallprozesse, ein professionelles Lieferantenmanagement und als ergänzender Baustein eine leistungsfähige Cyberversicherung bilden gemeinsam die Grundlage, um den wachsenden Bedrohungen wirksam zu begegnen.

Denn Cyberangriffe können das Vertrauen von Patienten, Partnern und der Öffentlichkeit nachhaltig beschädigen. Angesichts zunehmender Professionalisierung der Täter und wachsender Abhängigkeit von digitalen Prozessen muss die IT-Sicherheit immer stärker in den Fokus rücken.

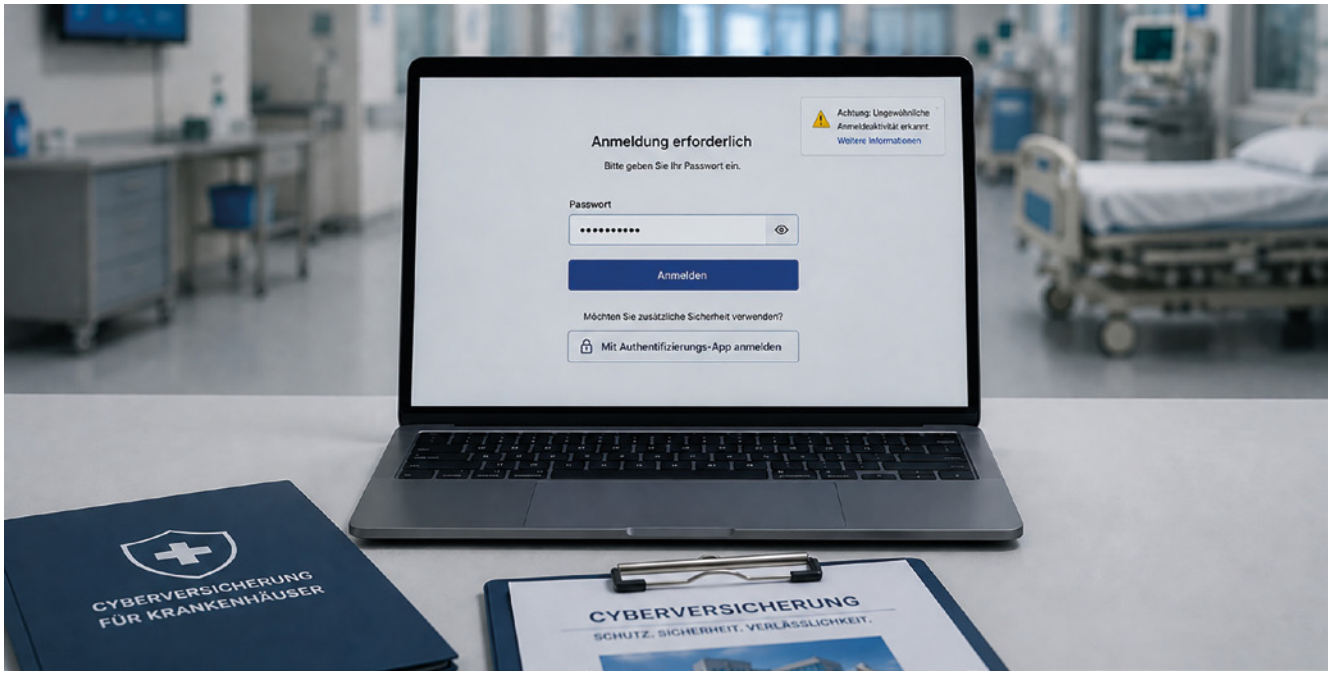
Autor:

Sejdin Sejdini, Geschäftsführer der ProFina Deutschland GmbH

Bild: ProFina Deutschland

Kontakt:

ProFina Deutschland GmbH
Sejdin Sejdini
Castroper Straße 270–280
44791 Bochum
Tel.: +49 234 367106-40
info@pro-fina.de
www.pro-fina.de



Mehr als finanzielle Entschädigung: Viele Anbieter von Cyberversicherungen stellen im Ernstfall spezialisierte Incident-Response-Teams bereit, koordinieren IT-Forensiker, unterstützen bei der Wiederherstellung und begleiten die Kommunikation mit Datenschutzbehörden.

Bilder: ProFina (KI-generiert)

Warum Telemedizin zur neuen Versorgungsstruktur der Krankenhausreform gehören muss

Spezialisierung braucht Vernetzung

Die Krankenhauslandschaft steht vor einem grundlegenden Umbau. Spezialisierung, knappe personelle Ressourcen und wirtschaftlicher Druck verändern die Versorgung. Doch Konzentration allein schafft noch keine zukunftsfähigen Strukturen. Die Deutsche Gesellschaft für Telemedizin fordert deshalb, telemedizinisch unterstützte Versorgung konsequent in die anstehenden Strukturreformen mit einzubeziehen. Wie das konkret aussehen kann, zeigt das Hospital of the Future vom 16. bis 19. November auf der Medica in Düsseldorf.

Krankenhäuser können aufgrund von Fachkräftemangel und zunehmender Spezialisierung durch die Krankenhausreform nicht mehr sämtliche Leistungen an jedem Standort vorhalten. Doch die Konzentration von Leistungen kann zugleich zu längeren Wegen und fragmentierter Versorgung führen. Genau hier liegen zentrale Potenziale der Telemedizin. Denn damit muss spezialisierte medizinische Kompetenz nicht an jedem Ort physisch vorgehalten werden, um für die Versorgung verfügbar zu sein:

- Professionelle telemedizinische Versorgungsnetzwerke können Häuser der Grund- und Regelversorgung mit Maximal- und Supramaximalversorgern verbinden.
- Durch telekonsiliarische Mitbehandlung kann spezialisierte Expertise standortübergreifend eingebunden werden.
- Telemonitoring begleitet Versorgung über den einzelnen Arztkontakt hinaus.
- Eine digitale Ersteinschätzung kann Patienten gezielter in passende Versorgungsangebote steuern.

Aus Sicht der Deutschen Gesellschaft für Telemedizin (DGTelemed) e. V. braucht es deshalb einen Paradigmenwechsel – weg vom sektoralen Einzelkämpfer hin zu vernetzter, interdisziplinärer und standortübergreifender Zusammenarbeit. Für Krankenhäuser ist das nicht nur eine medizinische, sondern auch eine strategische und wirtschaftliche Frage.

Digitale Vernetzung für effizienteren Ressourceneinsatz

Ihr ökonomisches Potenzial entfaltet Telemedizin vor allem dort, wo sie Versorgungsprozesse sinnvoll weiterentwickelt und vorhandene Ressourcen gezielter und effektiver nutzbar macht. Kann etwa spezialisierte Expertise telemedizinisch eingebunden werden, ohne sie an jedem Standort rund um die Uhr physisch vorhalten zu müssen, entstehen neue Möglichkeiten für eine effizientere und zugleich qualitativ hochwertige Versorgung.

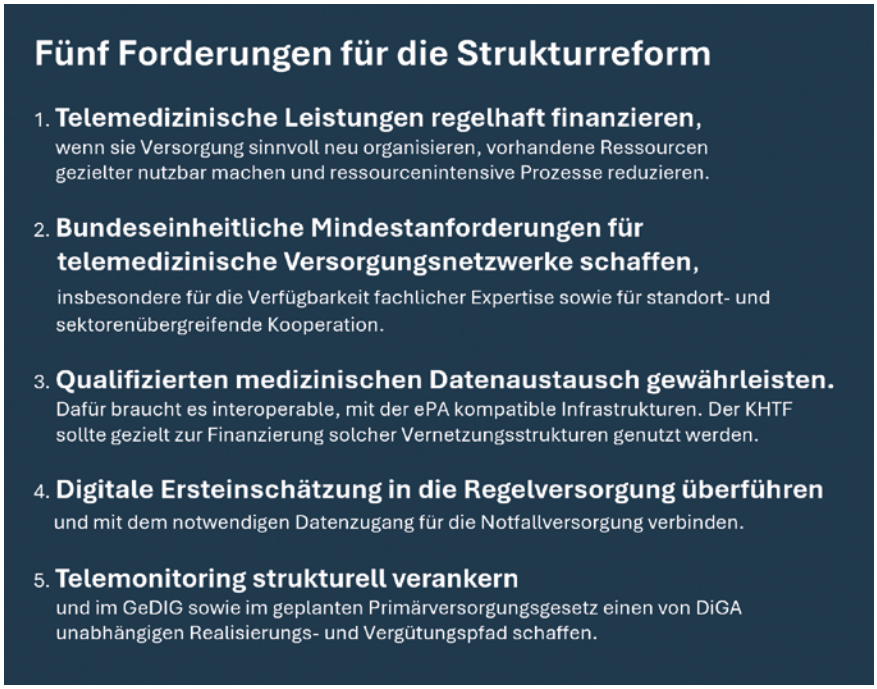
Die DGTelemed plädiert deshalb dafür, telemedizinische Leistungen insbesondere dort regelhaft zu finanzieren, wo sie zu einer medizinisch sinnvollen Neuorganisation von Versorgungsprozessen beitragen und beispielsweise Präsenzvorhaltungen oder unnötige Transporte reduzieren können. Für Krankenhausverantwortliche bedeutet das, Digitalisierung nicht primär als IT-Projekt zu betrachten. Entscheidend ist vielmehr: Wie können Versorgungsprozesse durch digitale Vernetzung effizienter gestaltet und medizinische Expertise dort verfügbar gemacht werden, wo sie gebraucht wird?

Telemonitoring: Kontinuierlich statt punktuell versorgen

Ein wichtiger Baustein ist das Telemonitoring, mit dem medizinisch relevante Daten strukturiert erhoben, übermittelt und ausgewertet werden können. Veränderungen im Krankheitsverlauf werden früher sichtbar und es kann gezielter reagiert werden. Gerade bei chronisch kranken Menschen eröffnet das die Chance, proaktiv und datenbasiert zu betreuen. Medizinische Kontakte können auf diese Weise stärker am tatsächlichen Versorgungsbedarf ausgerichtet werden. Zugleich unterstützt Telemonitoring die Zusammenarbeit zwischen Haus- und Facharztpraxen, Krankenhäusern und telemedizinischen Zentren.

Medizinische Expertise dort verfügbar machen, wo sie gebraucht wird: Die DGTelemed plädiert dafür, telemedizinische Leistungen insbesondere dort regelhaft zu finanzieren, wo sie zu einer medizinisch sinnvollen Neuorganisation von Versorgungsprozessen beitragen können. Bild: ZTG/Artvertise

Voraussetzung dafür sind professionelle Strukturen, klare Verantwortlichkeiten, interoperable Datenwege und definierte Prozesse. Bislang fehlt für viele Einsatzfelder ein geeigneter Weg in die Regelversorgung. Die DGTelemed fordert deshalb in das Gesetz für Daten und digitale Innovation im Gesundheitswesen (GeDIG) und in das geplante Primärversorgungsgesetz einen von digitalen Gesundheitsanwendungen (DiGA) unabhängigen Realisierungs- und Vergütungspfad für Telemonitoring aufzunehmen.
Auch künstliche Intelligenz ist in diesem Kontext ein Thema, denn gerade beim Telemonitoring können KI-basierte Verfahren perspektivisch helfen, große Datenmengen zu strukturieren, relevante Veränderungen zu erkennen und medizinisches Personal bei der Priorisierung zu unterstützen.



Krankenhäuser können aufgrund von Fachkräftemangel und zunehmender Spezialisierung durch die Krankenhausreform nicht mehr sämtliche Leistungen an jedem Standort vorhalten. Die DGTelemed fordert deshalb, Telemedizin konsequent in die anstehenden Strukturreformen mit einzubeziehen.

Bild: DGTelemed

Notfallversorgung: Digital steuern, Daten verfügbar machen

Auch in der Notfallversorgung sieht die DGTelemed erhebliches Potenzial. Eine digitale Ersteinschätzung kann Patienten bereits vor der Behandlung zur geeigneten Anlaufstelle lotsen und so unnötige Wege vermeiden helfen. Sie ist dabei klar von der notfallmedizinischen Triage zu unterscheiden: Während diese die medizinische Dringlichkeit im akuten Kontext bewertet, dient die digitale Ersteinschätzung der vorgelagerten Steuerung.

Für eine effektive Notfallversorgung reicht Steuerung allein jedoch nicht aus. Behandelnde müssen auch über eine digitale Fallübergabe hinaus auf relevante Daten zugreifen können. Erprobte Modelle der digitalen Ersteinschätzung sollten daher nach Auffassung der DGTelemed in die Regelversorgung überführt und mit dem notwendigen Zugriff auf behandlungsrelevante Daten verbunden werden.

Krisenresilienz durch telemedizinische Netzwerke

Telemedizinische Vernetzung ist auch eine Frage der Krisenvorsorge. Wenn regionale Versorgungskapazitäten in besonderen Lagen an ihre Grenzen stoßen, können telemedizinische Netzwerke medizinische Expertise einrichtungs- und länderübergreifend verfügbar machen. Dafür braucht es überregionale, beispiels-

Wie eine vernetzte Versorgung praktisch aussehen kann, zeigt das Hospital of the Future auf der Medica. Es präsentiert Technologien nicht isoliert, sondern verbindet Lösungen in einer realitätsnahen Krankenhausumgebung entlang konkreter Versorgungspfade.

Bild: DGTelemed

weise landesweite telekonsiliarische Vermittlungsplattformen. Strukturen, die im Versorgungsalltag funktionieren, können auf diese Weise auch dazu beitragen, das Gesundheitssystem in Krisensituationen resilienter zu machen.

Vom Einzelprojekt zum professionellen Netzwerk

Damit Telemedizin Bestandteil der Regelversorgung wird, darf Kooperation nicht von Einzelvereinbarungen oder persönlichem Engagement abhängen. Die DGTelemed fordert verbindliche, bundesweit übertragbare Mindestanforderungen an professionelle telemedizinische Versorgungsnetzwerke: technische Interoperabilität, qualitätsgesicherte 24/7-Verfügbarkeit fachlicher Expertise, klar geregelte Zuständigkeiten und Haftungsfragen sowie einheitliche Prozess- und Vertragsstrukturen.
Dafür braucht es einrichtungsübergreifende Vermittlungsplattformen und eine digitale Infrastruktur, über die medizinische Daten sicher und vollständig ausgetauscht werden können. Mittel aus dem Krankenhaustransformationsfonds (KHTF) sollten gezielter für digitale Vernetzungsinfrastrukturen eingesetzt werden.

Die ePA allein reicht nicht

Gerade bei telekonsiliarischer Mitbehandlung müssen Ärzte auf Befunde und Daten anderer Einrichtungen zugreifen können. Die politische Diskussion konzentriert sich häufig auf die elektronische Patientenakte (ePA). Für komplexe Behandlungssituationen greift das aus Sicht der DGTelemed zu kurz. Notwendig ist eine interoperable Infrastruktur für einen qualifizierten einrichtungsübergreifenden medizinischen Datenaustausch. Diese sollte mit der ePA kompatibel sein, darf sich funktional und inhaltlich aber nicht auf diese beschränken.

Vom politischen Konzept zur erlebbaren Versorgung

Wie eine solche vernetzte Versorgung praktisch aussehen kann, zeigt das Hospital of the Future (HOTF) auf der Medica 2026, das die DGTelemed gemeinsam mit der Messe Düsseldorf und klinischen Partnern gestaltet. Dort werden Technologien nicht isoliert präsentiert, sondern Lösungen in einer realitätsnahen Krankenhausumgebung entlang konkreter Versorgungspfade verbunden. So wird sichtbar gemacht, wie Technologie, medizinische Prozesse und Organisationsstrukturen ineinandergreifen können.
Gemeinsam mit Partnern wie der Uniklinik RWTH Aachen, der Technischen Universität München und dem Zentrum für Telemedizin in Bad Kissingen stellt die DGTelemed konkrete Versorgungsszenarien vor:

- Wie gelangt spezialisierte Expertise vom (Supra-)Maximalversorger zu anderen Krankenhäusern?
- Wie funktioniert Telemonitoring und an welchen Stellen im Versorgungspfad ist es auf welche Weise einsetzbar?
- Welche Infrastruktur ist notwendig?
- Wie müssen Prozesse und Verantwortlichkeiten organisiert sein?
- Welche Standards braucht ein Netzwerk, damit es dauerhaft funktioniert?
- Welche Anforderungen werden an professionelle telemedizinische Netzwerke gestellt?
- Wie können Mittel aus dem KHTF für digitale Vernetzungsstrukturen genutzt werden?

Als Kooperationspartner unterstützen auch mehrere medizinische Fachgesellschaften: die Deutsche Gesellschaft für Anästhesiologie und Intensivmedizin (DGAI), die Deutsche Gesellschaft für Kardiologie (DGK), die Deutsche Gesellschaft für Schlafforschung und Schlafmedizin (DGSM), die Deutsche Gesellschaft für Innere Medizin (DGIM) und die Deutsche Gesellschaft für Pneumologie (DGP).
Ein weiterer Schwerpunkt ist die künstliche Intelligenz (KI). Wie müssen Daten verfügbar und zwischen den beteiligten Professionen nutzbar sein, damit KI medizinische Entscheidungen sinnvoll unterstützen kann? Wie muss eine digitale Infrastruktur aufgesetzt sein, um KI integrieren zu können?

Ein wichtiger Baustein ist das Telemonitoring. Veränderungen im Krankheitsverlauf werden früher sichtbar und es kann gezielter reagiert werden. Gerade bei chronisch kranken Menschen eröffnet das die Chance, proaktiv und datenbasiert zu betreuen.
Bild: Oksana Klymenko/stock.adobe.com

Herausforderungen der Zukunft

Die zentrale Herausforderung der kommenden Jahre besteht nicht darin, möglichst viele digitale Einzelanwendungen einzuführen, sondern Versorgungsstrukturen neu zu denken. Telekooperation, Telemonitoring, digitale Patientensteuerung und KI können diesen Wandel unterstützen. Dafür müssen sie vom ergänzenden Digitalangebot zum integralen Bestandteil der Versorgung werden.
Das ‚Krankenhaus der Zukunft' ist deshalb kein digital aufgerüsteter Einzelstandort. Es ist ein Knotenpunkt in einem professionellen, interdisziplinären und sektorenübergreifenden Versorgungsnetzwerk. Wie ein solches Netzwerk medizinisch, technisch und organisatorisch funktioniert, gilt es jetzt gemeinsam zu gestalten – in der Gesundheitspolitik ebenso wie in der Versorgungspraxis.

Kontakt:

Deutsche Gesellschaft für
Telemedizin (DGTelemed) e. V.
Günter van Aalst
Luisenstraße 58/59
10117 Berlin
Tel.: +49 30 629369-290
info@dgtelemed.de
www.dgtelemed.de/hospital-of-the-future

Uniklinikum Hamburg-Eppendorf fördert bewegungsbezogene Gesundheitskompetenz seiner Pflegefachpersonen

Fit für die Schicht

Pflegefachpersonen bilden weltweit die größte Profession im Gesundheitswesen und haben aufgrund ihrer Tätigkeit eine hohe berufsbedingte körperliche Aktivität. Lange Laufwege, Heben, Umlagern und Tätigkeiten im Stehen – was auf den ersten Blick nach ausreichend Bewegung klingt, bringt jedoch nicht unweigerlich gesundheitliche Vorteile mit sich.

In der Wissenschaft wird das Phänomen als ‚Physical Activity Paradox' bezeichnet: Eine hohe körperliche Belastung im Beruf entfaltet nicht automatisch die gesundheitlichen Wirkungen, die von regelmäßiger körperlicher Aktivität in der Freizeit bekannt sind. Deshalb sollte eine Förderung ihren Schwerpunkt auf die Kompetenzen legen, die für eine gesunde Bewältigung körperlicher Aktivität erforderlich sind. Dabei spielt die bewegungsbezogene Gesundheitskompetenz eine zentrale Rolle. Im Projekt ‚BeGeKo-Care' am Universitätsklinikum Hamburg-Eppendorf (UKE) steht genau das im Mittelpunkt: die ‚Entwicklung einer hybriden Intervention zur Förderung der bewegungsbezogenen Gesundheitskompetenz bei Pflegefachpersonen'.

Anders als in der Freizeit erfolgt körperliche Aktivität im Berufsalltag selten selbstbestimmt. Arbeitsabläufe sind durch organisatorische Vorgaben, Zeitdruck und die Bedürfnisse der Patienten geprägt. Bewegungen werden häufig wiederholt ausgeführt, Regenerationsphasen sind kurz und Arbeitsbedingungen lassen sich nicht immer ergonomisch umsetzen. Aus diesem Grund reicht ein hohes Maß an körperlicher Aktivität allein nicht aus, um die Gesundheit langfristig zu fördern. Entscheidend ist vielmehr, wie Bewegung ausgeführt, reflektiert und in den Arbeitsalltag integriert wird. Vor diesem Hintergrund gewinnt die bewegungsbezogenen Gesundheitskompetenz als wichtige Voraussetzung für einen gesundheitsförderlichen Umgang mit körperlicher Aktivität an Bedeutung.

Gesunden Umgang mit körperlicher Aktivität fördern

Unter der Leitung von Prof. Dr. Susanne Klotz aus der Abteilung Physiotherapie entwickelt das Forschungsteam um Alicia Albers (M. Sc.) und Luisa Kresin (B. Sc.) gemeinsam mit Pflegefachpersonen eine Intervention, die ihre bewegungsbezogenen Gesundheitskompetenz stärken und langfristig zu einer gesundheitsförderlichen Gestaltung des Arbeitsalltags beitragen soll. Das von der DAK-Gesundheit geförderte Projekt läuft bis 2028 und verfolgt die Ziele,

- den aktuellen Ist-Stand der bewegungsbezogenen Gesundheitskompetenz und Selbstwirksamkeit sowie körperlichen Aktivität zu erfassen,
- gemeinsam mit Pflegefachpersonen eine hybride Intervention zu entwickeln,
- diese im Rahmen von ersten Durchgängen zu pilotieren und

Bewegungsbezogene Gesundheitskompetenz

Physical Activityrelated Health Competence (PAHCO) bezeichnet die Fähigkeit, Bewegung so zu gestalten und in den Alltag einzubinden, dass sie langfristig Gesundheit und Wohlbefinden fördert. Dazu gehören motorische Fähigkeiten ebenso wie die Kompetenz, körperliche Aktivität gesundheitsorientiert zu steuern und dauerhaft aufrechtzuerhalten.[1]

1. Carl, J., Sudeck, G., Geidl, W., Schultz, K. and Pfeifer, K. (2021): Competencies for a Healthy Physically Active Lifestyle-Validation of an Integrative Model. Res. Q. Exerc. Sport 2021, Vol. 92, No. 3, P. 1–15, doi: 10.1080/02701367.2020.1752885

Das Universitätsklinikum Hamburg-Eppendorf möchte langfristig ein gesünderes Arbeitsumfeld schaffen. Durch ein hybrides Modell aus Online- und Gruppenkursen soll die Gesundheitskompetenz des Personals gestärkt werden. Bild: UKE

Lange Laufwege, Heben, Umlagern und Tätigkeiten im Stehen – was auf den ersten Blick nach ausreichend Bewegung klingt, bringt jedoch nicht unweigerlich gesundheitliche Vorteile mit sich. Bild: UKE

- durch einen Implementierungsleitfaden ebenfalls für andere Settings zugänglich zu machen.

Das Projekt im Sinne einer betrieblichen Gesundheitsförderungsmaßnahme mit wissenschaftlicher Begleitung folgt einem Mixed-Methods-Ansatz: Die Daten werden mittels quantitativer und qualitativer Erhebungsmethoden generiert und ausgewertet. Dabei ist das Vorhaben in vier Phasen gegliedert: Ist-Stand-Analyse, Entwicklung der Intervention, Pilotierung und Implementierung.

In der Ist-Stand-Analyse nutzte das Forschungsteam standardisierte Fragebögen und qualitative Interviews zum Erfassen der bewegungsbezogenen Gesundheitskompetenz, der körperlichen Aktivität im Alltag und der Selbstwirksamkeit in Bezug auf körperliches Trainieren in der Freizeit. Die Ergebnisse bilden die Grundlage für die weitere Entwicklung der Intervention.

Interventionsentwicklung aus vielfältiger Perspektive

Aktuell befindet sich das Projekt in der Interventionsentwicklung, wobei durch den Einsatz verschiedener Maßnahmen möglichst viele Perspektiven in die Entwicklung mit einfließen sollen. Neben einer Literaturrecherche werden Experten aus unterschiedlichen Bereichen befragt. Ergänzend dazu wird ein sogenanntes Job-Shadowing durchgeführt: Die Forschenden begleiten die Pflegefachpersonen direkt im Alltag. Ziel ist es, die Ausführung pflegerischer Tätigkeiten hinsichtlich spezifischer Bewegungshandlungen zu beobachten, um Bewegungsabläufe, Belastungssituationen und Umgangsstrategien kennenzulernen. So soll ein möglichst realistisches Verständnis der beruflichen und physischen Anforderungen entwickelt werden.

Außerdem können Pflegefachpersonen des UKE in Workshops Ideen, eigenen Bedarf und individuelle Wünsche in den Prozess der Interventionsentwicklung mit einbringen. Fest steht bereits, dass die Intervention hybride Elemente miteinander verbinden soll. Geplant ist eine Kombination aus einem digitalen Lernangebot und Kleingruppenveranstaltungen in Präsenz, die sich möglichst gut in den Arbeitsalltag integrieren lassen.

Konsequente Beteiligung der betroffenen Pflegefachpersonen

Ein besonderer Schwerpunkt von BeGeKo-Care liegt auf der konsequenten Beteiligung der Zielgruppe: Pflegefachpersonen gestalten den Entwicklungsprozess von Beginn an mit. Dadurch soll sichergestellt werden, dass die Intervention nicht nur wissenschaftlich fundiert ist, sondern auch den tatsächlichen Anforderungen des Pflegealltags entspricht. Aspekte wie Schichtarbeit, Zeitressourcen oder unterschiedliche Tätigkeitsprofile können so bereits während der Entwicklung berücksichtigt werden. Gleichzeitig stärkt der partizipative Ansatz die Akzeptanz der späteren Intervention. Das erhöht die Wahrscheinlichkeit, dass entwickelte Maßnahmen langfristig in den Berufsalltag integriert werden können.

Nach Abschluss der Entwicklungsphase wird die Intervention in Zusammenarbeit mit ausgewählten Bereichen des UKE pilotiert. Die Pilotphase umfasst mehrere Schritte: Nach einer Baseline-Messung mit Fragebögen wird die hybride Intervention durchgeführt. Im Anschluss erfolgen eine Posttreatment-Messung und die Durchführung von Fokusgruppen. Ein Vergleich der Ergebnisse der Fragebögen soll die Darstellung sowohl positiver als auch negativer Effekte der Intervention ermöglichen. Die Fokusgruppen mit den Teilnehmern dienen dem gemeinsamen Austausch, um die Intervention bei Bedarf anpassen und optimieren zu können.

Auf Grundlage der Ergebnisse aus der Pilotierung wird anschließend ein Implementierungsleitfaden erstellt. Er soll anderen klinikinternen Bereichen und externen Gesundheitseinrichtungen ermöglichen, die entwickelte Maßnahme ebenfalls einzusetzen und an ihre jeweiligen Rahmenbedingungen anzupassen. So können die Erkenntnisse aus BeGeKo-Care auch über das UKE hinaus einen Beitrag zur betrieblichen Gesundheitsförderung leisten.

Pflegefachpersonen gestalten den Entwicklungsprozess von Beginn an mit, damit die Intervention nicht nur wissenschaftlich fundiert ist, sondern auch den tatsächlichen Anforderungen des Pflegealltags entspricht. Bild: UKE

Fazit und Ausblick

Das Projekt trägt zum besseren Verständnis der physischen Anforderungen in der Pflegeprofession bei. Die gewonnenen Erkenntnisse und die Intervention bilden eine fundierte Grundlage für die weiterführende Entwicklung gesundheitsfördernder Maßnahmen im Pflegesetting und können zugleich Impulse für deren praktische Umsetzung und für weitere Forschung liefern.

Projekt BeGeKo-Care: Unter der Leitung von Prof. Dr. Susanne Klotz (Mitte) entwickeln Alicia Albers (re.) und Luisa Kresin gemeinsam mit Pflegefachpersonen eine Intervention, die deren bewegungsbezogenen Gesundheitskompetenz stärken soll. Bild: UKE/Physiotherapie

Kontakt:

Universitätsklinikum
Hamburg-Eppendorf (UKE)
UKE Inside/Projekt BeGeKo-Care
Martinistraße 52
20251 Hamburg
www.uke.de

Luisa Kresin/Alicia Albers
Tel.: +49 152 22815605
begekocare@uke.de

Prof. Dr. Susanne Klotz
Tel.: +49 40 7410-18625
s.klotz@uke.de

Titelstory:

Warum Kliniken unter NIS2 neue Detektionsstrategien für Cybervorfälle brauchen

Sicherheitsrisiko Medizingeräte

Mit der Umsetzung der NIS2-Richtlinie rückt die Cybersicherheit in medizinischen Einrichtungen stärker in den Fokus. Während viele Diskussionen um Governance, Risikomanagement und Meldepflichten kreisen, stellt sich im Klinikalltag eine grundlegendere Frage: Wie lassen sich Medizingeräte absichern, deren Software sich über Jahre hinweg nicht aktualisieren lässt?

Moderne Kliniken betreiben heute je nach Größe zahlreiche bis tausende vernetzte Systeme – von MRT- und CT-Anlagen über Beatmungsgeräte und Infusionspumpen bis hin zu Laborautomatisierung und Patientenmonitoring. Viele sind für die Patientenversorgung unverzichtbar, basieren jedoch auf spezialisierten Betriebssystemen und unterliegen strengen Zulassungsanforderungen. Sicherheitsupdates lassen sich deshalb häufig nur eingeschränkt oder gar nicht einspielen.
Solange Kliniken zahlreiche Systeme aufgrund regulatorischer Vorgaben, Herstellerabhängigkeiten oder Betriebsanforderungen nicht zeitnah absichern können, genügt es nicht länger, allein auf Prävention und ein vollständiges Geräteinventar zu setzen. Es zeigt zwar, welche Systeme existieren, verrät jedoch nicht, ob sie sich gerade verdächtig verhalten. Genau diese Schutzlücke müssen Krankenhäuser durch kontinuierliche Überwachung und eine Anomalie-Erkennung aktiv kompensieren. Klassische IT-Sicherheitsstrategien stoßen hier an ihre Grenzen, neue Detektionsstrategien müssen an ihre Stelle treten.

Zwischen Patientensicherheit und Cybersecurity

NIS2 fordert angemessene technische, organisatorische und operative Maßnahmen, um Cyberrisiken für Netz- und Informationssysteme zu beherrschen. Für Krankenhäuser bedeutet das vor allem, Sicherheitsvorfälle frühzeitig zu erkennen und angemessen darauf zu reagieren.
Dabei entsteht ein Spannungsfeld: Ein Neustart eines Computers im Büro ist meist unproblematisch. Bei einem Beatmungsgerät kann dieselbe Maßnahme die Patientensicherheit gefährden. Verfügbarkeit besitzt deshalb in medizinischen Umgebungen höchste Priorität. Hinzu kommt, dass Medizingeräte im Vergleich zu klassischer IT-Hardware häufig zehn bis 15 Jahre oder länger in Betrieb sind. Betriebssysteme und Software bleiben also oft über Jahre unverändert und geraten damit zunehmend ins Visier von Angreifern, die genau diese bekannten Schwachstellen ausnutzen.

Sichtbarkeit als Entscheidungsgrundlage

Eine zentrale Herausforderung für Krankenhäuser besteht darin, überhaupt einen vollständigen Überblick über alle vernetzten Geräte zu erhalten. Klinknetzwerke wachsen kontinuierlich durch neue Stationen, Medizingeräte, externe Dienstleister und Herstelleranbindungen. Die Dokumentation hält mit dieser Entwicklung nicht immer Schritt.
Deshalb ist Transparenz die Grundlage jeder Sicherheitsstrategie. Neben klas-

Verfügbarkeit besitzt in medizinischen Umgebungen höchste Priorität. Für Krankenhäuser bedeutet das vor allem, Sicherheitsvorfälle frühzeitig erkennen und angemessen darauf reagieren zu können.

Bild: Arafat'e/stock.adobe.com (KI-generiert)

Kliniken betreiben verschiedenste vernetzte Systeme, die für die Patientenversorgung unverzichtbar sind. Solange sie diese jedoch aufgrund regulatorischer Vorgaben, Herstellerabhängigkeiten oder Betriebsanforderungen nicht zeitnah absichern können, genügt es nicht länger, allein auf Prävention und ein Geräteinventar zu setzen.

Bild: Business Image/stock.adobe.com(KI-generiert)

sischen IT-Systemen müssen Verantwortliche insbesondere Medizingeräte, IoT-Schnittstellen und deren Kommunikationsbeziehungen erfassen. Erst wenn bekannt ist, welche Systeme miteinander kommunizieren und welche für die Patientenversorgung besonders kritisch sind, lassen sich Risiken sinnvoll bewerten.

Dieser Überblick beschreibt jedoch nur einen Zustand. Seine Schutzwirkung entfaltet er erst, wenn Kliniken ihn fortlaufend mit dem tatsächlichen Verhalten der Geräte abgleichen. Genau hier setzt die Detektion an.

Anomalie-Erkennung als zentraler Schutzmechanismus

In Unternehmensnetzwerken gehören Schwachstellenscans und Sicherheitsagenten zum Standard. Bei Medizingeräten lassen sich solche Maßnahmen jedoch oft nicht einsetzen, weil sie die Stabilität oder Herstellerzertifizierungen beeinträchtigen könnten. Wo Verantwortliche ein Gerät weder patchen noch mit Agenten ausstatten dürfen, bleibt die kontinuierliche Beobachtung seines Verhaltens der wirksamste Weg, um Angriffe rechtzeitig zu bemerken. Passive Verfahren analysieren dazu den Netzwerkverkehr aus der Distanz und kommen ganz ohne direkten Zugriff auf die Geräte aus. Verändert sich das Kommunikationsverhalten, registrieren die Sicherheitsteams dies zuverlässig und der laufende Betrieb bleibt davon unberührt. Verhaltensbasierte Analysen liefern dabei Hinweise, die ein Inventar niemals sichtbar machen würde. Typische Muster, die auf einen Sicherheitsvorfall hindeuten, sind etwa

- die Kommunikation eines MRTs mit bislang unbekannten Zielen,
- auffällige SMB-Verbindungen eines Medizingeräts,
- ungewöhnliche Datenübertragungen,
- verdächtige Herstellerzugriffe außerhalb vereinbarter Wartungsfenster oder
- laterale Bewegungen im Kliniknetz, bei denen sich ein Angreifer schrittweise von einem System zum nächsten ausbreitet.

Jedes dieser Muster zeigt eine Abweichung vom eingespielten Normalverhalten und liefert damit einen frühen Hinweis auf ein Risiko, das ein reiner Blick auf den Gerätebestand übersehen würde. Zuständige Sicherheitsteams sollten Auffälligkeiten im Gesamtkontext der Infrastruktur bewerten, ihre Relevanz einordnen und zwischen sicherheitskritischen Ereignissen und unauffälligen Abweichungen unterscheiden.

Nicht jeder Alarm ist gleich kritisch

Die Erkennung eines kritischen Sicherheitsereignisses ist nur der erste Schritt. Entscheidend ist anschließend die richtige Bewertung, die sowohl Datenschutz- und Sicherheitsanforderungen als auch die Auswirkungen auf die Patientenversorgung berücksichtigt. Insbesondere die Verfügbarkeit medizinischer Systeme spielt eine zentrale Rolle, da Ausfälle unmittelbare Folgen für den Behandlungsbetrieb haben können.

Ein ungewöhnlicher Datenverkehr auf einem Verwaltungsserver hat eine andere Bedeutung als eine Kommunikationsstörung zwischen Intensivstation, Patientenmonitoring und KIS. Genau hier unterscheidet sich die Priorisierung in der Medizintechnik grundlegend von der im Office-Netzwerk: Sicherheitsteams müssen technische Alarme stets im Kontext der betroffenen Systeme, ihrer Funktion

Anomalie-Erkennung als wirksamer Schutzmechanismus: Wo Verantwortliche ein Gerät weder patchen noch mit Agenten ausstatten dürfen, bleibt die kontinuierliche Beobachtung seines Verhaltens der wirksamste Weg, um Angriffe rechtzeitig zu bemerken.

Bild: GreenOptix/stock.adobe.com(KI-generiert)

Wachsam bleiben: Cybersicherheit entwickelt sich zunehmend zu einer dauerhaften Management- und Betriebsaufgabe, die sich dynamisch an neue Technologien, Bedrohungen und Versorgungsstrukturen anpassen muss.

Bild: Biru Langit Desember/stock.adobe.com (KI-generiert)

im Klinikbetrieb und der möglichen Auswirkungen bewerten. Erst diese Einordnung ermöglicht es, Maßnahmen gezielt abzuleiten und angemessen zu reagieren. Zusätzlich erschwert die Vielzahl proprietärer Systeme die Lagebewertung. Medizingeräte unterschiedlicher Hersteller kommunizieren häufig über eigene Protokolle und liefern Informationen in unterschiedlichen Formaten. Die Herausforderung besteht darin, diese Daten mit Ereignissen aus der IT zusammenzuführen und in einen gemeinsamen Kontext zu bringen

Richtlinie verlangt, operativ handlungsfähig zu bleiben

Die Fähigkeit, Sicherheitsvorfälle schnell einzuordnen, ist zugleich Voraussetzung für die Anforderungen von NIS2. Im Ernstfall müssen Krankenhäuser innerhalb kurzer Zeit beantworten können: Welche Systeme sind betroffen? Welche Auswirkungen hat der Vorfall auf die Patientenversorgung? Und welche Maßnahmen wurden bereits eingeleitet?
Diese Informationen entstehen nicht erst im Krisenfall. Krankenhäuser müssen die Daten im laufenden Betrieb kontinuierlich erfassen, bewerten und nachvollziehbar dokumentieren. Nur so können sie Risiken realistisch einschätzen, angemessen reagieren und die regulatorischen Anforderungen von NIS2 erfüllen.

Erfolgreiche NIS2-Umsetzung bedeutet Handlungsfähigkeit

Sicherheitskonzepte aus der klassischen IT lassen sich nicht ohne Weiteres auf Medizingeräte übertragen. Wo Systeme über viele Jahre hinweg im Einsatz bleiben und sich weder patchen noch mit klassischen Schutzmechanismen ausstatten lassen, entscheidet die frühzeitige Erkennung verdächtiger Aktivitäten maßgeblich über das Sicherheitsniveau einer Klinik. Transparenz schafft dafür die Grundlage, die eigentliche Schutzwirkung entsteht jedoch erst durch die fortlaufende Verhaltensanalyse. Nur wenn Kliniken Auffälligkeiten frühzeitig erkennen und im Kontext der medizinischen Versorgung bewerten, priorisieren sie Risiken gezielt und leiten geeignete Maßnahmen ab.
NIS2 unterstreicht diese Entwicklung. Die Richtlinie verpflichtet Krankenhäuser, angemessene Sicherheitsmaßnahmen umzusetzen und Cybervorfälle nachvollziehbar zu erkennen, zu bewerten und zu bewältigen. Mit der fortschreitenden Vernetzung von Medizingeräten, digitalen Gesundheitsanwendungen und klinischen IT-Systemen wächst die Angriffsfläche in den kommenden Jahren weiter.
Cybersicherheit entwickelt sich damit zunehmend zu einer dauerhaften Management- und Betriebsaufgabe, die sich dynamisch an neue Technologien, Bedrohungen und Versorgungsstrukturen anpassen muss. Externe, professionelle Unterstützung können dabei Managed Security Service Provider wie 8COM bieten.

Autor:

Jürgen Crasser,
Senior Architect & Strategist
Cyber Resilience
bei 8COM

Kontakt:

8COM GmbH
Julia Olmscheid
Head of Communications
Europastraße 32
67433 Neustadt a. d. Weinstraße
Tel.: +49 6321 48446-2035
info@8com.de
www.8com.de

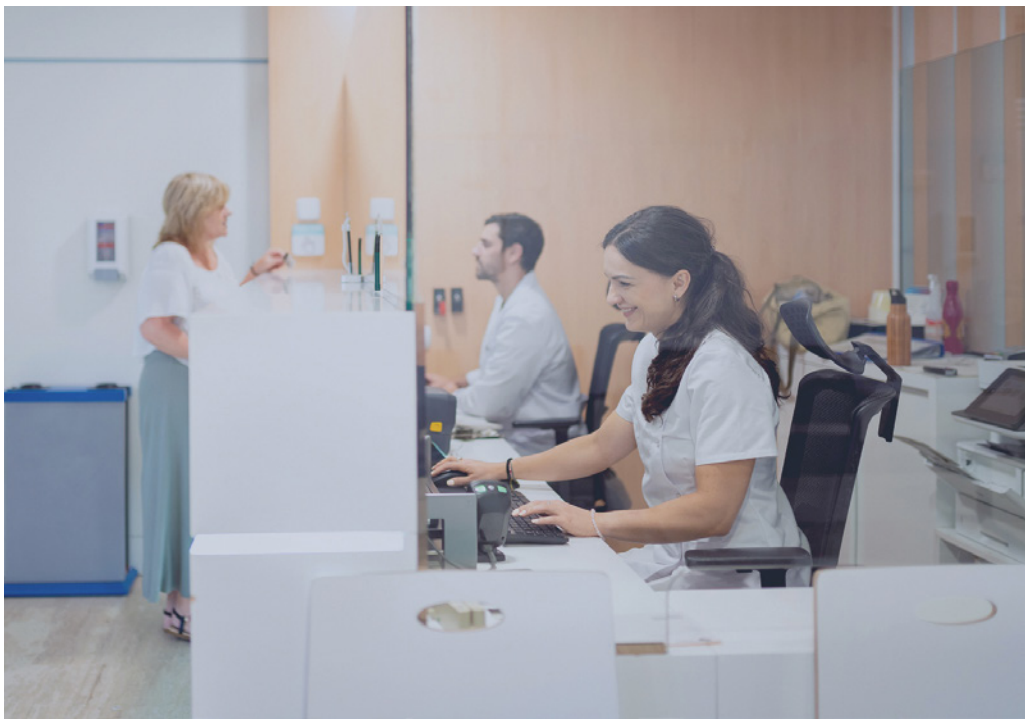
Mit der fortschreitenden Vernetzung wächst die Angriffsfläche weiter. Externe Experten wie die Analysten des Managed Security Service Providers 8COM übernehmen rund um die Uhr Alarmbearbeitung und Incident Response.

Bild: 8COM

Wie aus der Terminbuchung im Patientenportal ein orchestrierter Klinikprozess wird

Zwischen digitaler Terminbuchung und analoger Aufnahme

Auch die bestens eingespielte analoge Patientenaufnahme bringt strukturelle Herausforderungen mit sich: Mitarbeiter verbringen einen Großteil ihrer Arbeitszeit mit Datenerfassung oder Klärung von Fragen. Patienten sind nicht selten mit dem Aufnahmeprozess überfordert. Nachfolgende Prozesse können ins Stocken geraten. Ein Patientenportal kann genau hier ansetzen und Patienten aktiv bis in die Klinik hinein begleiten. Die Mitarbeiter werden von wiederkehrenden, manuellen Tätigkeiten entlastet. Die Patienten profitieren von mehr Sicherheit und Orientierung. Und schließlich wirkt sich der Prozess auch wirtschaftlich aus: weniger Aufwand, geringere Kosten, mehr Einnahmen.



Ein Patientenportal, das über die reine Terminbuchung hinausgedacht wird, kann zum echten Rückgrat des Aufnahmeprozesses werden. Bilder: Polavis

Paula A. muss für einen lange geplanten Routineeingriff ins Krankenhaus. Sie erscheint pünktlich um 8.30 Uhr mit einer Überweisung, verschiedenen Vorbefunden und weiteren Papierunterlagen bei der Patientenaufnahme. Hier prüft eine Mitarbeiterin die Personal- und Versicherungsdaten und übergibt ihr Aufnahmebögen, Einwilligungen und Wahlleistungsverträge, die A. händisch ausfüllt. Sie werden später zusammen mit den mitgebrachten Dokumenten eingescannt und Behandlern, Stationen oder Räumen zugeordnet. Da das Prozedere viel Zeit in Ansprung nimmt, bildet sich an der Aufnahme bereits eine längere Warteschlange.

Nach der administrativen Aufnahme wird Paula A. nacheinander zu verschiedenen Ambulanzen und Untersuchungsbereichen geschickt, die über die einzelnen Klinikgebäude und Etagen hinweg verteilt sind. Dabei muss sie mehrfach nach dem richtigen Weg fragen. In den einzelnen Bereichen wird sie jeweils mündlich aufgerufen, sie fühlt sich an diesem Vormittag häufig verloren. Gegen 12.30 Uhr sind endlich alle erforderlichen Untersuchungen abgeschlossen und die Unterlagen vollständig. Paula A. wird auf Station geschickt und bezieht dort ihr Zimmer.

Herausforderungen analoger Patientenaufnahme

Dieser bekannte Ablauf, so eingespielt er in vielen Häusern auch sein mag, bringt strukturelle Herausforderungen mit sich, die sich auf die nachgelagerten administrativen, klinischen und pflegerischen Prozesse auswirken. Mitarbeiter verbringen einen großen Teil ihrer Arbeitszeit mit Datenerfassung, Dokumentenprüfung und der Klärung von Fragen. Damit einher geht eine hohe Arbeitslast durch die Bedienung verschiedener Systeme, durch nur auf Papier vorliegende Informationen und fehlende Dokumente.

Ohne eine zentrale Steuerung der Patientenströme über Anlaufpunkte und Wartebereiche hinweg, kommt es zu ständigen Unterbrechungen durch Rückfragen von Patienten, Anrufe von Stationen oder die Suche nach Informationen. Der Administration fehlt Transparenz über den aktuellen Status aufgenommener Patienten und für die klinischen Bereiche bleibt oft unklar: Sind die Patienten bereits angekommen? Welche Schritte sind bereits abgeschlossen? Und wann ist mit der Übergabe zu rechnen? Bei hohen Patientenaufkommen sind situativen Priorisierungen die Folge.

Aber auch für Paula A. ist der Aufnahmeprozess belastend. Sie ist zunehmend unsicher, ob noch Schritte anstehen, wie lange sie noch warten und wo sie sich als nächstes melden muss. Außerdem verspätet sie sich auf ihrem Weg durch das Krankenhaus, weshalb ein Untersuchungstermin verschoben werden muss – für das Krankenhaus ein theoretisch leicht vermeidbarer Ressourcenausfall.

Endlich auf Station fragt sich Paula A., warum ihr alles so kompliziert erscheint, hat ihr Hausarzt doch den Termin für ihren Eingriff online über das Patientenportal der Klinik für sie vereinbart und alle Unterlagen vorab schon übermittelt. Hier zeigt sich die Herausforderung im Zusammenspiel zwischen digitaler Terminbuchung und analoger Aufnahme.

Die Lösung: Der digitale Aufnahmetag

Ein Patientenportal kann genau an der Schnittstelle zwischen digital und analog ansetzen: Über die Terminbuchung hinaus begleitet es Patientin Paula A. aktiv bis in die Klinik hinein. Sie erhält – auch bei Buchung durch ihren Hausarzt – automatisch eine Terminbestätigung und darüber hinaus eine persönliche Checkliste, Anfahrts- und Gebäudeinformationen sowie Hinweise zur Vorbereitung. Ein QR-Code erleichtert die Aufnahme vor Ort. Die Mitarbeiter der Patientenaufnahme können im Vorfeld prüfen, ob alle notwendigen Informationen und Dokumente vorliegen und sie ansonsten rechtzeitig nachfordern.

Am Tag der Aufnahme nutzt Paula A. den sogenannte Self-Check-in über die Kioskterminals. Sie meldet sich über den QR-Code an und lässt ihre elektronische Gesundheitskarte einlesen. Identität, Termin und vorhandene Daten werden automatisch abgeglichen. Bestehen noch Unklarheiten, wird sie an die Mitarbeiter der Aufnahme weitergeleitet. Ansonsten werden alle relevanten Informationen automatisch an die angebundenen Informationssysteme übergeben.

Ebenfalls automatisch ordnet das System Paula A. entsprechend ihrer im Vorfeld festgelegten Priorität in eine digitale Warteliste ein. Die Mitarbeiter behalten dabei die Möglichkeit, die Reihenfolge nach medizinischen oder organisatorischen Kriterien anzupassen. Über Aufrufmonitore wird Paula A. gezielt zum jeweiligen Behandler oder Wartebereich gesteuert und nach Abschluss aller administrativen Schritte mit vollständig vorliegenden digitalen Unterlagen an die Station übergeben.

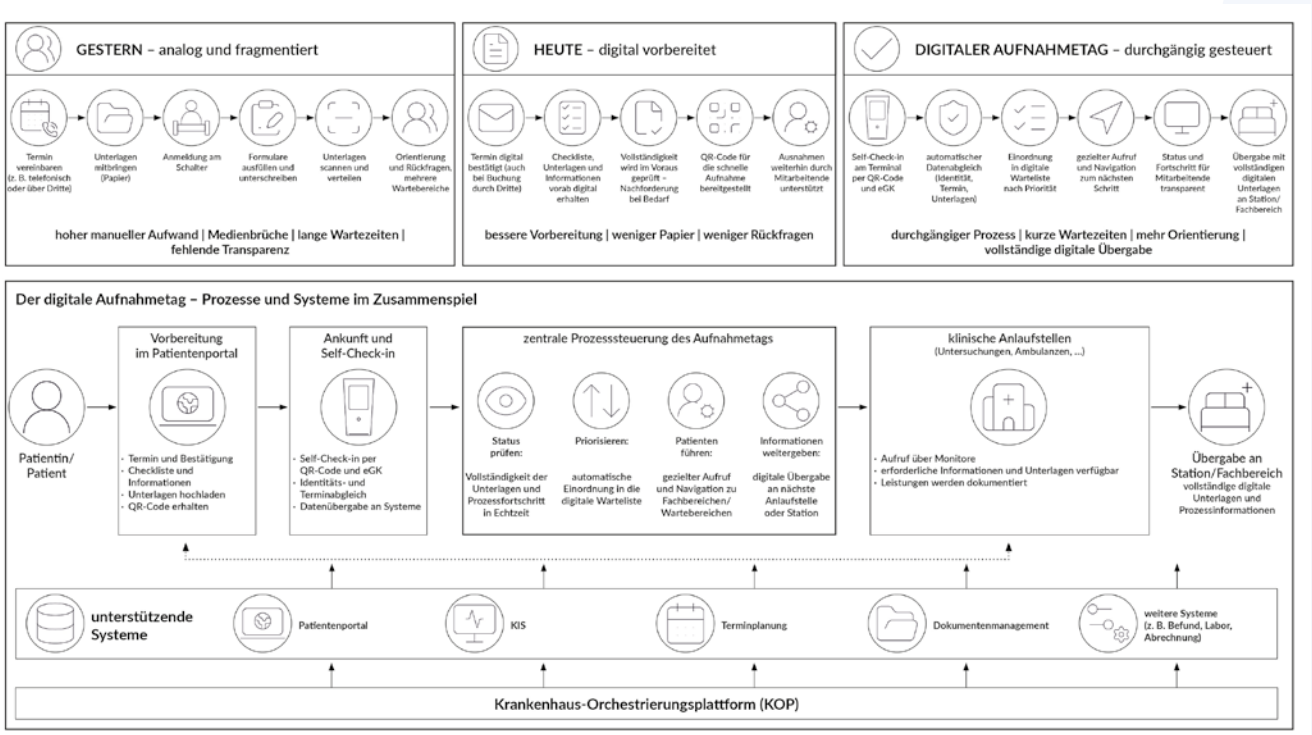
Positive Wirkung des digitalen Workflows auf mehreren Ebenen

Für die Patientin bedeutet der digitale Aufnahme-Workflow vor allem mehr Sicherheit und Orientierung: Welche Schritte folgen als nächstes? Was ist noch zu erledigen? Paula A. weiß, wo sie warten soll, und eine verlässliche Navigation reduziert Laufwege und Fehlleitungen. Der zuverlässige Zugriff auf bereits erfasste Daten vermeidet Mehrfachangaben, zudem müssen persönliche Daten nicht hörbar am offenen Schalter genannt werden – insgesamt ein wesentlich besseres Patientenerlebnis.

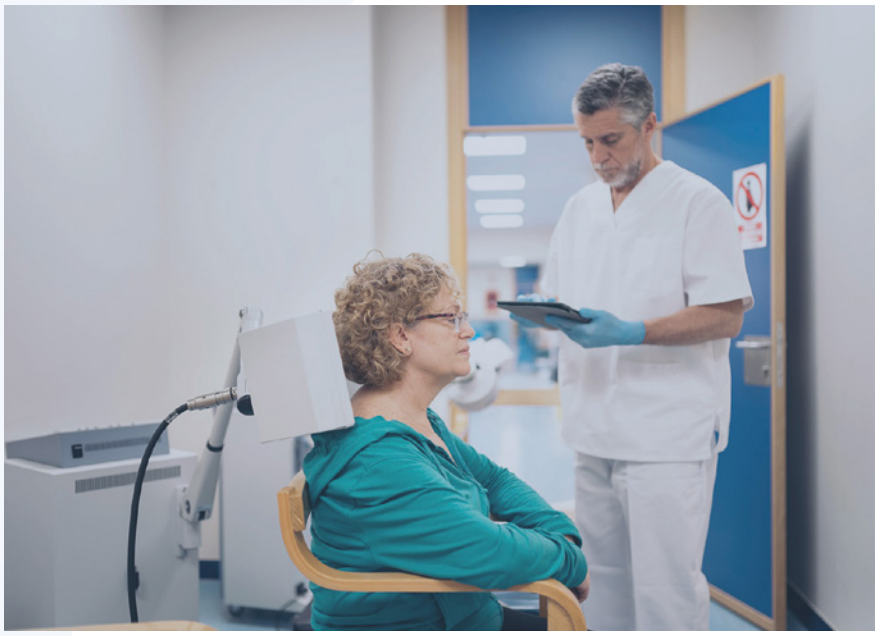
Die Mitarbeiter der Patientenaufnahme werden von wiederkehrenden Tätigkeiten wie manuellen Dateneingaben, Scannen und Sortieren von Dokumenten, Standardauskünften zum weiteren Ablauf, telefonischen Statusanfragen oder der Suche nach Patienten und fehlenden Unterlagen entlastet. Dadurch bleibt mehr Zeit für Patienten, die persönliche Unterstützung benötigen, etwa älteren Menschen, Personen mit Sprachbarrieren oder komplexen Aufnahmefällen. Zugleich verbessert sich die Datenqualität, weil Angaben nur noch einmal übertragen und Dokumente eindeutig zugeordnet werden.

Im Ergebnis verkürzen sich administrative Durchlauf- und Wartezeiten. Schalter, Räume und Untersuchungsbereiche lassen sich besser auslasten. Medienbrüche entfallen, Workflows werden standardisiert und nachvollziehbar. Verspätete oder ungeplant eintreffende Patienten werden frühzeitig sichtbar und können gezielt in den Ablauf eingeordnet werden.

Auch die Organisation profitiert: Behandlungsteams können sich besser vorbereiten, weil relevante Informationen frühzeitig verfügbar sind. Fehlende Unterlagen oder Einwilligungen können rechtzeitig nachgefordert werden. Digital vorliegende Daten ermöglichen eine vorausschauende Planung des Aufenthalts, womit Diagnostik und Behandlungen auch termingerechter beginnen können. Schließlich wirkt sich der Prozess auch wirtschaftlich aus: Der administrative Aufwand pro Aufnahme sinkt. Es entstehen weniger Kosten für Papier, Druck, Scannen und Archivierung sowie Nachbearbeitung fehlender Dokumente. Wahlleistungen werden vollständiger erfasst und dokumentiert, was die Einnahmen steigert. Einwilligungen und Verträge können leichter nachgewiesen



Aufnahmeprozesse intelligent steuern: So wird aus der Terminbuchung im Patientenportal ein orchestrierter Klinikprozess.



Die Patienten werden gezielt zum jeweiligen Behandler oder Wartebereich gesteuert und nach Abschluss aller administrativen Schritte an die Station übergeben. Bilder: Polavis

werden. Und die Wahrscheinlichkeit sinkt, dass verfügbare klinische Ressourcen durch fehlgeleitete oder verspätete Patienten ungenutzt bleiben.

Implementierungshürden lassen sich überwinden

Die Implementierung eines komplett digitalen Prozesses von Terminbuchung und Patientenaufnahme ist anspruchsvoll. Sie bedeutet weit mehr als das Aufstellen von Selbstbedienungsterminals und das Aufhängen von Aufrufmonitoren. Entscheidend ist die Einbindung in die bestehende Systemlandschaft. Patientenportal, KIS, Terminplanung, Dokumentenmanagement und weitere Anwendungen müssen Informationen zuverlässig austauschen und aufnehmen. Zudem unterscheiden sich Aufnahmeprozesse erheblich: Elektive Patienten durchlaufen beispielsweise andere Schritte als ungeplant eintreffende. Fachabteilungen benötigen unterschiedliche Dokumente und Prüfungen. Diese Prozessvielfalt muss abbildbar sein.

Auch bei dieser Digitalisierungsmaßnahme ist die Akzeptanz eine Herausforderung. Manche Patienten sind mit digitalen Angeboten ungeübt und überfordert. Gleichzeitig müssen Mitarbeiter gewohnte Abläufe verändern und einen Teil der bisherigen Steuerung an ein digitales System abgeben. Hinzu kommen Anforderungen an Datenschutz, Informationssicherheit und die technische Ausstattung.

Diese Hürden lassen sich jedoch überwinden, wenn einige Prinzipien beachtet werden. Um die Komplexität zu mindern, sollte die digitale Patientenaufnahme eng an das bestehende Patientenportal angebunden werden, denn eine isolierte Anwendung schafft neue Schnittstellen und erhöht den Pflegeaufwand.

Sinnvoll sind konfigurierbare Prozesse, die sich an die Abläufe einzelner Standorte und Fachbereiche anpassen lassen. Dabei empfiehlt sich ein schrittweises Vorgehen:

1. Auswahl eines klar abgegrenzten Pilotbereichs
2. Aufnahme und Vereinfachung des bestehenden Aufnahmeprozesses
3. Einbindung der betroffenen Mitarbeiter in die Gestaltung
4. Test mit unterschiedlichen Patientengruppen
5. Auswertung der Ergebnisse und Anpassung des Workflows
6. Übertragung auf weitere Bereiche

Für Patienten muss die Bedienung verständlich und eindeutig sein. Klare Anweisungen, wenige Eingabeschritte und eine sichtbare Möglichkeit, Unterstützung anzufordern, sind wichtiger als große Funktionsvielfalt. Digitale und persönliche Aufnahme sollten so verstanden werden, dass sie sich gegenseitig ergänzen. Die Technik übernimmt geeignete Standardabläufe, Mitarbeiter konzentrieren sich auf Ausnahmen und individuelle Hilfestellung.

Erfolg messbar machen

Ob die digitale Patientenaufnahme tatsächlich Mehrwerte schafft, sollte andhand weniger, aber aussagekräftiger Kennzahlen überprüft werden. Geeignet sind beispielsweise:

- Dauer vom Betreten der Klinik bis zum Abschluss der administrativen Aufnahme,
- Wartezeit an den einzelnen Anlaufstellen,
- Anteil vollständig vorbereiteter Patienten,
- Anteil der Aufnahmen über den digitalen Check-in,
- Zahl der Fälle mit Unterstützungsbedarf,
- Rückfragen zwischen Aufnahme und Fachbereichen,
- Anteil pünktlich begonnener Folgeprozesse,
- Bearbeitungsaufwand für die Mitarbeiter,
- Zufriedenheit von Patienten und Mitarbeitern.

Ein Patientenportal, das in dieser Form über die reine Terminbuchung hinausgedacht wird, wird zum echten Rückgrat des Aufnahmeprozesses. Die digital unterstützte Führung am Aufnahmetag zeigt, wie ein wirksames Instrument der Prozesssteuerung entsteht. Der Aufwand für Integration, Change Management und technische Ausstattung ist hoch – doch die Effekte, die sich für Patienten, Personal, Organisation und Wirtschaftlichkeit erzielen lassen, lohnen den Einsatz.

Und Paula A. hofft, dass sie bei ihrem nächsten Krankenhausaufenthalt auch von den Annehmlichkeiten eines digitalen Aufnahmeprozesses profitiert.

Autorin:

Kathrin Jeckel, Produktmanagerin bei Polavis

Kontakt:

Polavis GmbH
Kathrin Jeckel
Französische Straße 8
10117 Berlin
kathrin.jeckel@polavis.de
www.polavis.de

Effiziente und nachhaltige Kühlkonzepte für moderne Krankenhaus-Rechenzentren umsetzen

Kritische Infrastruktur im Fokus

In modernen Krankenhäusern ist der reibungslose und stabile Betrieb der IT-Infrastruktur unabdingbar für eine sichere Patientenversorgung. Ob digitale Patientenakten, bildgebende Verfahren in der Radiologie oder das Echtzeit-Monitoring auf den Intensivstationen – ohne leistungsfähige Rechenzentren steht der Klinikbetrieb still. Doch während die digitale Transformation medizinische Abläufe effizienter macht, wächst im Hintergrund eine physische Herausforderung: der massive Energiebedarf und die damit einhergehende Wärmeentwicklung der Server. Die richtige Klimatisierung bildet dabei eine zentrale Voraussetzung für Betriebssicherheit und Nachhaltigkeit.

Rechenzentren in klinischen Einrichtungen unterscheiden sich grundlegend von gewöhnlichen Unternehmens-IT-Standorten. Ein Systemausfall hat hier nicht nur wirtschaftliche Folgen, sondern kann unmittelbar Menschenleben gefährden. Entsprechend hoch sind die Anforderungen an Verfügbarkeit und Ausfallsicherheit, die sich häufig an strengen Tier-III-Standards orientieren. Redundanz ist in allen zentralen Bereichen unerlässlich – von der Stromversorgung über die Netzwerkpfade bis hin zur Kühlung.

Ein wesentlicher Unterschied liegt im Lastprofil: Während Bürogebäude nachts in einen Ruhemodus gehen können, arbeiten klinische Systeme wie die OP-Planung oder das Labor-Informationsmanagement rund um die Uhr unter Hochlast. Der 24/7-Dauerbetrieb erfordert Kühlsysteme, die ohne jede Unterbrechung funktionieren und sich im laufenden Betrieb warten lassen. Zudem treiben innovative Technologien wie KI-gestützte Diagnostik und hochauflösende Bildarchivierung die Performance-Anforderungen in den Racks massiv nach oben. Die Konzentration von Rechenpower auf engstem Raum führt zu thermischen Belastungen, die herkömmliche Luftkühlsysteme an ihre Grenzen bringen.

Regulatorischer Druck und Effizienzziele

Neben den technischen Anforderungen erhöhen auch regulatorische Vorgaben den Druck auf Rechenzentrumsbetreiber, ihre Energieeffizienz kontinuierlich zu verbessern. Maßgeblich ist dabei insbesondere das Energieeffizienzgesetz (EnEfG). Nach derzeit geltendem Recht müssen Rechenzentren, die vor dem 1. Juli 2026 in Betrieb genommen wurden, ab dem 1. Juli 2027 dauerhaft eine Power Usage Effectiveness (PUE) von höchstens 1,5 im Jahresdurchschnitt erreichen. Ab dem 1. Juli 2030 sinkt dieser Grenzwert auf 1,3. Für Rechenzentren, die ab dem 1. Juli 2026 ihren Betrieb aufnehmen, gilt ein PUE-Wert von höchstens 1,2. Nach geltender Rechtslage muss dieser spätestens zwei Jahre nach Inbetriebnahme dauerhaft im Jahresdurchschnitt erreicht werden.

Allerdings befindet sich Stand August 2026 eine Novelle des EnEfG im Gesetzgebungsverfahren. Der vom Bundeskabinett beschlossene Entwurf sieht vor, die Anforderungen für Bestandsrechenzentren moderat anzupassen: Ab dem 1. Juli 2027 soll ein PUE-Wert von höchstens 1,6 und ab dem 1. Juli 2030 von höchstens 1,4 gelten. Für neue Rechenzentren soll der Grenzwert von 1,2 bestehen bleiben, allerdings soll die Übergangsfrist bis zur Einhaltung von zwei auf vier Jahre verlängert werden. Darüber hinaus ist eine Anhebung der für die Anforderungen relevante Leistungsschwelle geplant: Während das geltende EnEfG Rechenzentren ab einer nicht redundanten Nennanschlussleistung von 300 kW

Hinter den Kulissen moderner Klinikkorridore ist der reibungslose Betrieb der IT-Infrastruktur unabdingbar für die Sicherheit der Patientenversorgung. Leistungsfähige Rechenzentren und deren effiziente Klimatisierung bilden dafür die Basis.

Bild: krismicrostoker/stock.adobe.com (KI-generiert)

Der steigende Bedarf an Rechenzentrumsleistung erfordert effiziente Kühlsysteme. Betreiber müssen dabei zahlreiche Gesetze mit strengen Anforderungen an Energieverbrauch, Abwärmenutzung und Umweltschutz einhalten.

Bild: Gorodenkoff/stock.adobe.com

erfasst, sieht der Entwurf eine Schwelle von 500 kW vor.

Gezielte Kühlstrategien

Für Krankenhausbetreiber bedeutet das: Sie müssen prüfen, ob sie von den EnEfG-Regelungen betroffen sind und gegebenenfalls veraltete Kühlanlagen dringend modernisieren. Denn sie verschlingen oft bis zu 50 Prozent des gesamten IT-Energiebedarfs. Um die hohen Anforderungen zu erfüllen, sollten Klimaverantwortliche über die klassische Luftkühlung hinausdenken. Bei moderaten Leistungsdichten bleibt sie zwar bewährter Standard, doch mit steigender Serverdichte wächst das Risiko kritischer Hotspots.

Für Healthcare-Rechenzentren empfehlen sich daher gezielte Kühlstrategien. Eine Kalt- und Warmgangtrennung in Kombination mit CRAC- (Computer Room Air Conditioner) oder CRAH-Einheiten (Computer Room Air Handler) ermöglicht beispielsweise eine präzise Temperatursteuerung. Die Systeme regulieren Temperatur und Luftfeuchtigkeit entsprechend den Empfehlungen der American Society of Heating, Refrigerating and Air-Conditioning Engineers (ASHRAE) und tragen so dazu bei, die Hardware zuverlässig vor thermischer Belastung zu schützen.

Von der Luft- zur Wasserkühlung

Da Wasser eine signifikant höhere Wärmekapazität als Luft besitzt, eignen sich wassergekühlte Systeme besonders für Umgebungen mit hoher Leistungsdichte. Dabei kommen oft hocheffiziente Flüssigkeitskühler zum Einsatz, die auch für die anspruchsvollen Bedingungen im Gesundheitswesen konzipiert sind. Darüber hinaus gilt die Nutzung der Außenluft als eine der effizientesten Kühlungsmethoden. Insbesondere in kälteren Regionen lässt sich durch direkte oder indirekte Freikühlung ein Großteil der jährlichen Kühlleistung ohne energieintensive Kompressoren erbringen. Zu empfehlen sind insbesondere hybride Modelle, die Komponenten aus den verschiedenen Kühlsystemen intelligent kombinieren. Denn sie verbinden in einer Anlage vielfältige Vorteile wie höhere Energieeffizienz und bessere Kühlleistung.

Ein weiterer wichtiger Faktor für die Klimatisierung von Rechenzentren ist die konsequente Nutzung von Abwärme. Denn nahezu die gesamte, in die IT investierte elektrische Energie wird in Wärme umgewandelt. Gerade für Krankenhäuser besteht darin ein enormes Potenzial. In herkömmlichen Rechenzentren

Hocheffiziente Kältetechnik für den 24/7-Dauerbetrieb: Leistungsstarke und kompakte Kühlgeräte bilden das Rückgrat der Rechenzentrums-Klimatisierung. Auch bei enormer Serverdichte, zum Beispiel durch KI-gestützte Diagnostik, sorgen sie für höchste Ausfallsicherheit und PUE-Werte im Zielbereich.

Bilder: Carrier

wird die Abwärme oft ungenutzt an die Umwelt abgegeben. In einer Klinik hingegen ist der Wärmebedarf für Heizung und Warmwasserbereitung das ganze Jahr über konstant hoch, sodass sich die Abwärmenutzung hier in besonderem Maße anbietet.

Durch den Einsatz von Wärmepumpen und Wärmetauschern lässt sich die Abwärme des Rechenzentrums auf ein höheres Temperaturniveau heben und für verschiedene Zwecke auf dem Krankenhauscampus nutzen:

- Beispielsweise können die Heizkreisläufe von Bettenhäusern, Ambulanzen, Laboren und Verwaltungsgebäuden unterstützt werden. Auch lässt sich die Warmwasserversorgung von Patientenzimmern, OP-Bereichen, Küchen und Wäschereien durch die Bereitstellung von Grundlastwärme optimieren.
- Darüber hinaus benötigt die zentrale Sterilgutversorgung für Reinigungs- und Desinfektionsprozesse große Mengen an thermischer Energie, die sich aus Abwärme ideal generieren lässt.
- Und schließlich können auch große Universitätskliniken von der Abwärme profitieren, wenn sie über klinikinterne Nahwärmenetze effizient zwischen verschiedenen Gebäuden verteilt wird.

So lässt sich dank CO_2-Einsparung die ökologische Bilanz verbessern, während gleichzeitig die Betriebskosten des gesamten Standorts signifikant sinken.

Die erzeugte Abwärme muss zuverlässig abgeführt werden, um Hardware vor Überhitzung und Schäden zu schützen. Herkömmliche Luftkühlung stößt bei steigender Serverdichte an ihre Grenzen. Bild: jarmoluk/pixabay

Richtig kühlen: Fünf Tipps für Klinik-Verantwortliche

Für Verantwortliche in Krankenhäusern empfiehlt es sich, die Kühlung nicht isoliert, sondern als Teil der technischen Gebäudeausrüstung zu betrachten. Fünf Aspekte sollten dabei im Fokus stehen:

- Ganzheitliche Systembetrachtung: IT, Stromversorgung und Klimatechnik sollten als Einheit geplant werden. Nur wer die Wechselwirkungen versteht, kann die Abwärmequote maximieren und den PUE-Wert dauerhaft senken.
- Intelligente Steuerung und Sensorik: Echtzeitmessungssensoren sowie die prädiktive Analyse von Luftströmen und Feuchtigkeit sorgen für eine bedarfsgerechte, ggf. KI-basierte Regelung der Kühlanlagen. Die Einbindung in das zentrale Gebäudemanagementsystem ist dabei für Krankenhäuser essenziell.
- Standortfaktoren einbeziehen: Regionale Gegebenheiten sollten für Freikühlkonzepte genutzt werden, um den energetischen Fußabdruck zu minimieren.
- Zukunftssichere Dimensionierung: Kühlanlagen sollten so kompakt wie möglich, aber modular erweiterbar geplant werden. So wird wertvolle Fläche im Gebäude nicht verschwendet, während gleichzeitig mit wachsenden IT-Anforderungen Schritt gehalten werden kann.
- Nachhaltige Kältemittel: Der Wechsel zu modernen Kältemitteln mit geringem Treibhauspotenzial (Low-GWP) ist ein wichtiger Schritt, um Nachhaltigkeitsziele zu erreichen und rechtliche Vorgaben einzuhalten.

Fazit: Mix führt zum Ziel

Die hochverfügbare und gleichzeitig effiziente Kühlung von Krankenhaus-Rechenzentren ist eine komplexe Herausforderung, bietet aber enorme Chancen. Durch die enge Verzahnung von IT-Infrastruktur und klinischer Gebäudetechnik lassen sich wertvolle Synergien heben. Setzen Verantwortliche auf einen intelligenten Mix aus Flüssigkeitskühlung, Freikühlung und konsequenter Abwärmenutzung, sind sie auf der sicheren Seite. Sie gewährleisten nicht nur den Klinikbetrieb von morgen, sondern tragen auch messbar zum Klimaschutz bei.

Zu beachten ist auch, dass der Bedarf an Rechenleistung durch den zunehmenden Einsatz künstlicher Intelligenz (KI) im Krankenhaus-Umfeld enorm wächst. Um mit dieser Entwicklung Schritt zu halten, lohnt sich die Investition in skalierbare Kühlungslösungen. Sie erfüllen die Anforderungen von heute und leisten gleichzeitig einen wichtigen Beitrag zur positiven Bilanz einer Anlage in der Zukunft.

Autor:

Frank Krause,
Sales Manager
Data Center, Carrier
Klimatechnik GmbH

Kontakt:

Carrier Klimatechnik GmbH
Stefanie Machauf
Parkring 33
85748 Garching
Tel.: +49 89 32154-203
stefanie.machauf@carrier.com
www.carrier.de