«Datenschutzrechtliche Fragen sind noch nicht vollständig geklärt»

Kommunikationssysteme in Spitälern wandeln sich und bergen Risiken. Welche das sind, verraten Drazen-Ivan Andjelic, General Manager Alpine bei Mitel, Klaus Späth, CIO Spital STS Thun, und Carmelo Salmeri, Senior Account Manager und Fachspezialist Healthcare bei UMB. Interview: Tanja Mettauer

Das Spital STS Thun setzt als vormaliger Unify- und neu Mitel-Kunde seit vielen Jahren auf UCC-Lösungen. Welche speziellen Anforderungen müssen Kommunikationssysteme in Spitälern erfüllen?

Drazen-Ivan Andjelic: Der Healthcare-Sektor stellt vielfältige und mit die höchsten Anforderungen an UCC-Produkte und UCC-Services. Effiziente und schnelle Prozesse sind entscheidend für die professionelle Patientenpflege. Ein klinikweites mobiles Kommunikationssystem mit verschiedenen Endgeräten für alle Bereiche des Klinikpersonals stellt geschützte Echtzeitkommunikation bereit. Es dient ausserdem als abhörsicheres Alarmierungs- und Ortungssystem – bis hin zur gesicherten virtuellen Ferndiagnostik. Dabei sind Sicherheitsaspekte zum Schutz von Patientendaten von grösster Bedeutung. Viele Betreiber steigern die Attraktivität ihres Angebots durch den Mix mit Lösungen für weniger hohen Sicherheitsbedarf, wie etwa Besucher-Internetzugänge und Patienten-Entertainmentsysteme.

Welche Strategie verfolgt das Spital STS Thun bei seinen Kommunikationsdiensten, welche Systeme stellen den reibungslosen Austausch sicher?

Klaus Späth: Wir sind vor über 20 Jahren von einer papierbasierten Krankenakte auf ein digitales Klinikinformationssystem umgestiegen und heute in den meisten Bereichen komplett digital unterwegs. Trotzdem ist für uns eine stabile und zuverlässige Telefonie, neben einem guten Netzwerk und einem ausfallsicheren Rechenzentrum, elementar wichtig. Wir haben mit Unify/Mitel eine Lösung gefunden, die besonders in den Bereichen Stabilität, Ausfallsicherheit und Integrationsfähigkeit punktet und damit hochverfügbare und redundante Telefonie-Services möglich macht. Zusätzlich haben wir Microsoft Teams für die interne Kommunikation im gesamten Verwaltungsbereich integriert. Im Bereich Patientenruf und Alarmierung nutzen wir Lösungen von Ascom, die vollständig integriert sind. In die Patiententelefonie und das -entertainment sind Unify-OpenScape-Healthstation-HiMed-Patiententerminals eingebunden. Als Endgeräte nutzen wir neben Unify- Telefonen spezielle Smartphones auf Basis von Ascom Myco.

Spitäler wie das STS nutzen verschiedene Kommunikationsdienste im Arbeitsalltag. Wie stellen Anbieter sicher, dass ihre Lösungen langfristig zum Einsatz kommen?

Drazen-Ivan Andjelic, General Manager Alpine, Mitel.

Andjelic: Kommunikationsprozesse durchlaufen immer unterschiedliche, ineinander verzahnte Anwendungen und Datenbanken – jeweils mit steigender Komplexität. Deshalb ist die Qualität der beteiligten Komponenten entscheidend und unterstreicht die Bedeutung der Bereitstellung zukunftssicherer und sich entwickelnder Lösungen. So wird etwa bei der virtuellen Ferndiagnostik die Patientenhistorie aus dem Krankenhausinformationssystem genutzt und entsprechend um den aktuellen Befund ergänzt. Diese Optimierung kann nur langfristig wirken, da solche Integrationen oft zu kostenintensiv sind, um beteiligte Komponenten in kurzen Zeitabständen wieder auszutauschen.

Spitäler zählen zu den kritischen Infrastrukturen und somit zu den am stärksten regulierten Umgebungen. Welche Bereitstellungsoptionen bieten Sie Gesundheitseinrichtungen?

Andjelic: Die im Healthcare-Umfeld nach wie vor bevorzugte Bereitstellungsoption ist On-Premise. Für Arbeitsplatzmodelle, die zwingend einen Public-Cloud-Lösungsbestandteil benötigen, bietet Mitel eine gesicherte Anbindung an die On-Premise-Infrastruktur. So werden in der Verwaltung Arbeitsplätze mit Microsoft Teams aus der Public Cloud ausgestattet und mit der lokalen UC-/Voice-Plattform für die Patientenkommunikation inklusive Alarmierung und Ortung verbunden.

Um sich in die Systeme von Unternehmen einzuschleichen, nutzen Cyberkriminelle verschiedene Mittel und Wege. Wie können Spitäler ihre (Kommunikations-)Systeme effizient absichern?

Carmelo Salmeri: Um sich vor Cyberangriffen zu schützen, können Spitäler verschiedene Massnahmen ergreifen:

- Endpoint Security: Mit «Endpoint Detection and Response»-Lösungen (EDR) können sie verdächtiges Verhalten auf Endgeräten erkennen und entsprechend handeln. Die Endpunkte müssen rund um die Uhr überwacht werden, denn Cyberkriminelle kennen keine Ferien oder Feiertage.
- Cyber Defense Center (CDC): Die Etablierung eines CDC kann eine zentrale Stelle für die Überwachung, Analyse und Reaktion auf Sicherheitsvorfälle bieten.
- SIEM (Security Information and Event Management): Dank Technologien wie SIEM können verdächtige Aktivitäten in Echtzeit identifiziert und Massnahmen ergriffen werden.
- Schulungen und Sensibilisierung: Mitarbeitende müssen regelmässig geschult werden. So können sie Phishing-Angriffe oder andere Social-Engineering-Techniken leichter erkennen und angemessen darauf reagieren.

Wie unterstützen Kommunikationsausrüster ihre Kunden in Sachen Geräte-Security?

Andjelic: Mobile Geräte gewinnen an Bedeutung, weil mit ihnen Informationen effizienter und schneller ausgetauscht werden können. Deshalb sind typische Sicherheitselemente wie die Sprach- und Signalisierungsdaten-Verschlüsselung auf dem Verbindungsweg und systemseitig «at rest» obligatorisch. Für die Systemanmeldung wird bei Lösungen von Mitel eine Zwei-Faktor-Authentifizierung genutzt, um Datenmissbrauch zu vermeiden. Dieser Sachverhalt ermöglicht einen Wandel vom «festen» Arbeitsplatz hin zum vollständig mobilen Arbeitsplatz. Jedoch ist das nicht bei allen Arbeitsplatzprofilen möglich, sodass es gilt, alle Arbeitsplatzrollen medienbruchfrei miteinander zu verbinden.

Wie schützt sich das Spital STS vor Hackerangriffen?

Späth: Hackerangriffe auf Spitäler sind mittlerweile leider fast schon Standard. Neben den klassischen Schutzmechanismen wie Firewall oder Antivirensystemen versuchen wir, Hackern zunehmend weniger Angriffsflächen zu bieten. Dabei setzen wir auf ein stark segmentiertes Netzwerk und nutzen Network Access Control (NAC). Wir haben strenge Passwortrichtlinien mit Multi-Faktor-Authentisierung, betreiben Security Information and Event Management (SIEM) und Security Operations Center (SOC). Zudem ist ein sehr gutes Patch- und Vulnerability-Management implementiert. Des Weiteren gehen wir mit dem Engagement von ethischen Hackern einen eher unkonventionellen Weg. Organisationen, wie etwa Bug Bounty Switzerland, vermitteln «gute» Hacker («White Hacker») und simulieren mit ihnen einen realen Angriff auf unsere Infrastruktur. Werden Schwachstellen entdeckt, erhalten die Hacker ein Preisgeld – abhängig von der Kritikalität der gefundenen Sicherheitslücke.

Klaus Späth, CIO, Spital STS Thun.

Von welchen Hackerangriffen werden Spitäler am häufigsten bedroht?

Salmeri: Ransomware-Angriffe sind mitunter eine der grössten Bedrohungen für Spitäler. Bei diesen Angriffen verschlüsseln Angreifer die Daten des Spitals und verlangen von ihnen ein Lösegeld, um die Daten wieder freizugeben. Ransomware kann den Betrieb von Spitälern stark beeinträchtigen und die Patientenversorgung gefährden. Zudem sind Phishing-Angriffe weit verbreitet und zielen häufig auf Mitarbeitende ab. Aber nicht alle Bedrohungen kommen von aussen. Interne Bedrohungen, sei es durch versehentliches oder absichtliches Fehlverhalten von Mitarbeitenden, können ebenfalls ernsthafte Auswirkungen haben – etwa in Form von Datendiebstählen oder Beschädigungen von Systemen.

Cyberkriminelle machen sich auch KI-Funktionen zunutze. Welche Bedrohung stellen etwa Deep Fakes für Spitäler dar?

Salmeri: Stehlen Angreifer die Identität von medizinischem Personal, könnten sie sich damit in Systeme einschleusen oder schädliche Aktionen wie Erpressungsversuche in ihrem Namen ausüben. Mithilfe von Deep Fakes sind Kriminelle ebenfalls fähig, falsche Informationen über medizinische Behandlungen, Krankheiten oder Gesundheitsrisiken zu verbreiten. Dies könnte Verwirrung unter Patientinnen und Patienten stiften und ihr Vertrauen in das Gesundheitssystem untergraben. Darüber hinaus können Kriminelle Deep Fakes verwenden, um etwa Röntgenaufnahmen oder CT-Scans zu manipulieren und so Befunde vortäuschen. Solche Manipulationen könnten zu falschen Diagnosen führen und letztlich die Gesundheit von Patientinnen und Patienten gefährden.

Intelligente Assistenten kommen in immer mehr Bereichen zum Einsatz. Wo greift das Spital STS bereits auf KI-Assistenten zurück?

Späth: Eine der grössten Stärken der KI ist die Mustererkennung. In der Radiologie kommt die Technologie seit mehreren Jahren

Carmelo Salmeri, Senior Account Manager, UMB.

zum Einsatz. Intelligente Assistenten machen eine ärztliche Diagnose keineswegs überflüssig, sondern unterstützen Ärztinnen und Ärzte bei der Priorisierung ihrer Arbeiten. Diagnostiziert die KI einen pathologischen Befund, erhält diese Untersuchung höchste Priorität. So stellen wir sicher, dass kritische Diagnosen innerhalb sehr kurzer Zeit vorliegen und sowohl von der KI wie auch vom Radiologen verifiziert wurden. Andere Einsatzgebiete für KI sind etwa die Personaleinsatzplanung oder die Optimierung unseres OP-Programms. Künstliche Intelligenz kann auch bei Patientenanrufen in Form von Chatbots oder in Verbindung mit dem Operationssystem Da Vinci genutzt werden. Einige Einsatzbereiche sind zwar noch im Testbetrieb. Aber ich bin sicher, wir werden einen Grossteil in den nächsten Jahren fest in unsere Arbeitsprozesse integrieren können.

Microsofts KI-Assistent Copilot kann grundsätzlich auf alle Daten zugreifen, die für ihn freigegeben wurden. Wie handhabt das STS den Umgang mit dem Copilot?

Späth: Wir testen Microsoft Copilot im Zusammenhang mit der Einführung unseres neuen Intranets und unserer neuen Kollaborationsplattform auf Basis MS-Teams. Bisher war das Finden von internen Dateien wie etwa Reglementen oder Weisungen für die Patientenbehandlung sehr mühsam und zeitintensiv. Copilot findet innert wenigen Sekunden die richtige Antwort in den gespeicherten Dokumenten. Zur Absicherung soll Copilot zudem das Dokument anzeigen, in dem er die Information gefunden hat. So erhalten die Mitarbeitenden viel schneller die passende Antwort und können zudem überprüfen, ob es sich um das korrekte Dokument handelt. Leider sind die datenschutzrechtlichen Fragen noch nicht vollständig geklärt und es wird bis zum produktiven Einsatz noch einige Tests und Abklärungen brauchen.

Wie kann künstliche Intelligenz die Kommunikation in Spitälern unterstützen?

Salmeri: Ein Einsatzgebiet ist etwa die Spracherkennungsfunktion für medizinische Dokumentationen. KI-Assistenten helfen dem medizinischen Personal dabei, schneller und effizienter Berichte oder Patientenakten zu erstellen, indem gesprochene Informationen in Text umgewandelt werden. Chatbots unterstützen Spitäler in der Patientenkommunikation, indem sie vielgestellte Fragen automatisiert beantworten – sei es zu Behandlungen, Medikamenten oder zum Aufenthalt.

Wo setzen Kommunikationsausrüster KI-Lösungen bereits erfolgreich ein?

Andjelic: Eingesetzt wird die KI etwa in der virtuellen Telemedizin zur Terminvereinbarung im virtuellen Wartezimmer sowie zur Diagnostikunterstützung oder um vordefinierte und standardisierte Befunde auszustellen. Ein nächster Meilenstein wird sein, Bilderkennung und -referenzierung zur Symptomdefinition und Krankheitsermittlung zu nutzen.

Was sollten Unternehmen beim Umgang mit KI und insbesondere mit generativer KI berücksichtigen?

Salmeri: Alle eingesetzten KI-Anwendungen müssen mit den geltenden Gesetzen und Vorschriften im Einklang sein. Des Weiteren müssen alle Daten, die in der Entwicklung oder im Betrieb der KI-Systeme zur Anwendung kommen, angemessen geschützt sein und urheberrechtliche Aspekte berücksichtigen. GenAI-Modelle neigen noch dazu, unvorhergesehene Ergebnisse oder fehlerhafte Resultate zu liefern. Strenge Qualitätssicherungsmassnahmen sind deshalb unabdingbar. Spitäler sollten deshalb Auswirkungen und potenzielle Risiken vor der Implementierung sorgfältig analysieren und Massnahmen zur Risikominimierung ergreifen. Diese können die Entwicklung von Notfallplänen, die regelmässige Überprüfung von KI-Systemen und die Zusammenarbeit mit Experten für Cybersicherheit und Risikomanagement umfassen.

Welche Bedenken hat das STS hinsichtlich Datenschutz und Vertraulichkeit beim Einsatz von KI?

Späth: Uns ist ein ausgewogener Ansatz wichtig, der die Vorteile von KI nutzt, gleichzeitig aber die Privatsphäre und Vertraulichkeit der Benutzer maximal schützt. Da es sich bei KI-Systemen in der Regel um cloudbasierte Anwendungen handelt, reicht es nicht aus, dass wir unsere Systeme sicher aufsetzen und im Griff haben. Wir müssen auch die Sicherheitsstandards unserer Cloud-Anbieter überwachen. Die beste Sicherheit ergibt sich aus unserer Erfahrung dann, wenn der Datenschutz bereits bei der Entwicklung der KI-Systeme berücksichtigt wurde. Ein letzter Punkt ist die missbräuchliche Verwendung der Daten. Nutzerinnen und Nutzer müssen sich darauf verlassen können, dass die Daten ausschliesslich für den angegebenen Zweck verwendet werden. Hier ist insbesondere der Gesetzgeber gefordert und muss klare Richtlinien und Gesetze erlassen, um den Datenschutz im KI-Bereich zu gewährleisten.

Den vollständigen Artikel finden Sie online
www.netzwoche.ch