XM Cyber | Case Study

# Kontinuierliche Sichtbarkeit: wie XM Cyber das Vertrauen der Patienten im gesamten Netzwerk der Sana Kliniken schützt


## Die Herausforderung

### Das Vertrauen der Patienten in einer streng regulierten digitalen Landschaft schützen

Die Sana Kliniken AG ist einer der größten Gesundheitsdienstleister in Deutschland mit einem großen Netzwerk aus rund 50 Kliniken, 58 Medizinischen Versorgungszentren und weiteren Gesundheitsdiensten. Mit über 40.000 Mitarbeitenden verbindet das bundesweite Netzwerk des Unternehmens Krankenhäuser, Sanitätshäuser und weitere ambulante Einrichtungen, die entscheidend auf den ständigen Zugriff auf genaue und sichere Patientendaten angewiesen sind.

Das Gesundheitswesen in Europa unterliegt einem der anspruchsvollsten regulatorischen Rahmenbedingungen der Welt. Strenge Datenschutzgesetze, fest vereinbarte Preise und komplexe Compliance-Regeln erschweren Modernisierungen und IT-Investitionen besonders. Folglich sind viele Krankenhäuser noch auf isolierte Legacy-Systeme angewiesen, die Schwierigkeiten haben, Daten effizient zu wachsen. CEO Thomas Lemke beschreibt eine zentrale Herausforderung der Branche: „Was den Grad der Digitalisierung und den Einsatz moderner und vernetzter Tools angeht, hat das Gesundheitswesen erheblichen Nachholbedarf."

Um sicher zu modernisieren, mussten die Sana Kliniken diese Hürden überwinden und eine belastbare, richtlinienkonforme IT-Basis schaffen, die sowohl sensible Patientendaten schützt, als auch den reibungslosen Betrieb jeder Einrichtung gewährleistet.

## Die Lösung

### Durchgängige, pragmatische Cybersicherheit über kritische Systeme hinweg

Die Sana Kliniken haben sich für die XM Cyber Continuous-Expositions-Management-Plattform entschieden, die in der souveränen STACKIT Cloud ausgeführt wird, um die Transparenz und Ausfallsicherheit in ihren komplexen Klinik- und IT-Umgebungen deutlich zu stärken. Die Plattform bildet kontinuierlich potenzielle Gefährdungspfade ab und erkennt Schwachstellen, die interne Systeme mit externen Bedrohungen verbinden könnten. „Kein einziges Blatt Papier, keine Richtlinie und kein IT-Zertifikat helfen uns wirklich dabei, Cyberrisiken zu minimieren und uns davor zu schützen." Wer sich einzig darauf verlässt, formale Vorgaben als Mindeststandard zu erfüllen, handelt nicht im Sinne des Gemeinwesens. Sana vertritt daher die klare Haltung, dass Sicherheit aktiv und kontinuierlich im "Maschinenraum" der IT gelebt werden muss.

Der Angriffsgraph von XM Cyber deckt kritische Offenlegungen im Ökosystem der Sana Kliniken in Echtzeit auf. Insbesondere werden Risiken im Zusammenhang mit Medizingerätenetzwerken und Fernwartungspflichtanbindungen thematisiert. Vor allem ermöglicht die Lösung es den Teams von Sana, die Fehlerbehebungen zu priorisieren, die am wichtigsten sind, ohne die grundlegende Patientenversorgung zu unterbrechen.

sana

**Kunde:**

Sana Kliniken AG

**Branche:**

Gesundheitswesen

**Standort:**

Deutschland

**Herausforderung:**

Schutz sensibler Gesundheitsdaten und Gewährleistung der Kontinuität in einem komplexen, streng regulierten klinischen Netzwerk.

**Lösung:**

XM Cyber Exposure-Management-Plattform auf der STACKIT-Infrastruktur.

**Ergebnisse:**

Kontinuierliche Transparenz, proaktive Prävention und ein souveräner Rahmen für die sichere digitale Transformation.

## Vorteile und Ergebnisse

### Belastbarkeit, Sichtbarkeit und Bereitschaft für kritische Ereignisse

Mit XM Cyber erhalten die Sana Kliniken eine integrierte Live-Übersicht der Bedrohungen in ihrem landesweiten Netzwerk. Durch die Hervorhebung von Gefährdungen mit hohen Auswirkungen hilft es der IT-Organisation, kostspielige Ausfälle proaktiv zu verhindern und die Betriebskontinuität für über 200 Betriebseinheiten aufrechtzuerhalten. Thomas Lemke formulierte XM Cyber nicht als Luxus, sondern als essenzielle Infrastruktur: „Es ist eine lebensnotwendige Ader, die wir benötigen, um das System am Laufen zu halten."

Die Plattform ermöglicht eine schnellere Identifizierung von Schwachstellen, unterstützt eine koordinierte Reaktion auf Vorfälle in allen Einrichtungen und ermöglicht eine messbare Reduzierung der Gesamtexpositionsrisiken. Die Teams von Sana können jetzt handeln, bevor Risiken zu großen Vorfällen eskalieren, um sowohl Patienten als auch wichtige Betriebsabläufe zu schützen.

## Ausblick:

### Digitale Souveränität als Bedingung für Innovation

Thomas Lemke betrachtet Souveränität nicht als Sahnehäubchen, sondern als Grundvoraussetzung für Fortschritt im Gesundheitswesen. Der Betrieb von XM Cyber auf STACKIT stellt sicher, dass sensible Patientendaten entsprechend der DSGVO behandelt werden. Dies unterstützt das strategische Ziel einer sicheren digitalen Unabhängigkeit. „Es ist nicht nur eine hinreichende, sondern eine notwendige Bedingung, Partner zu finden, die dieses Grundbedürfnis aufnehmen und Lösungen anbieten und so, von Deutschland aus, die Unabhängigkeit in diesen ursprünglichen Dienstleistungen zu verankern", sagt Thomas Lemke.

Auf dieser Grundlage können die Sana Kliniken die digitale Versorgung in sicherer Art und Weise weiter ausbauen und erfolgreich Innovationen mit der vollen Kontrolle über ihre Systeme, Daten und das Vertrauen der Patienten zu verbinden.

## Key Outcomes

- **Kontinuierliches Monitoring über Klinik- und IT-Systeme**
- **Früherkennung und Priorisierung von Risiko- Exposures**
- **Einhaltung europäischer Datenschutz- und Souveränitätsstandards**
- **Stärkere Ausfallsicherheit und operative Kontinuität an 200 Standorten**
- **Sicheres Fundament für die weitere digitale Transformati**