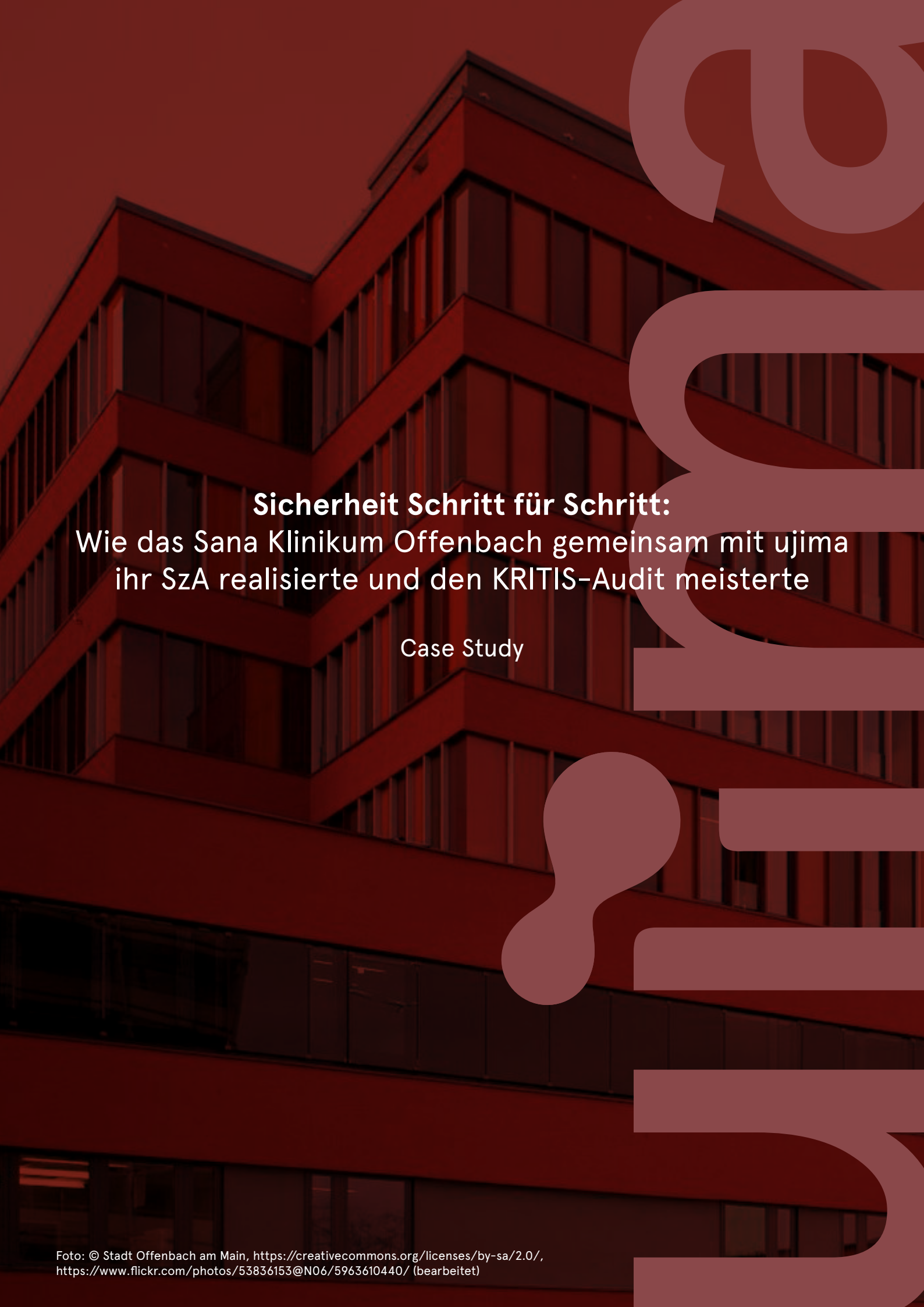

Sicherheit Schritt für Schritt:
Wie das Sana Klinikum Offenbach gemeinsam mit ujima ihr SzA realisierte und den KRITIS-Audit meisterte

Case Study

Projekt-Timeline im Überblick

05/2024
Ausschreibungsstart des Sana Klinikum Offenbach

06-07/2024
Teilnahme und Gewinn der Ausschreibung durch ujima

10/2024
Projektstart, Onboarding

12/2024 – 02/2025
Umsetzung der Kernsysteme, Anbindung von ca. 100 Logquellen, System-Tuning

02/2025
Erfolgreicher KRITIS-Audit, begleitet durch ujima

04/2025
Abschluss der Projektphase, Übergang in den 24/7-Regelbetrieb

Einleitung

Als Einrichtung der Kritischen Infrastruktur ist das Sana Klinikum Offenbach gesetzlich verpflichtet, ein oder mehrere Systeme zur Angriffsabwehr (SzA) zu betreiben – mit Fokus auf Patientensicherheit, Behandlungseffektivität und die Absicherung der kritischen Dienstleistung.

Gemeinsam mit ujima gelang es, innerhalb weniger Monate ein zentrales SOC/SIEM-System aufzubauen, den Betrieb sicherzustellen und den anstehenden KRITIS-Audit erfolgreich zu bestehen. Die partnerschaftliche Zusammenarbeit zeigte: Gesetzliche Anforderungen lassen sich strukturiert, realistisch und praxisnah umsetzen.

Kundenprofil

Das Sana Klinikum Offenbach ist eines der größten Krankenhäuser in Hessen und zählt als Maximalversorger zur Spitzenklasse der medizinischen Versorgung im Rhein-Main-Gebiet. Mit rund 900 Betten und jährlich 39.000 stationären und 74.000 ambulanten Patient:innen bietet das Haus ein umfassendes medizinisches Leistungsspektrum. Als akademisches Lehrkrankenhaus der Johann Wolfgang Goethe-Universität Frankfurt beschäftigt das Klinikum rund 2.800 Mitarbeitende und ist Teil der Sana Kliniken AG, einem der größten privaten Klinikverbunde Deutschlands.

Das Sana Klinikum Offenbach wurde im Rahmen der KRITIS-Verordnung als Betreiber kritischer Infrastruktur eingestuft. Damit trägt die Klinik eine besondere Verantwortung für die Absicherung der medizinischen Versorgung und unterliegt strengen gesetzlichen Anforderungen an die IT-Sicherheit, insbesondere gemäß §8a BSIG.

Als Gesundheitsdienstleister mit Fokus auf die kritische medizinische Versorgung muss die Sana Klinik nicht nur die Patientensicherheit gewährleisten, sondern auch nachweisbar sicherstellen, dass Angriffe auf IT-Systeme frühzeitig erkannt, bewertet und abgewehrt werden. Besonderer Fokus liegt dabei auf den Systemen der sogenannten kritischen Dienstleistung (kDL), die für den reibungslosen Betrieb der Versorgung unverzichtbar sind.

Foto: © Sana Klinikum Offenbach GmbH

Ausgangslage und Herausforderung

Der Krankenhaussektor steht weiterhin vor der großen Herausforderung, mit begrenzten finanziellen und personellen Ressourcen den zurecht hohen Sicherheitsanforderungen gerecht zu werden und diese dauerhaft aufrechterhalten zu müssen. Besonders im Gesundheitswesen ist die Diskrepanz zwischen den Anforderungen an die IT-Sicherheit und den verfügbaren Mitteln deutlich spürbar. Die große Vielfalt und Komplexität der IT-Landschaft eines Krankenhauses stellt eine zusätzliche Herausforderung dar, insbesondere vor dem Hintergrund des operativen Tagesgeschäfts.

Zitat IT-Leiter Sana Klinikum Offenbach Marcus Schmidt:
„Immer wieder treffen Anforderungen ein, die eine Umsetzung erwarten, ohne den technischen und wirtschaftlichen Kontext realistisch zu bewerten – etwa die Vorstellung, veraltete Medizintechnik ohne Weiteres in moderne IT-Sicherheitskonzepte zu integrieren. Solche Altgeräte, beispielsweise 10 Jahre alte Ultraschallgeräte, stellen ein erhebliches Risiko dar und müssen häufig außer Betrieb genommen oder durch Neuinvestitionen ersetzt werden."

Im Wesentlichen stand die Sana Klinik vor Projektbeginn vor den folgenden Herausforderungen bezogen auf die Cybersicherheit:

Es fehlte eine zentrale, leistungsfähige Lösung zur frühzeitigen Bedrohungserkennung und zur Überwachung der kritischen Systeme in Echtzeit.

Der nächste KRITIS-Audit war bereits für Februar 2025 fest terminiert. Somit musste die Umsetzung des SzA innerhalb weniger Monate erfolgen.

Begrenzte interne Ressourcen boten keine Grundlage für einen eigenen effektiven 24/7-Sicherheitsbetrieb und erforderten externe Unterstützung beim Aufbau und Betrieb eines SOC/SIEM. Die bestehende Infrastruktur war nicht auf die Anforderungen eines modernen Systems zur Angriffsabwehr ausgerichtet.

Zitat IT-Leiter Sana Klinikum Offenbach Marcus Schmidt:
„Ein eigenes Security Operations Center (SOC) nützt wenig, wenn im Ernstfall – etwa bei einem sicherheitsrelevanten Vorfall um 23:15 Uhr – nur eine eingeschränkte Erreichbarkeit vorliegt, weil viele IT-Mitarbeitende sich im wohlverdienten Wochenende befinden. Genau an diesem Punkt wird deutlich, warum ein durchgängig verfügbarer Sicherheitsbetrieb für uns unverzichtbar ist."

Der Fokus lag bewusst auf einer praxistauglichen, risikobasierten Absicherung – nicht maximale Technik, sondern gezielte Schutzmaßnahmen für die Systeme der kDL.

Um die gesetzlichen Vorgaben zuverlässig zu erfüllen und die Anforderungen für den nächsten KRITIS-Audit zu bestehen, startete das Sana Klinikum Offenbach im Sommer 2024 ein formales Ausschreibungsverfahren. ujima konnte im Vergabeverfahren überzeugen. Das Konzept von ujima setzte gezielt auf eine pragmatische, schrittweise Umsetzung der gesetzlichen Anforderungen und stimmte inhaltlich mit den definierten Vorgaben der Sana Klinik überein.

Zitat IT-Leiter Sana Klinikum Offenbach Marcus Schmidt:
„Wir haben einen Partner mit echter Krankenhauserfahrung gesucht – und das auf einem gewissen Niveau, jemanden, der die Komplexität größerer Häuser kennt. Unserem ujima-Projektmanager muss man nicht erst erklären, was ein KIS oder ein PACS ist. Er weiß, wie die Hersteller ticken und welche Herausforderungen mit neuer Medizintechnik realistisch auf uns zukommen."

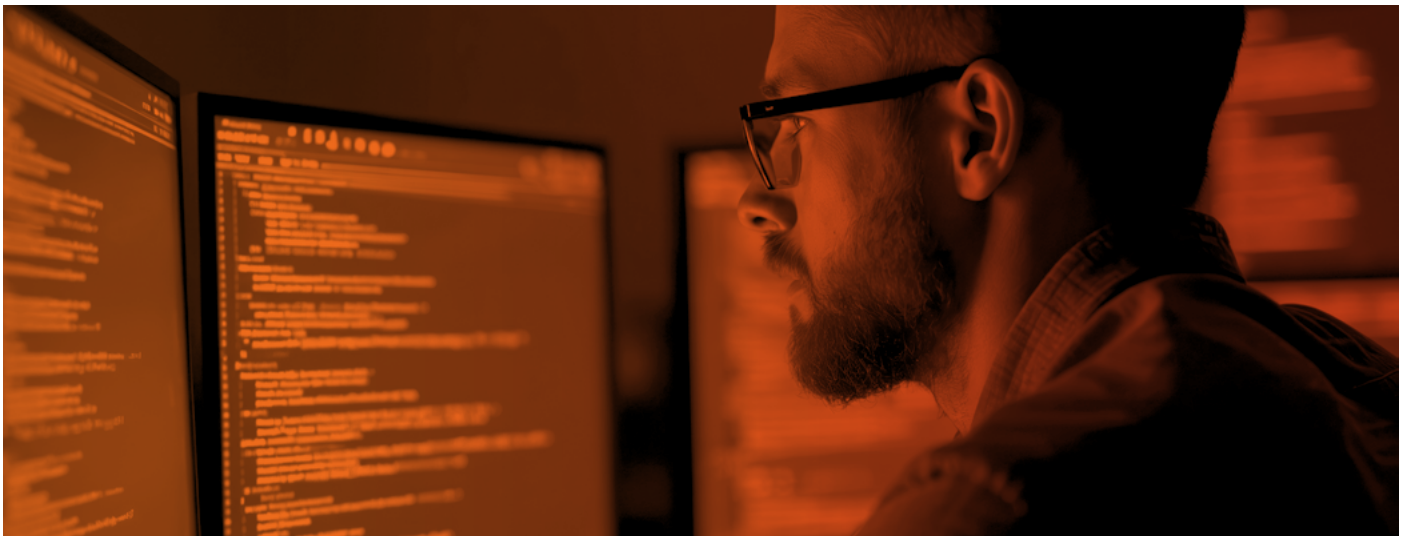

Foto: © Vadym / Adobe Stock

Lösung und Implementierung

Das Vorgehensmodell von ujima basiert auf einem strukturierten 5-Phasen-Ansatz, der gezielt auf die Anforderungen von KRITIS-Betreibern ausgerichtet ist:

1. Probebetrieb mit Basis-Use-Cases
(bei der Sana Klinik übersprungen,
da ein unmittelbarer Produktivstart gewünscht war)

2. GAP-Analyse & kDL-Definition
(an die Bedürfnisse der Sana Klinik angepasst als gezielte Überprüfung der Systeme der kritischen Dienstleistung)

3. Technischer Rollout, Betriebsaufbau, Prozess- und Eskalationsdefinitionen, Logquellenanbindung, Regeltuning und -optimierung

4. SOC/SIEM-Regelbetrieb (24/7/365)

5. Erweiterung der Log-Quellenanbindung, Optimierung & Umsetzungsgrad-Entwicklung
(UG 4 & UG 5 gemäß BSI OH SzA, NIS 2.0,
EU Cyber Resilience Act) (in Progress)

Die Einführung der SOC/SIEM-Lösung erfolgte bewusst in mehreren klar strukturierten Stufen, die sich am Umsetzungsgrad-Modell orientieren. In der ersten Ausbaustufe wurde gezielt Umsetzungsgrad 3 angesetzt, mit dem Fokus auf den Schutz der kritischen Systeme auf Betriebssystemebene. Die Umsetzung konzentrierte sich dabei zunächst auf rund 100 definierte IT-Systeme, die zur kritischen Dienstleistung (kDL) der Klinik gehören. Das Sana Klinikum Offenbach legte den Umfang dieser Systeme eigenverantwortlich fest, während ujima den Auswahlprozess beratend unterstützte.

Zitat IT-Leiter Sana Klinikum Offenbach Marcus Schmidt:
„Im Krankenhausumfeld wird oft schnell von großen Strategien und Zielen gesprochen, aber ich bin eher der Meinung, dass man zunächst kleine Schritte machen sollte, um zu sehen, wie etwas funktioniert, und dann kann man sukzessive die Dinge weiterentwickeln. Das hat auch unser ujima-Projektmanager bestätigt, dass viele ihrer Krankenhaus-Kunden diesen Ansatz verfolgen; genauso wie der Kreis der Krankenhäuser, der sich über die DKG-Zirkel getroffen hat."

Foto: © Sana Klinikum Offenbach GmbH

Ergebnisse und Mehrwerte

Die Zusammenarbeit zwischen dem Sana Klinikum Offenbach und ujima führte in kurzer Zeit zu messbaren Erfolgen und einer zukunftssicheren Sicherheitsarchitektur:

Schnelle Absicherung
Bereits innerhalb von drei Monaten wurde die technische Basis für das System zur Angriffsabwehr (SzA) geschaffen und rund 100 kritische Systeme erfolgreich angebunden. Seit April 2025 läuft das SOC/SIEM stabil im 24/7-Regelbetrieb, inklusive kontinuierlicher Bedrohungsüberwachung.

Zukunftssichere Skalierbarkeit
Durch den bewusst gewählten Einstieg über Umsetzungsgrad 3 auf Betriebssystemebene konnten Überlastung und unnötige Komplexität gezielt vermieden werden. Die weiteren Entwicklungsschritte sind planvoll vorbereitet. SOC/SIEM ist kein Sprint, es ist ein Marathon und setzt auch einen kontinuierlichen Entwicklungsprozess, der den Anforderungen des Unternehmens folgt, voraus.

Transparenz & Betriebssicherheit
Die Umsetzung des Projekts erfolgte von Beginn an mit einem klar definierten Umfang und konsequentem Fokus auf die Systeme der kDL – technische Maßnahmen, die gezielt die Patientensicherheit und Behandlungseffektivität unterstützen. Ergänzt durch das strukturierte Stufenmodell und kontinuierliches System-Tuning, wurde eine optimierte Sicherheitslage geschaffen.

Audit-Erfolg
Die Sana Klinik bestand den gesetzlich vorgeschriebenen KRITIS-Audit im Februar 2025 erfolgreich. ujima war als technischer Ansprechpartner direkt eingebunden und begleitete aktiv die Auditvorbereitung und den Termin.

Zitat IT-Leiter Sana Klinikum Offenbach Marcus Schmidt: *„Manche Institutionen versuchen direkt Umsetzungsgrad 5 zu erreichen und scheitern an der Komplexität. Die stufenweise Einführung mit Fokus auf das Wesentliche ist der richtige Weg – das bestätigte auch unser Auditor."*

Zukunftsausblick und weiterführende Zusammenarbeit

Das Sana Klinikum Offenbach steht nun vor den nächsten Entwicklungsschritten: Im Fokus steht die horizontale Erweiterung durch die Anbindung weiterer Systeme sowie die vertikale Erweiterung durch die Absicherung der Applikationsebene. Gleichzeitig beginnt die Vorbereitung auf die Umsetzungsgrade 4 und 5 im Hinblick auf den KRITIS-Audit 2027. Der Fortschritt muss dabei klar erkennbar sein.

Die zweite Jahreshälfte 2025 wird genutzt, um gemeinsam mit ujima die nächsten Schritte im Detail zu planen, unter Berücksichtigung von Ressourcen, Zeitrahmen und wirtschaftlichen Bedingungen. ujima bleibt strategischer Partner und begleitet die Sana Klinik weiterhin bei der Optimierung und Absicherung ihrer kritischen Infrastruktur.

Zitat IT-Leiter Sana Klinikum Offenbach Marcus Schmidt:
„Die Zusammenarbeit ist offen, direkt und auf Augenhöhe – genau so, wie wir uns das gewünscht haben. Es gibt persönliche Ansprechpartner, kurze Wege und einen ehrlichen, verlässlichen Austausch über das, was gut läuft oder was noch gemeinsam erarbeitet werden muss. Das schafft Vertrauen und bringt alle weiter. Für uns hat sich bestätigt: Wir haben den richtigen Partner gefunden."

Schlussfolgerung

Das Projekt mit dem Sana Klinikum Offenbach zeigt: Mit ujima lassen sich gesetzliche Anforderungen nicht nur erfüllen, sondern sinnvoll ins medizinische Umfeld integrieren. Durch ein realistisches, strukturiertes Vorgehen wurde nicht nur die gesetzliche KRITIS-Konformität erreicht, sondern eine zukunftssichere IT-Sicherheitsstrategie geschaffen. Und diese Strategien lassen sich jederzeit auch auf Unternehmen mit dem gleichen Mehrwert anwenden, die nicht direkt der KRITIS- oder NIS-2-Verordnung unterliegen.

Möchten auch Sie ein praxiserprobtes, gesetzeskonformes SOC/SIEM Schritt für Schritt, partnerschaftlich und audittauglich umsetzen?

Sprechen Sie uns an. Gemeinsam sichern wir Ihre kritischen Dienste.

ujima GmbH
Kennedyallee 93 \\ 60596 Frankfurt

\\ +49 69 15322793-0
\\ info@ujima.de
\\ www.ujima.de

Allianz für Cyber-Sicherheit
Teilnehmer

Stand: November 2025