KUNDEN CASE STUDY

Sicherer Klinikbetrieb rund um die Uhr: Wie der Gesundheitsverbund Landkreis Konstanz seine Cyberabwehr neu aufstellt

Mit einer zentralen Sicherheitsplattform und Managed Detection and Response stärkt der Klinikverbund Transparenz, Reaktionsfähigkeit und Compliance im laufenden Betrieb.

SOPHOS

Gesundheitsverbund Landkreis Konstanz

Gesundheitsverbund
Landkreis Konstanz
gemeinnützige GmbH

Industrie
Gesundheitswesen

Sophos-Partner
ACP IT Solutions GmbH

Sophos-Lösungen
Managed Detection and Response
Network Detection and Response
Mobile Security
Next-Gen Firewall

Mitarbeiter
3.700

Cyberangriffe auf Einrichtungen des Gesundheitswesens haben in den vergangenen Jahren deutlich zugenommen – mit potenziell dramatischen Folgen für Patientenversorgung und Betriebssicherheit. Krankenhäuser zählen zu den kritischsten Infrastrukturen überhaupt: Sie müssen rund um die Uhr funktionieren, verarbeiten hochsensible Daten und arbeiten oft mit historisch gewachsenen IT-Strukturen. Genau diese Mischung macht sie besonders anfällig. Vor diesem Hintergrund hat der Gesundheitsverbund Landkreis Konstanz seine IT-Sicherheitsstrategie grundlegend modernisiert – mit dem Ziel, Risiken zu minimieren und gleichzeitig die IT-Teams zu entlasten.

Die Herausforderung

Die IT-Landschaft des Gesundheitsverbunds ist geprägt von einer komplexen Hybridstruktur aus On-Premises-Systemen und cloudbasierten Anwendungen. Kritische Subsysteme wie Krankenhausinformationssysteme, Radiologie- und Laborsysteme sowie zahlreiche medizinische Geräte sind eng miteinander verzahnt und müssen hochverfügbar betrieben werden. „Unsere IT ist historisch gewachsen und weist die typische Komplexität eines kommunalen Krankenhauses auf – mit einer hohen Integrationsdichte und gleichzeitig sehr strengen Anforderungen an Verfügbarkeit und Sicherheit“, erklärt Tino Hartmann, Geschäftsbereichsleiter IT & Medizininformatik.

Angesichts steigender Bedrohungen, wachsender regulatorischer Anforderungen und begrenzter personeller Ressourcen wurde deutlich, dass die bestehende Sicherheitsarchitektur nicht mehr ausreichte. Es fehlte insbesondere an Transparenz über Endpunkte und Netzwerkaktivitäten sowie an einer zentralen Steuerung der Sicherheitsmaßnahmen. Ziel war daher eine ganzheitliche, skalierbare Lösung, die sowohl den Schutz sensibler Daten verbessert als auch die IT-Abteilung im Alltag entlastet.

Die Lösung

Mit der Einführung von Sophos Central und der Managed Detection and Response Complete Lösung entschied sich der Gesundheitsverbund für einen plattformbasierten Ansatz, der verschiedene Sicherheitsfunktionen in einer zentralen, cloudbasierten Oberfläche bündelt. Ein wesentliches Element ist dabei die automatisierte Zusammenarbeit zwischen Endpunkten, Servern und Netzwerkkomponenten, die Bedrohungen schneller erkennt und Gegenmaßnahmen einleitet. „Der automatische Informationsaustausch zwischen den Systemen ermöglicht es uns, Angriffe frühzeitig zu erkennen und kompromittierte Geräte sofort zu isolieren – das ist für unsere Umgebung ein echter Gamechanger“, so Hartmann.

„Der automatische Informationsaustausch zwischen den Systemen ermöglicht es uns, Angriffe frühzeitig zu erkennen und kompromittierte Geräte sofort zu isolieren – das ist für unsere Umgebung ein echter Gamechanger.“

Tino Hartmann, Geschäftsbereichsleiter IT & Medizininformatik

Die Implementierung stellte besondere Anforderungen, da viele medizinische Geräte nicht ohne Weiteres verändert oder gepatcht werden dürfen und der Klinikbetrieb zu keinem Zeitpunkt unterbrochen werden kann. Entsprechend erfolgte die Einführung schrittweise in definierten Wartungsfenstern und in enger Abstimmung mit Herstellern medizinischer Systeme. Trotz dieser Rahmenbedingungen konnte die neue Sicherheitslösung erfolgreich in die bestehende Infrastruktur integriert werden.

Das Ergebnis

Im täglichen Betrieb profitiert der Gesundheitsverbund heute von einer deutlich verbesserten Transparenz über alle IT-Systeme sowie von schnelleren Reaktionszeiten bei Sicherheitsvorfällen. Automatisierte Prozesse reduzieren den manuellen Aufwand und entlasten die IT-Teams spürbar, während gleichzeitig die Anforderungen an Compliance und Auditfähigkeit besser erfüllt werden.

„Wir haben heute nicht nur ein deutlich höheres Sicherheitsniveau, sondern auch die Gewissheit, kritische Prozesse stabil und geschützt betreiben zu können – und genau das ist im Krankenhausumfeld entscheidend“, resümiert Hartmann.

Der Partner ACP IT Solutions GmbH

Die ACP Group AG ist ein in Österreich gegründetes IT-Unternehmen mit mehr als 50 Standorten in der DACH-Region. Geschäftsbereiche sind die Errichtung und der Betrieb von IT-Infrastruktur, Softwarelösungen sowie dazugehörige Dienstleistungen. Kunden sind Unternehmen sowie Organisationen der öffentlichen Hand.

„Wir haben heute nicht nur ein deutlich höheres Sicherheitsniveau, sondern auch die Gewissheit, kritische Prozesse stabil und geschützt betreiben zu können – und genau das ist im Krankenhausumfeld entscheidend.“

Tino Hartmann, Geschäftsbereichsleiter IT & Medizininformatik

Mehr Informationen unter www.sophos.de

2026-05-20 CCS-DE (NP)