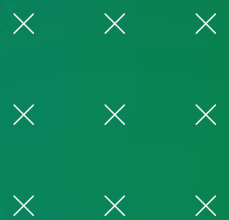




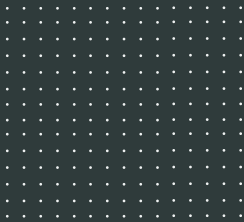
sure[secure]

DER HEALTHCARE- BEREICH IM FOKUS

*Warum die digitale Souveränität der Branche so
bedeutend ist und wie ein Managed SOC dabei hilft.*



Der Healthcare-Sektor ist keine Nische, sondern tragende Säule der Versorgung und einer der am dichtesten regulierten Bereiche Deutschlands. 1.841 Krankenhäuser versorgen jährlich rund 17,5 Mio. stationäre Patientinnen und Patienten und beschäftigen über 1,45 Millionen Menschen im ärztlichen und nichtärztlichen Dienst. Mit der NIS2-Umsetzung wächst der Kreis regulatorisch verpflichteter Einrichtungen bundesweit von rund 4.500 auf etwa 29.500, ein erheblicher Teil davon im Gesundheitswesen.



1.841

Krankenhäuser in
Deutschland (2024)

> 1,45 Mio.

Beschäftigte im ärztlichen
+ nichtärztlichen
Krankenhausdienst

472.900

aufgestellte Betten, davon
26.000 Intensivbetten

29.500

NIS2-pflichtige Einrichtungen
bundesweit (von zuvor ~4.500)



Gesetzlich verordnete Digitalisierung trifft auf gesetzlich verordnete Sicherheit

Mit dem Krankenhauszukunftsgesetz (KHZG) hat der Bund milliardenschwere Mittel für die digitale Modernisierung von Kliniken bereitgestellt. Verpflichtend sind dabei mindestens 15 % der geförderten Ausgaben für IT-Sicherheit. Seit Januar 2021 schreibt § 75c SGB V zudem allen Krankenhäusern in Deutschland eine Absicherung nach Stand der Technik vor, nicht mehr nur den großen KRITIS-Häusern.

Am 6. Dezember 2025 ist das NIS2-Umsetzungsgesetz in Kraft getreten. Es verpflichtet einen deutlich größeren Kreis von Einrichtungen zu Risikomanagement, Lieferkettensicherheit und einem gestuften Meldesystem: Erstmeldung innerhalb 24 Stunden, Bewertung innerhalb 72 Stunden, Abschlussbericht innerhalb eines Monats. Geschäftsführungen haften persönlich für die Umsetzung. Im März 2026 kam mit dem KRITIS-Dachgesetz eine zweite Ebene hinzu, die den physischen Schutz kritischer Anlagen regelt.

Einrichtungstyp	Regulatorischer Rahmen
Krankenhäuser oberhalb der KRITIS-Schwelle	BSI-KritisV, NIS2, § 75c SGB V
Kleinere Kliniken und MVZ	§ 75c SGB V, zunehmend NIS2-Pflicht
Arztpraxen, Pflegeeinrichtungen	DSGVO
Telematikinfrastruktur (E-Rezept, ePA)	gematik-Vorgaben, BSI-Aufsicht
Medizinprodukte-Hersteller	MDR, Cyber Resilience Act (CRA)



Die Konsequenz:

Mehr regulatorische Pflichten als je zuvor und ein Sektor, der bei der Umsetzung strukturell hinterherhinkt.

Executive Summary

Cyberkriminalität ist heutzutage zu einem lukrativen Business gereift. Angreifergruppen zielen primär auf Erpressung ab und suchen sich Branchen, in denen der Impact eines erfolgreichen Angriffs maximal ist. Healthcare erfüllt dieses Profil in besonderem Maße: sensible Daten, vernetzte Medizintechnik und ein Sektor, der aus nachvollziehbaren Gründen zuerst in Versorgung investiert, nicht in IT-Sicherheit.

Die drei Kernbefunde:

- Gesundheitsdaten erzielen im Darknet ein Vielfaches des Preises von Kreditkartendaten: Rund 250 € gegenüber durchschnittlich 4,34 €. Das macht Kliniken, Praxen und Labore zu einem strukturell attraktiven Ziel.
- 90 % der befragten Krankenhäuser schätzen die Bedrohung durch Cyberkriminalität als hoch oder sehr hoch ein. Gleichzeitig geben 70 % mangelnde finanzielle Mittel als Hemmnis an, und ein Drittel hat unbesetzte Stellen in der IT-Sicherheit.
- Angriffe auf vernetzte medizinische Geräte oder Klinik-Infrastruktur gefährden im Extremfall Menschenleben, 2020 erstmals belegt durch den Todesfall am Universitätsklinikum Düsseldorf.

×

×

×

×

×

×

×

×

×

Die digitale Patientenakte und ihr blinder Fleck

Noch vor wenigen Jahren war eine Klinik-IT ein geschlossenes System. Heute laufen Patientenakte, Telematikinfrastruktur, E-Rezept und vernetzte Medizingeräte über eine wachsende Zahl digitaler Schnittstellen. Das ist gut für Versorgungsqualität und Effizienz.

Das Problem: Die Sicherheitsinfrastruktur ist nicht im gleichen Tempo mitgewachsen. Die gemeinsame Krankenhausstudie 2025 von BDO und dem Deutschen Krankenhausinstitut (177 befragte Krankenhäuser) zeigt: Jedes fünfte deutsche Krankenhaus war in den letzten drei Jahren von einem meldepflichtigen Cybervorfall betroffen. Technische Basisschutzmaßnahmen wie Antivirensoftware und Firewalls sind zwar weit verbreitet, fortgeschrittene Maßnahmen wie praktische Notfallübungen dagegen deutlich seltener.

Digitalisierung ohne Sicherheitsstrategie: Die Zahlen

Laut BSI erfasste der Berichtszeitraum Oktober 2024 bis September 2025 insg. 138 sicherheitsrelevante Vorfälle mit Bezug zum Gesundheitswesen, bei ausdrücklich anerkannter Dunkelziffer, da Pflegeeinrichtungen und ambulante Versorger bislang nicht meldepflichtig sind. Die Telematikinfrastruktur war mit 62 Vorfällen die größte Kategorie, Leistungserbringer (Krankenhäuser, Pflegeeinrichtungen, Praxen) folgten mit 43 Vorfällen bei stabiler Fallzahl gegenüber dem Vorjahr.

Dazu kommt ein strukturelles Problem: In vielen Häusern trifft eine gewachsene, historisch fragmentierte IT-Landschaft auf immer mehr angebundene externe Systeme – von Laborpartnern bis zu Medizingeräte-Herstellern. Der Generalunternehmer der IT hat vielleicht ein modernes SIEM. Der angeschlossene Pflegedienst oder das externe Labor nicht. Und genau dort liegt häufig das Einfallstor.



PODCAST

CYBER SECURITY

Basement

In unserem Podcast spricht Michael Döhmen alle 14 Tage mit spannenden Gästen über Themen aus dem Bereich Cybersecurity.

Jetzt Reinhören

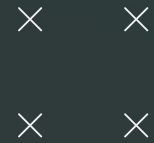




ANGRIFFSVEKTOREN

Wo es im Gesundheitswesen brennt

Cyberangriffe auf Gesundheitseinrichtungen folgen keinem Zufallsprinzip. Sie nutzen strukturelle Schwächen, und der Sektor hat davon mehr als genug.



Vektor 1

Vernetzte Medizingeräte

Infusionspumpen, bildgebende Systeme und Monitoring-Geräte kommunizieren zunehmend vernetzt, oft über veraltete Protokolle und mit langen Lebenszyklen, die Patches erschweren. Wer ein solches Gerät kompromittiert, sitzt im Kliniknetzwerk – mit potenziellem Zugriff auf weit mehr als nur das Gerät selbst.

Vektor 2

Patientendaten, Telematikinfrastruktur und Cloud

Elektronische Patientenakte, E-Rezept und Cloud-basierte Praxisverwaltungssysteme bündeln hochsensible Daten. Genau diese Bündelung macht sie für Ransomware-Gruppen so attraktiv: Wer eine Klinik trifft, deren Daten im Darknet auftauchen, bringt sie in eine Lage, in der Zahlung oft schneller erscheint als der öffentliche Reputationsschaden.



Vektor 3

Lieferkette: Medizintechnik-Zulieferer, Labore, Pflegedienste

Der gefährlichste Angriff kommt selten von der Klinik selbst, sondern von ihrem schwächsten angebundenen Partner. Externe Labore, Pflegedienste und Medizingeräte-Hersteller sind über Schnittstellen eng verzahnt und oft schlechter geschützt als die Klinik, mit der sie verbunden sind.

Vektor 4

Der Mensch

KI-gestützte Phishing-Mails sind heute kaum noch von echter Klinikkommunikation zu unterscheiden. In einer Branche, in der Personal chronisch knapp und Weiterbildungszeit begrenzt ist, bleibt Security Awareness häufig auf der Strecke, obwohl Phishing eines der größten Einfallstore bleibt.

138

gesundheitsbezogene
Sicherheitsvorfälle laut BSI
(Okt. 2024–Sep. 2025)

43

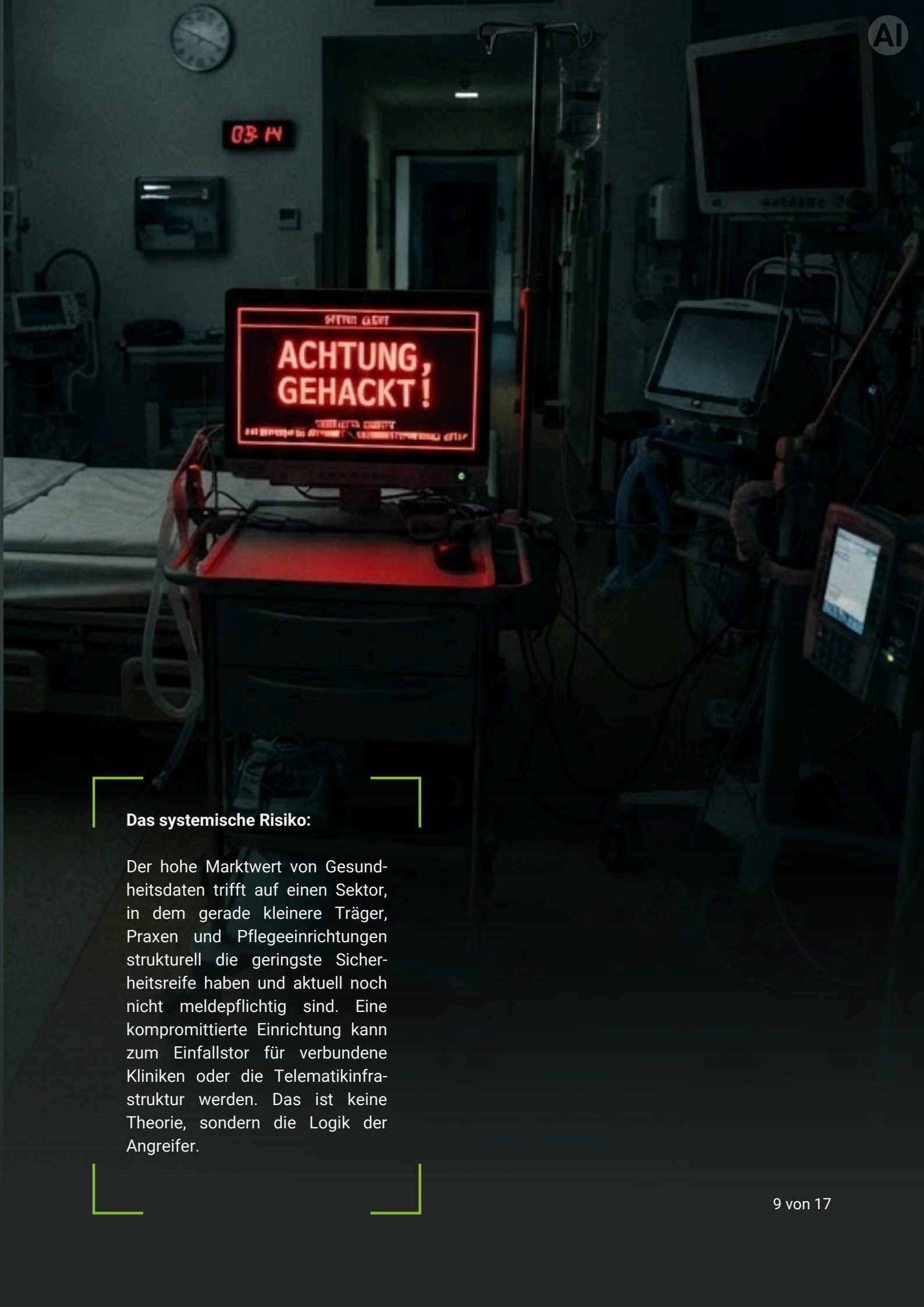
davon bei Leistungserbringern
(Krankenhäuser, Praxen, Pflege)

250 € vs. 4,34 €

Darknet-Preis eines
Gesundheitsdatensatzes vs.
eines Kreditkarten-
Datensatzes

182

Ransomware-Opfer in
Deutschland Jan.–Mai
2026 (+7,7 % ggü.
Vorjahr)



Das systemische Risiko:

Der hohe Marktwert von Gesundheitsdaten trifft auf einen Sektor, in dem gerade kleinere Träger, Praxen und Pflegeeinrichtungen strukturell die geringste Sicherheitsreife haben und aktuell noch nicht meldepflichtig sind. Eine kompromittierte Einrichtung kann zum Einfallstor für verbundene Kliniken oder die Telematikinfrastruktur werden. Das ist keine Theorie, sondern die Logik der Angreifer.

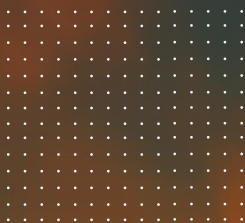
Wenn es passiert...

Drei Vorfälle zeigen, wie unterschiedlich die Folgen ausfallen können, und wie ähnlich die Muster sind.

Juli 2025

AMEOS Gruppe

Die AMEOS Gruppe, einer der größten Klinikbetreiber im deutschsprachigen Raum mit über 100 Einrichtungen, identifizierte am 7. Juli 2025 einen Cyberangriff und schaltete vorsorglich alle digitalen Systeme ab. Der E-Mail-Verkehr fiel konzernweit aus, Röntgen- und Laboruntersuchungen waren zeitweise nicht möglich. Im August bestätigte AMEOS den Abfluss personenbezogener Daten; mehrere Landesdatenschutzbehörden leiteten DSGVO-Prüfverfahren ein.



Januar 2026

Kreisklinik Roth

Nach einem mutmaßlichen Hackerangriff auf das interne IT-Netzwerk trennte die Kreisklinik Roth am 7. Januar 2026 vorsorglich die Internetverbindung. Die Notaufnahme musste kurzzeitig schließen und Rettungswagen wurden umgeleitet, die stationäre Versorgung lief über analoge Verfahren weiter. Das LKA Bayern nahm die Ermittlungen auf.

Februar 2026

BDH-Klinik Greifswald

In der Nacht zum 22. Februar 2026 fiel nach einem Cyberangriff das Kommunikationsnetz der BDH-Klinik Greifswald komplett aus, Stationen stellten auf analoge Arbeitsweise um. Wochen später bestätigte die Klinik den Abfluss von Patientendaten; Betroffene wurden anschließend gezielt zu Erpressungszwecken kontaktiert.

Drei Fragen, die jede Gesundheitseinrichtung beantworten sollte.

1. Wer hat Zugang zu welchen Systemen, und ist das lückenlos dokumentiert?

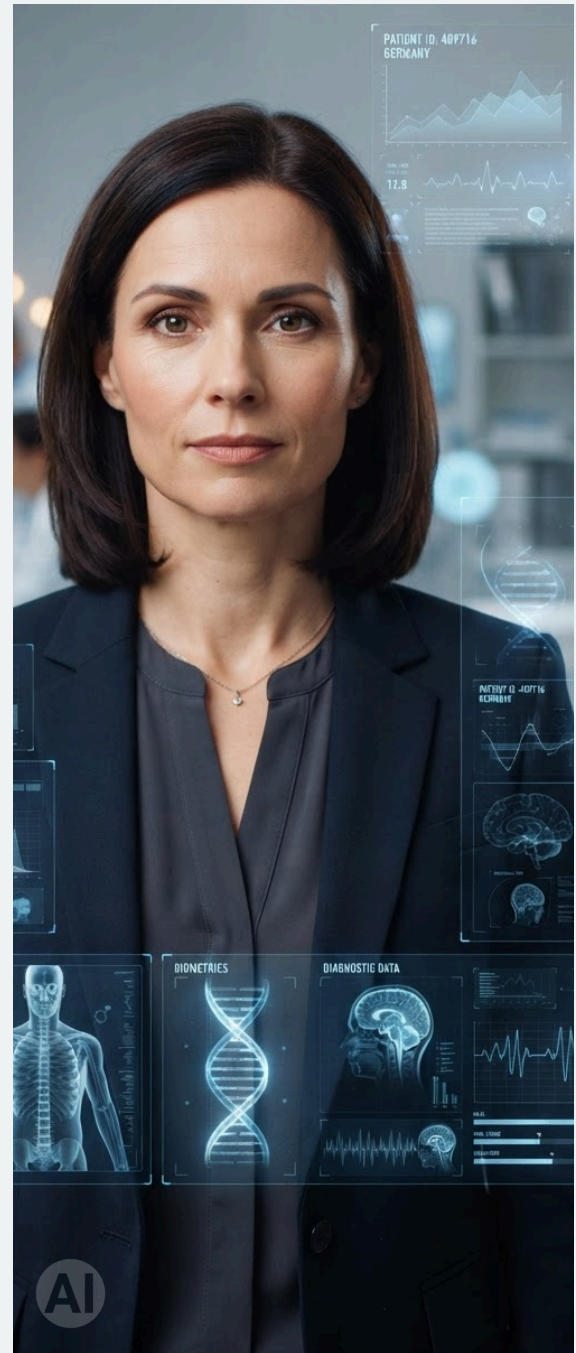
Auf vernetzten Klinikinfrastrukturen mit externen Laboren, Pflegediensten und Medizingeräte-Herstellern ist die Antwort selten befriedigend. Was nicht inventarisiert ist, kann nicht geschützt werden.

2. Sind Sicherheitsanforderungen an externe Partner vertraglich verbindlich?

Labore, Pflegedienste und Medizingeräte-Hersteller sind über Schnittstellen eng mit der Klinik-IT verzahnt. Ohne vertraglich festgelegte Mindeststandards bleibt jeder zusätzliche Anschluss ein unkontrolliertes Risiko – unabhängig davon, wie gut die eigene IT abgesichert ist.

3. Ist IT-Sicherheit personell und finanziell so ausgestattet, dass sie handlungsfähig ist?

Laut BDO/DKI-Krankenhausstudie 2025 geben 70 % der Krankenhäuser mangelnde finanzielle Mittel als Hemmnis für IT-Sicherheit an, ein Drittel hat unbesetzte Stellen in diesem Bereich. Wo Budget und Personal fehlen, bleibt Sicherheit ein Lippenbekenntnis statt gelebter Praxis.



WAS JETZT ZU TUN IST:

Konkret, nicht theoretisch

Cybersicherheit ist kein Einmal-Projekt, sondern ein Betriebszustand. Fünf Maßnahmen mit dem größten Wirkungsgrad für Kliniken, Praxen und Gesundheitseinrichtungen:

Angriffsfläche inventarisieren

Was nicht bekannt ist, kann nicht geschützt werden. Alle vernetzten Medizingeräte, Schnittstellen zu Laboren und Pflegediensten sowie Cloud-Zugänge gehören auf die Liste.

Patch-Management als Pflicht

Medizingeräte mit langen Lebenszyklen brauchen ein eigenes Vorgehen für Updates und kompensierende Maßnahmen, wo Patches nicht möglich sind.

Security Awareness schulen

Phishing bleibt eines der größten Einfallstore. KI macht Angriffe täuschend echt: Regelmäßige, realistische Schulungen sind kein Nice-to-have.

Standards für externe Partner definieren

Sicherheitsanforderungen gehören in Verträge mit Laboren, Pflegediensten und Medizintechnik-Zulieferern. Wer an die Klinik-IT angebunden wird, muss Mindeststandards nachweisen.

Notfallplan etablieren

Ein Notfallplan, der nie geprobt wurde, ist im Ernstfall nur ein Blatt Papier. Realistische Übungen zeigen, wo die analogen Rückfallebenen tatsächlich tragen.

Ein Managed SOC als Antwort

Ein spezialisierter Security Service Provider kann helfen, diese Herausforderungen gezielt und effizient zu meistern. Unser Managed Security Operations Center schützt Forschungsergebnisse, unterstützt

die Einhaltung regulatorischer Vorgaben, minimiert wirtschaftliche Risiken und leistet einen wichtigen Beitrag zur Patientensicherheit.



„In einem SOC zu arbeiten heißt, Verantwortung für etwas zu übernehmen, das man nicht sehen kann, aber das jeder Mensch täglich braucht.“

Mohamed Abdelfattah, Senior SOC-Analyst, suresecure GmbH

Interdisziplinär aufgestellt

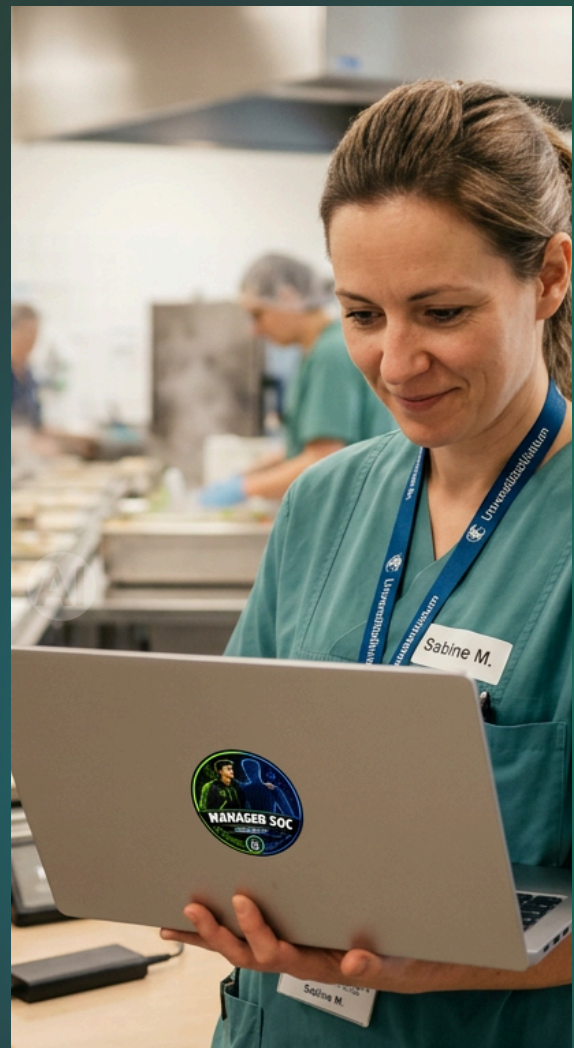
Interdisziplinär bedeutet bei uns, alle benötigten Expertisen mindestens doppelt zu besetzen. Unser SOC-Team besteht aus Platform Engineers, Incident Analysts, SOC-Analysts, Detection Engineers, dem Incident Manager, Consultants und Customer Success Managern. Neun Rollen, die gemeinsam dafür sorgen, dass eine Klinik oder ein Labor rund um die Uhr geschützt ist.

Was ist drin im Managed SOC?

Unser SOC hat einen hohen Reifegrad erreicht und setzt auf eine Cloud-native Lösung von Google: SIEM, SOAR und Google Threat Intelligence. SIEM sammelt und korreliert die Logs relevanter Quellen, SOAR führt automatisierte Reaktionen aus, und Google Threat Intelligence liefert Zugriff auf eine der größten Cybersecurity-Datenbanken der Welt. Zusätzlich verfügt unser SOC-Service über einen integrierten Schwachstellen-Scanner, der kontinuierlich kritische Schwachstellen erkennt und an das SOC-Team übermittelt.

Onboarding

Wir akzeptieren es nicht, dass Onboardings lange dauern. Vom ersten Tag an, an dem sich ein Partner für uns entscheidet, stellen wir einen Transition Manager bereit. Bereits nach etwa einer Woche findet das Kick-off statt, nach vier Wochen geht der Service live, nach spätestens sechs Wochen ist die vollständige Überwachung durch unser SOC in place.





Schlusswort

Wer Cyberbedrohungen nachhaltig entgegenwirken möchte, sollte sich Gedanken über ein Frühwarnsystem machen. Ein SOC, wie hier beschrieben, stellt derzeit die effektivste Verteidigung dar. Zwar garantiert auch ein SOC keine hundertprozentige Sicherheit, aber früh erkannte Angriffe führen in der Regel nur zu minimalen Folgeschäden.

Sicherheit ist tief in unserer Kultur verankert, und wir setzen alles daran, eure digitale Souveränität zu gewährleisten. Wir freuen uns auf ein Kennenlernen.



Quellen & Nachweise

- Statistisches Bundesamt (Destatis): 2,0 % mehr stationäre Krankenhausbehandlungen im Jahr 2024. Pressemitteilung PD25_398_231, 6. November 2025. www.destatis.de
- Detecon: IT-Sicherheit im Krankenhaus – Anforderungen, Risiken und erste Schritte. NIS2UmsuCG in Kraft seit 6. Dezember 2025. www.detecon.com
- PwC Deutschland: Sicherheit und digitale Hygiene im Krankenhaus. KHZG, § 75c SGB V. www.pwc.de
- Solidaris: Zur aktuellen Lage der IT-Sicherheit im Krankenhaus. KRITIS-Dachgesetz in Kraft seit März 2026. www.solidaris.de
- Augsburger Allgemeine / heise online: Gesundheitsdaten als Handelsware, 2024/2025
- BDO AG Wirtschaftsprüfungsgesellschaft / Deutsches Krankenhausinstitut (DKI): Krankenhausstudie 2025 „Cybersicherheit im Krankenhaus“, 177 befragte Krankenhäuser. www.bdo.de, www.dki.de
- Handelsblatt: Todesfall nach Hackerangriff auf Uniklinik Düsseldorf, 2020
- Bundesamt für Sicherheit in der Informationstechnik (BSI): Cybersicherheit im Gesundheitswesen 2025 (Broschüre), veröffentlicht April 2026, Berichtszeitraum Oktober 2024 – September 2025. www.bsi.bund.de
- AMEOS Gruppe: Pressemitteilung „Cyberangriff – personenbezogene Daten teilweise betroffen“, 26. August 2025. www.ameos.de; Security-Insider, 1. September 2025
- kma-online: Hackerangriff auf Kreisklinik Roth? Internet getrennt, Notaufnahme abgemeldet, 8. Januar 2026. www.kma-online.de
- kma-online: BDH-Klinik Greifswald wurde Opfer einer Cyberattacke, 26. Februar 2026; Security-Insider: Cyberattacke auf BDH-Klinik Greifswald – LKA ermittelt, 31. März 2026
- Security-Insider: Ransomware 2026 – Opferzahlen in Deutschland steigen (Datenquelle: ransomware.live), Juli 2026

suresecure gmbh

Dreischeibenhaus 1
40211 Düsseldorf

Phone: +49 (0) 2156 974 90 60

E-Mail: kontakt@suresecure.de
www.suresecure.de