

Diagnose: Hackerangriff

So schützt IT-Sicherheit
Krankenhäuser vor
Cyberattacken



Inhaltsverzeichnis

Cyberkriminalität – hohe Gefährdungslage.....	4
Gravierende Folgen – gesellschaftlich und finanziell.....	6
KRITIS-Dachgesetz und NIS-2-Richtlinie – verschärfte Sicherheitsanforderungen für Kliniken.....	8
Mensch und Maschine – die typischen Angriffsvektoren.....	10
Sicherheit & Zeit gewinnen im Krankenhaus – mithilfe von Security-Spezialisten.....	14
Cyberbedrohungen und Cybergesetze – auch in komplexen Klinikumgebungen zu meistern.....	18
IT-Sicherheit ist Vertrauenssache.....	20
Quellenverzeichnis	21
Abbilungsverzeichnis.....	22

Einleitung

Die Digitalisierung des Gesundheitswesens, neue Gesetze und Richtlinien wie NIS 2 sowie deren Umsetzung in nationales Recht, die Datenschutz-Grundverordnung (DSGVO) plus die verschärften Anforderungen von Cyberversicherungen stellen Krankenhäuser vor große Herausforderungen. Sie müssen ihre IT-Infrastruktur umfassend gegen immer bedrohlichere Cyberangriffe absichern und die hochsensiblen Daten schützen, die sie verwalten und verarbeiten. Das erfordert robuste Sicherheitsstrategien und bindet zudem Ressourcen. In dieser Situation lohnt es sich für Kliniken, auf die Expertise spezialisierter Dienstleister zu setzen. Das verschafft ihnen Sicherheit, und sie gewinnen Zeit und Personal für ihre Kernaufgabe: die Behandlung und Versorgung ihrer Patientinnen und Patienten.

Gesetzliche Initiativen tragen zunehmend dazu bei, die fortschreitende Digitalisierung des Gesundheitswesens in Deutschland wirksam zu flankieren und zu fördern. Ob elektronische Patientenakte (ePA), mobile Pflegedokumentation, telemedizinische Nachsorge oder KI-gestützte Entscheidungsunterstützungssysteme – digitale Lösungen helfen dabei, das medizinische Fachpersonal zu entlasten und die selbstbestimmte Mitarbeit von Patientinnen und Patienten zu stärken. Die Digitalisierung des Gesundheitswesens soll zu effizienteren Abläufen, einer effektiveren Versorgung und einer schnelleren und präziseren Diagnostik führen. Für die Krankenhäuser bedeutet sie aber auch, eine komplexe IT-Infrastruktur zu managen und deren Sicherheit zu gewährleisten.

Definition „Krankenhaus“

Zur besseren Lesbarkeit wird in diesem Whitepaper der Begriff „Krankenhaus“ verwendet. Dieser Begriff dient als Sammelbezeichnung und umfasst – sofern nicht ausdrücklich anders angegeben – gleichermaßen Kliniken.

Cyberkriminalität – hohe Gefährdungslage

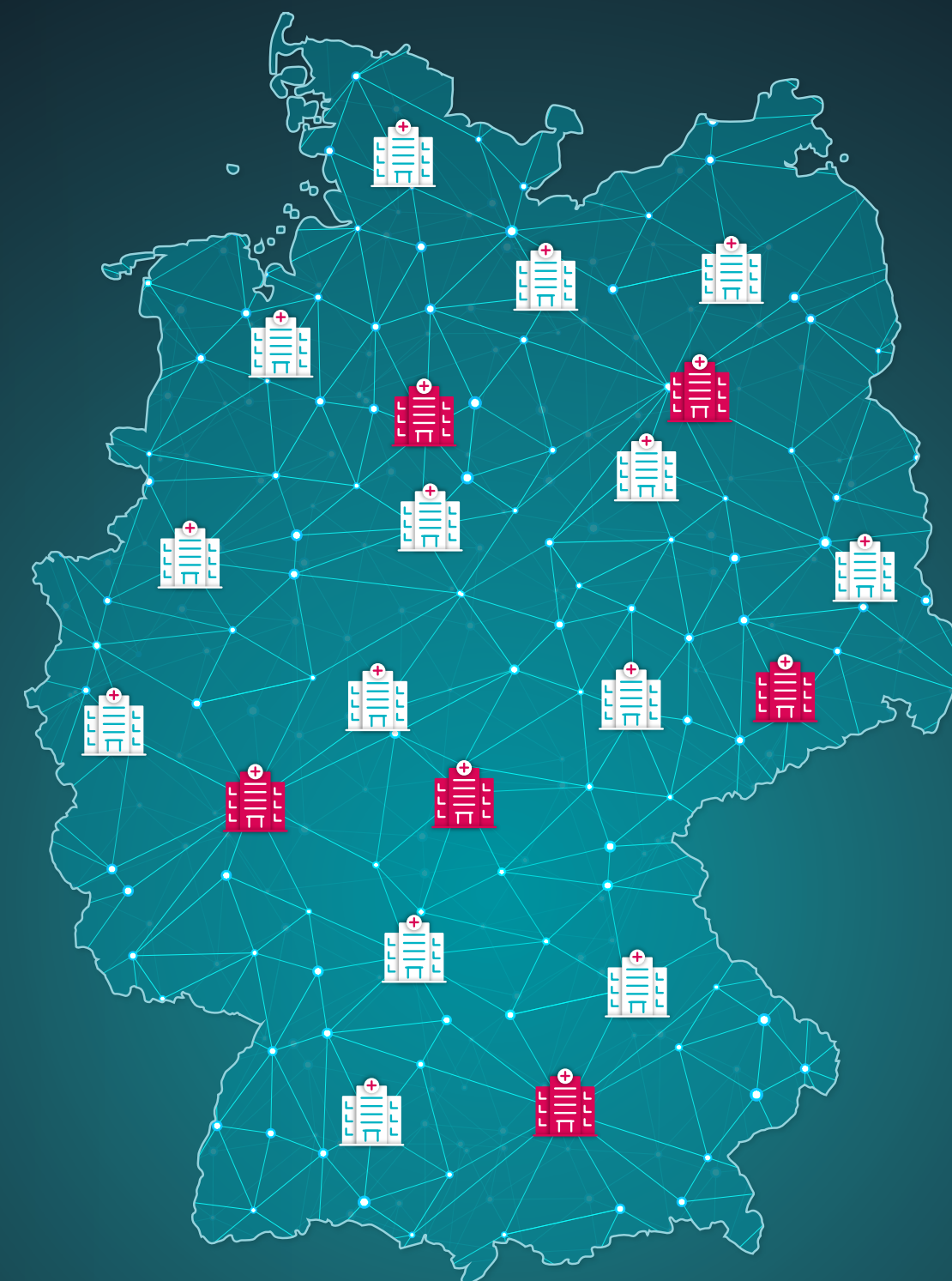
Keine leichte Aufgabe, denn gerade die IT-Security muss angesichts der zunehmenden Cyberkriminalität immer höheren Anforderungen gerecht werden. 2024 erfasste die Statistik des [Bundeskriminalamts \(BKA\)](#)¹ rund 330.000 Cybercrime-Fälle. Als „angespannt“ beschreibt auch das Bundesamt für Sicherheit in der Informationstechnik (BSI) in seinem [Lagebericht zur IT-Sicherheit](#)² von 2025 die aktuelle Gefährdungslage.

Aufgrund seiner Bedeutung für die Versorgung der Bevölkerung und der hochsensiblen Daten, die seine Institutionen verwalten, ist der Gesundheitsbereich besonders bedroht. Krankenhäuser und andere medizinische Einrichtungen stellen für Cyberkriminelle äußerst attraktive Ziele dar und verzeichneten in der Folge in den letzten Jahren einen signifikanten [Anstieg der Angriffe](#)³. Von den mehr als 700 Störungen, die die Betreiber kritischer Infrastrukturen allein zwischen Juli 2024 und Juni 2025 meldeten, ereigneten sich die meisten im Gesundheitsbereich. Einem [Bericht](#)⁴ der Europäischen Agentur für Cybersicherheit (ENISA) von 2023 zufolge zielten europaweit 42 Prozent der Cyberattacken im Gesundheitsbereich auf Krankenhäuser ab. Bestätigt wird dieser Trend unter anderem durch die Zusammenstellung von [Cyberangriffen auf Krankenhäuser](#)⁵ durch die Heinrich-Böll-Stiftung – und durch Forschungen des Hasso-Plattner-Instituts an der Universität Potsdam. Sie ergaben, dass in Deutschland in den letzten Jahren rund [30 Prozent aller Kliniken](#)⁶ bereits mindestens einen Sicherheitsvorfall hatten.

Das Mittel der Wahl ist dabei für die Cyberkriminellen sehr häufig Ransomware. Wie schon in den Jahren zuvor stand sie 2024 im Lagebericht des Bundeskriminalamts ganz oben auf der Liste der Cyberangriffe.

Betroffen waren alle Sektoren, auch das Gesundheitswesen und insbesondere Krankenhäuser. Zu den bekannten Fällen zählten 2024 die Angriffe auf die [Bezirkskliniken Mittelfranken](#)⁷, den Klinikenverbund im [Kreis Soest](#)⁸ und die [Wertachkliniken Bobingen & Schwabmünchen](#)⁹. Die Liste ließe sich noch weiter fortsetzen und riss auch 2025 nicht ab. Die Schadprogramme beschränkten beziehungsweise verhinderten nicht nur den Zugriff auf Daten und Systeme, sondern zogen auch Daten ab.

Daneben stieg auch noch die Zahl von DDoS-Angriffen (Distributed Denial-of-Service, also die Überlastung von Servern, um Dienste lahmzulegen) die darüber hinaus immer effizienter werden. Durch schädlichen Traffic überflutet und lahmgelegt wurde unter anderem im Juli 2025 die IT der [Ameos-Kliniken](#)¹⁰. Mit ernststen Folgen: Der Angriff schränkte den Klinikbetrieb und Rettungsdienst erheblich ein, darüber hinaus wurden personenbezogene Daten von Patienten und Mitarbeitenden abgezogen.



30% aller Kliniken hatten
bereits mindestens einen
Sicherheitsvorfall

Abb. 1: Schematische Darstellung der Kliniken mit mindestens einem Sicherheitsvorfall in Deutschland, ESET Deutschland GmbH

Gravierende Folgen – gesellschaftlich und finanziell

Für die Geschädigten können diese Straftaten äußerst verlustreich sein. So verursachten dem Bitkom¹¹ zufolge Cyberattacken in Deutschland im Jahr 2025 einen Schaden von ca. 202 Milliarden Euro – gut 22 Milliarden mehr als noch 2024. Abgesehen von möglichen Zahlungen einer Versicherung können die Betroffenen kaum auf Kompensation hoffen: Während die allgemeine Aufklärungsquote von Straftaten in Deutschland bei 58 Prozent liegt, dümpelt sie bei Cybercrime-Delikten mit 32 Prozent deutlich darunter.

Wenn Krankenhäuser aufgrund von Cyberattacken nicht mehr auf ihre IT, die damit vernetzten Geräte und auf die Daten ihrer Patientinnen und Patienten zugreifen können, sind die möglichen Folgen gravierend. Eine Studie in den USA¹² hat ergeben, dass Cyberattacken in 75 Prozent der Fälle eine Verschlechterung der Patientenversorgung nach sich ziehen und dadurch indirekt die Sterblichkeit erhöhen. Ein erfolgreicher Angriff kann zu lebensbedrohlichen Situationen führen:

- Einschränkung oder Stillstand der medizinischen Versorgung und Notfallversorgung
- Verzögerung von Behandlungen und Operationen
- Risiko von fehlerhaften Medikamentenverabreichungen, Behandlungen und Diagnosen
- Ausfall von medizinischen Geräten und des Intensiv-Monitorings
- Der Verlust der Daten sowohl der Patientinnen und Patienten als auch der Mitarbeitenden, die für kriminelle Zwecke wie Betrug, Diebstahl und Identitätsdiebstahl missbraucht werden können

Auch der wirtschaftliche Schaden für betroffene Krankenhäuser ist enorm. Mittlerweile muss man wohl eher mit Folgekosten in Millionenhöhe rechnen. Die Summen können für Einrichtungen existenzbedrohend sein, tatsächlich haben Cyberattacken weltweit sogar schon zu Schließungen von Kliniken geführt. Negativ zu Buche schlagen unter anderem:

- direkte Aufwendungen, wie Lösegeldzahlungen bei einem Ransomware-Angriff
- Ausfälle durch Betriebsunterbrechungen
- Ausfälle durch den Datenverlust für Abrechnungen
- Kosten für die Wiederherstellung der IT-Systeme und der Daten
- erhöhte Prämien für Cyberversicherungen
- Bußgelder, wie sie unter anderem die DSGVO vorsieht.

Beim letzten Punkt kommt der Krankenhausleitung eine besondere Verantwortung zu. Dazu gehört auch, angemessene technische und organisatorische Maßnahmen zu treffen, um die sensiblen personenbezogenen Daten zu schützen. Bekannte Beispiele für **geahndete Datenschutzverstöße**¹³ sind das Haga Hospital in Den Haag (460.000 Euro) oder die Uniklinik Mainz¹⁴ (105.000 Euro).

Kosten eines Cybervorfalls im DACH-Gesundheitswesen



Betriebsunterbrechungen

1,5 – 4,0 Mio.



IT-Wiederherstellung/ Forensik

0,8 – 2,0 Mio.



Externe Dienstleistung / Incident Response

0,5 – 1,5 Mio.



Recht / DSGVO / Kommunikation

0,3 – 1,0 Mio.

Abb. 2: Kosten eines Cybervorfalls im DACH-Gesundheitswesen; Quellen: DKI, BSI, NCSC Schweiz, ENISA, Analogie zu europäischen Healthcare-Kosten

KRITIS-Dachgesetz und NIS-2-Richtlinie – verschärfte Sicherheitsanforderungen für Kliniken

Einschnitte in der medizinischen Versorgung, Vertrauensverlust, Verunsicherung, finanzielle Einbußen bis hin zum Bankrott – die Folgen von erfolgreichen Cyberattacken können sowohl für das Gemeinwohl als auch für die Kliniken selbst einschneidend sein. Der Gesetzgeber ist deshalb in den letzten Jahren verstärkt der Bedrohung durch Angriffe begegnet. So ist es seit 2022 gemäß § 75c SGB V¹⁵ Pflicht für alle Krankenhäuser, ein Informationssicherheits-Managementsystem (ISMS) nach dem aktuellen Stand der Technik bzw. den branchenspezifischen Sicherheitsstandards (BS3¹⁶) zu betreiben. Darüber hinaus gilt es spezifische Maßnahmen zur Betriebs- und Informationssicherheit einzuhalten, wie sie die jeweiligen Landeskrankenhausesetze (LKG) vorschreiben.

Mit weitreichenden Bestimmungen hat nun die Europäische Union mit ihrer zweiten Network-and-Information-Security-Richtlinie NIS 2¹⁷ auf die Cybergefahren reagiert, die neben dem Gesundheitssystem auch in anderen Bereich drohen. Das in Deutschland im Dezember 2025 in Kraft getretene NIS-2-Umsetzungsgesetz¹⁸ regelt die Cyber- und Informationssicherheit von privaten und öffentlichen Unternehmen und Institutionen in 18 verschiedenen Sektoren, die eine bestimmte Größe aufweisen oder kritische Anlagen betreiben. Damit ist NIS 2 eine Ergänzung der CER-Richtlinie zur Resilienz kritischer Einrichtungen, die mit dem im Januar 2026 beschlossenen KRITIS-Dachgesetz¹⁹ in deutsches Recht umgesetzt wurde und sich auf den physischen Schutz und das Krisenmanagement konzentriert. Die Umsetzung der von NIS 2 vorgegebenen Rahmenbedingungen erfolgt über § 30 BSI-Gesetz²⁰.

Die EU-weite NIS-2-Richtlinie soll das Niveau der IT-Sicherheit in allen Mitgliedsstaaten verbessern und deren Anforderungen vereinheitlichen. Die Richtlinie umfasst einen weiteren Kreis als das KRITIS-Dachgesetz. Sie bezieht sich unter anderem auf alle Krankenhäuser, Universitäts- und Reha-Kliniken, die entweder mehr als 50 Angestellte beschäftigen oder einen Jahresumsatz bzw. eine Bilanzsumme von mehr als zehn Millionen Euro aufweisen. In Deutschland erfüllt nahezu jedes der insgesamt mehr als 1.800 Krankenhäuser diese Kriterien. Sie werden nun gesetzlich in die Pflicht²¹ genommen und müssen einige Anforderungen erfüllen.

Insbesondere die Geschäftsleitungen²² sind für die NIS-2-Umsetzung voll verantwortlich und müssen die hierfür notwendigen Ressourcen und Prozesse sicherstellen. Verstöße gegen NIS-2-Regularien werden mit Bußgeldern von bis zu zehn

Millionen Euro beziehungsweise zwei Prozent des weltweiten Vorjahresumsatzes belangt (hier zählt jeweils die höhere Schadenssumme). Führungskräfte haften dabei persönlich, falls sie durch unzureichende Sicherheitsvorkehrungen eine Cyberattacke möglich gemacht haben.

Detailliertes Risikomanagement, IT-Sicherheit, geprüfte Lieferketten, Notfall- und Wiederherstellungsmanagement: Die verschärften Vorgaben der NIS-2-Richtlinie fordern heutzutage meist auch Cyberversicherungen – neben der Einhaltung des Patientendaten-Schutz-Gesetzes (PDSG) und der DSGVO. Um ihren Versicherungsschutz nicht zu verlieren, müssen Krankenhäuser den Gesellschaften häufig ihre NIS-2-Konformität durch ausführliche Dokumentationen, Informationssicherheits-Managementsysteme und/oder ergänzende Maßnahmen zu bestehenden ISO-27001-Zertifizierungen belegen.



Registrierung: Diese erfolgt bei der gemeinsamen Registrierungsstelle der Bundesämter für Sicherheit in der Informationstechnik (BSI) sowie für Bevölkerungsschutz und Katastrophenhilfe (BBK).



Geschäftsleitung: Die Geschäftsleitung muss ihre Umsetzungs-, Überwachungs- und Schulungspflichten einhalten.



Risikomanagement: Krankenhäuser sind verpflichtet, ein angemessenes Risikomanagement für alle IT-Systeme, -Komponenten und -Prozesse zu implementieren und zu dokumentieren. Die hierfür erforderlichen Maßnahmen (Risikoanalyse, Wirksamkeitsprüfungen, Verschlüsselung, Firewalls, Multi-Faktor-Authentifizierung und Virenschutz) müssen dem Stand der Technik entsprechen sowie europäische und internationale Normen berücksichtigen.



Sicherheitsvorfälle und Wiederherstellung: Zum Risikomanagement gehören zudem Pläne, Regeln und Maßnahmen für Sicherheitsvorfälle sowie für die Aufrechterhaltung und Wiederherstellung des Betriebs, etwa durch Back-up- und Krisenmanagement.



Lieferkette: Krankenhäuser müssen auch die Cybersicherheitspraxis ihrer Lieferanten und Dienstleister in ihr Risikomanagement aufnehmen und sich diese vertraglich nachweisen lassen. Des Weiteren sind beim Kauf von IT-Systemen und -Komponenten Sicherheitsmaßnahmen einzuhalten.



Personal: Die Angestellten benötigen Cybersicherheitsschulungen.



Meldung: Erhebliche IT-Sicherheitsvorfälle sind dem BSI zu melden. Zu den Meldungen gehören eine Bewertung des Vorfalls inklusive Schweregrad, Auswirkungen, Kompromittierungsindikatoren sowie Kontaktinformationen.

Mensch und Maschine – die typischen Angriffsvektoren

Die strikten Sicherheitsanforderungen der neuen Gesetze sind sinnvoll und nachvollziehbar. Sie stellen für Krankenhäuser jedoch eine immense Herausforderung dar. Die nationalen Umsetzungsgesetze der NIS-2-Richtlinie einzuhalten, erfordert finanzielle Investitionen in Technik und Personal. Möglich ist dies mithilfe der Finanzierung über die Bundesländer – allerdings reichen diese Gelder oft nicht. Zudem ist die finanzielle Decke der meisten Kliniken durch das Dauerschuldverhältnis mit den Krankenkassen in der Regel sehr dünn.

Auf technischer Seite stellt die für Krankenhäuser typische heterogene IT-Infrastruktur ein großes Problem dar. In Kliniken werden parallel unterschiedliche Systeme wie Krankenhausinformationssysteme (KIS), Laborinformationssysteme und Bildarchivierungssysteme (PACS) genutzt, die häufig nicht miteinander verbunden sind. Hinzu kommt eine breite Hardware-Palette. Diese reicht von Computern in der Verwaltung über Tablets und mobile medizinische Geräte für das Fachpersonal, die in der Pflege und Behandlung zum Einsatz kommen, bis hin zu fest installierten bildgebenden Systemen wie Röntgengeräten oder Computertomografen. Entsprechend vielfältig ist die installierte Software, die es zu verwalten und stets auf dem neuesten Stand zu halten gilt.

Eine unübersichtliche und komplexe IT-Infrastruktur bietet verschiedene Angriffsflächen für Cyberattacken. Erschwerend kommt hinzu, dass die IT-Security oft noch „klassisch“ in Silos

für Endgeräte wie Computer und medizinische Geräte, Messaging (E-Mails), Netzwerk und Internet mit jeweils unterschiedlichen Sicherheitslösungen aufgeteilt ist, die einen umfassenden Überblick und eine übergreifende Verwaltung erschweren. Es braucht Investitionen, eine Digitalisierungsstrategie und einige Anstrengung, die vielfältigen Systeme zu harmonisieren, um eine effiziente IT-Struktur auf NIS-2-Niveau zu erreichen.

Typische Sicherheitslücken entstehen beispielsweise durch veraltete oder End-of-Life-Versionen von Betriebssystemen und Applikationen. Diese sind oft nicht mehr mit modernen Sicherheitsstandards kompatibel und erhalten keine Updates oder Patches mehr. Sehr häufig sind davon auch über das Internet vernetzte medizinische Geräte betroffen. Risiken können zudem durch mobile Geräte entstehen, die nach dem BYOD-Prinzip (Bring Your Own Device) im Kliniknetzwerk zum Einsatz kommen, aber nicht ausreichend gesichert sind. Probleme verursachen auch Schatten-IT und ungesicherte Tools, wenn Beschäftigte ohne Wissen oder Genehmigung der zentralen IT-Verwaltung Hardware (zum Beispiel Laptops), Apps (allen voran Messenger-Dienste) und Cloud-Dienste nutzen, die nicht den Security-Richtlinien entsprechen, weil sie zum Beispiel bekannte Schwachstellen aufweisen. Zu einem Sicherheitsproblem können auch Datensilos führen, die bei der Anbindung von Technologien wie KI-Systemen an die vorhandene IT-Infrastruktur entstehen.

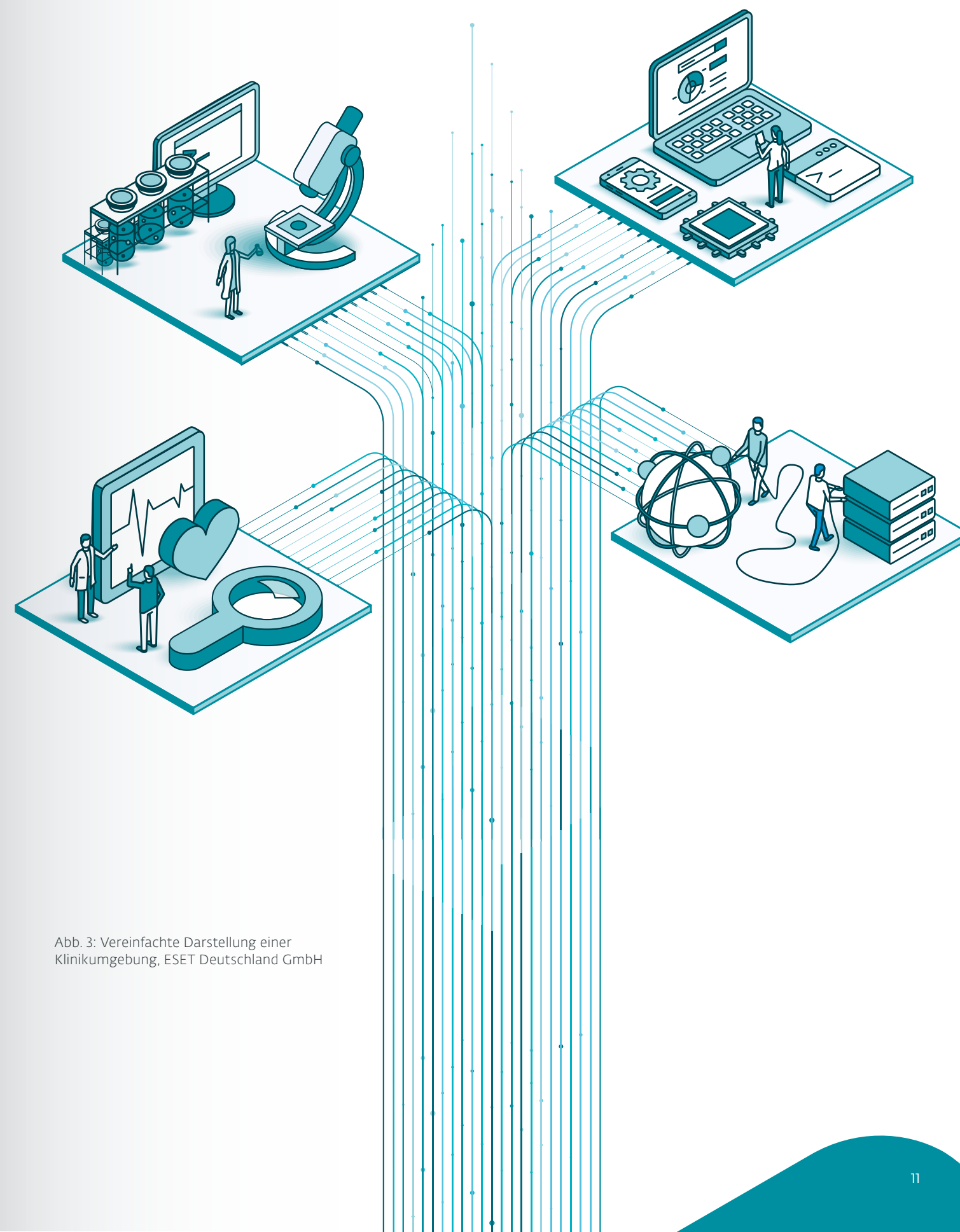


Abb. 3: Vereinfachte Darstellung einer Klinikumgebung, ESET Deutschland GmbH

Die technische Ausstattung von Krankenhäusern und deren Verwaltung bieten also reichlich Angriffsfläche, um Malware über Sicherheitslücken in der Software oder über physische Datenträger wie USB-Sticks oder Laptops einzuschleusen. Die Gefahr steigt weiter, wenn schwache Passwörter erlaubt und Benutzerberechtigungen unzureichend verwaltet werden. Dann sind die Tore schon ziemlich weit geöffnet für Viren, Würmer, Malware wie Ransom- bzw. Spyware & Co., die unbemerkt in die Systeme eindringen. Dort können sie zum Beispiel einen unerwünschten Fernzugriff ermöglichen, Daten ausspähen oder die Systeme verschlüsseln beziehungsweise lahmlegen.

Der Krankenhausbetrieb bringt es darüber hinaus mit sich, dass sich für die einzelnen Bereiche Schutzschirme leichter und schwerer spannen lassen. So kann zum Beispiel die Verwaltung umfangreicher und präventiver geschützt werden als Notaufnahmen ohne medizinische Fachangestellte, in denen viele Geräte im Dauerbetrieb laufen. Und nicht zuletzt darf man den menschlichen Faktor nicht vergessen. Hier gilt es, Awareness für Cybersecurity und Gefahren wie Phishing-Mails zu schaffen, die zu den **Haupteintrittsvektoren**²³ für Schadsoftware und Datendiebstahl zählen.

Schutz vor Erpressung – Ransomware Shield und Ransomware Remediation von ESET

Die Gefahr ist groß und sie wächst stetig an: „Ransomware-Angriffe stellen eine der größten Cyberbedrohungen für Staat, Wirtschaft und Gesellschaft dar“ mahnt das BSI²⁴ – und sie hat sich mittlerweile zu einem profitablen, professionell betriebenen kriminellen Geschäftsmodell entwickelt. Ransomware ist dem BKA²⁵ zufolge die „prägende Bedrohung im Cyberraum“, gefolgt von Phishing, Passwortangriffen, Malware und DDoS-Angriffen. Die Europäische Union ist eines der Hauptziele von Cyberattacken, wobei die Bedrohungen aus **unterschiedlichen Richtungen**²⁶ (vor allem von russischen und chinesischen **Hackern**²⁷) kommen und unterschiedliche Ziele verfolgen: sei es, um durch Erpressung und gestohlene Daten Geld zu ergaunern, Wirtschaftsspionage zu betreiben oder aus politischen Gründen (und gegen Bezahlung) Infrastrukturen lahmzulegen. Einen wirksamen Schutz bieten die beiden eng kooperierenden ESET Module Ransomware Shield und Ransomware Remediation. Während Ransomware Shield automatisch alle verdächtigen Anwendungen sperrt, die sich wie Ransomware verhalten, stellt Ransomware Remediation als ergänzende Absicherung verschlüsselte Dateien wieder her. Damit bei einem Ransomware-Angriff keine Daten verloren gehen, erstellt das zweistufige Sicherheitssystem während der Überprüfung eines potenziell schädlichen Prozesses Sicherheitskopien.

Ransomware-Behebung

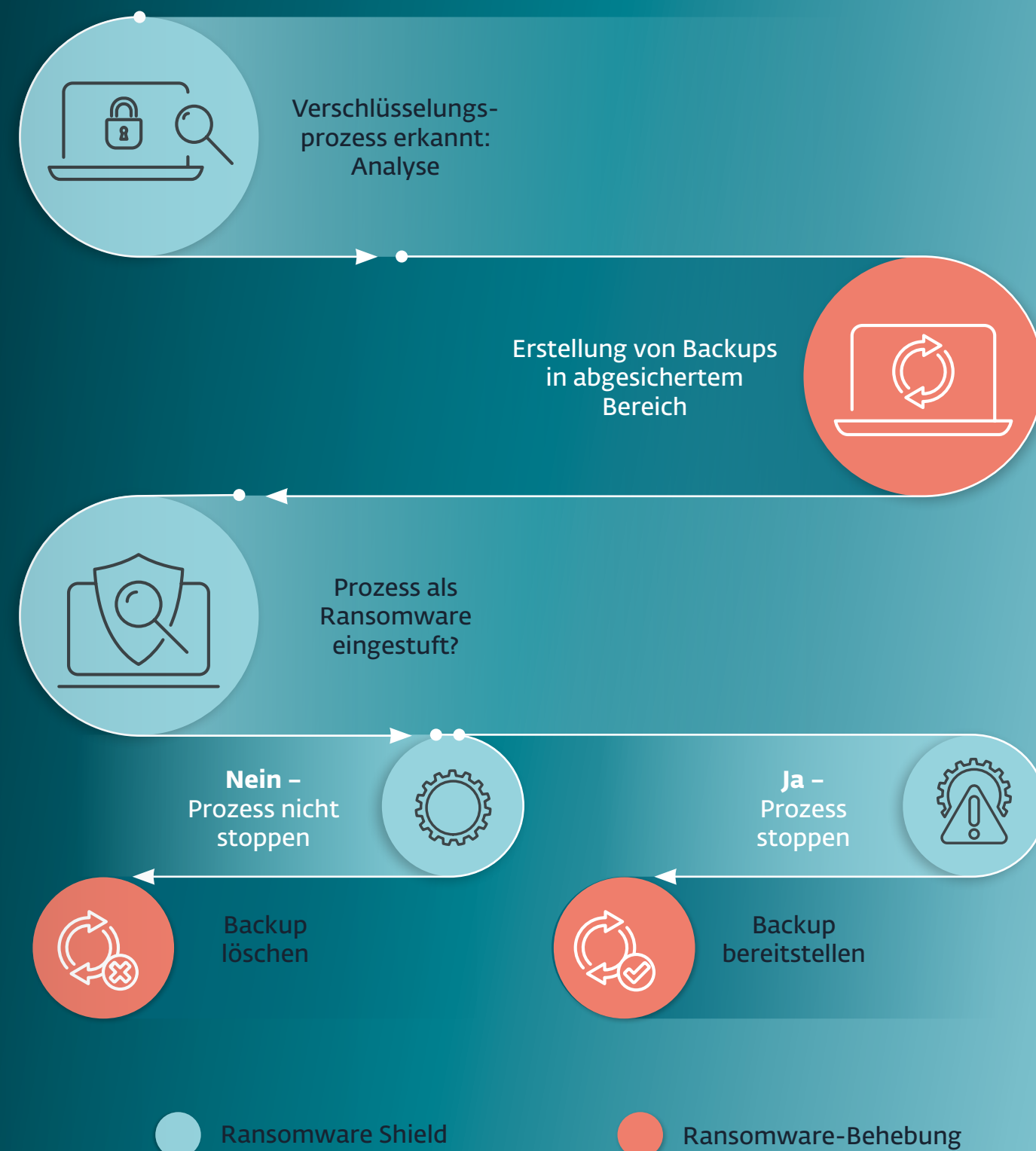


Abb. 4: Infografik zur Ransomware-Behebung, ESET Deutschland GmbH

Sicherheit & Zeit gewinnen im Krankenhaus – mithilfe von Security-Spezialisten

Auf dem Weg zu einer leistungsstarken IT-Security, die den Vorgaben der europäischen Gesetzgebung entspricht, benötigen Krankenhäuser Konzepte für die Risikoanalyse, Bewertungsverfahren zur Wirksamkeit von Risikomanagementmaßnahmen, gesicherte Sprach-, Video- und Textkommunikation sowie gegebenenfalls gesicherte Notfallkommunikationssysteme und noch vieles mehr. Komplexe Aufgaben, die ein geschultes Fachpersonal erfordern – das jedoch nicht jeder Klinik ausreichend zur Verfügung steht. Hinzu kommt der Zeitfaktor: Im Krankenhaus zählt jede Minute in der Behandlung, der Patientenversorgung und der Aufenthaltsdauer.

An dieser Stelle kann es sich für Krankenhäuser lohnen, auf spezialisierte und zertifizierte Sicherheits- und Schutzlösungen von Herstellern wie ESET zurückzugreifen. Mit seinem umfassenden Portfolio deckt das Unternehmen sämtliche IT-Security-Anforderungen ab und unterstützt Krankenhäuser dabei, die [NIS-2-Konformität](#)²⁸ zu erreichen. Die Lösungen von ESET sind nach den Qualitäts- und Informationssicherheitsstandards [ISO 9001:2015](#)²⁹ und [ISO/IEC 27001:2022](#)³⁰

zertifiziert. Für die Sicherheit der Kliniken und deren Lieferketten verfolgt ESET den [Zero Trust-Ansatz](#)³¹. Dieser vereint bekannte Sicherheitsmaßnahmen und Best-Practices in einem ganzheitlichen Ansatz und findet auch branchenunabhängig Anwendung.

Mit einem simplen Reifegradmodell ist die Umsetzung mit ESET stufenweise möglich und für jede Organisationsgröße sinnvoll. Ob als Laufzeitpaket oder als Managed Service, der ESET Multi Secured Endpoint, also die Kombination aus modernem Endpoint-Schutz, Verschlüsselung, Multi-Faktor-Authentifizierung, Cloud Sandboxing und Schutz für Cloud-Anwendungen bildet dabei das richtige Fundament für Zero Trust. Für Organisationen, die zudem ein eigenes Security Operations Center (SOC) betreiben und dem Risiko gezielter Angriffe ausgesetzt sind, ist es wichtig, ein geeignetes Frühwarnsystem mittels Threat Intelligence Service zu betreiben. Hier kann ESET helfen, mittels Informationen zur globalen Bedrohungslage, aufkeimende oder geplante Angriffe frühzeitig zu enttarnen und wichtige Assets optimal zu schützen.

Besonders effizient minimieren viele Kliniken ihre Cyberrisiko durch [Managed Detection and Response \(MDR\) Services](#)³². ESET übernimmt dabei den operativen Betrieb einer Extended Detection and Response (XDR) Lösung für Clients (Endpoint, Server) Cloud, Netzwerk, E-Mail etc. Diese Sicherheitslösungen nutzen künstliche Intelligenz, um Cyberbedrohungen in Echtzeit zu erkennen, zu untersuchen und automatisiert zu bekämpfen.

Je nachdem, welche Lösung man wählt, wird man entweder mit den nötigen Daten, zum Beispiel über aktuelle Bedrohungen und Angriffsvektoren, und den entsprechenden Abhilfemaßnahmen versorgt, oder man lässt sie umfassend von ESET implementieren, optimieren und verwalten, sodass man weder ein spezielles IT-Team noch weitere Hilfsmittel dafür benötigt. Eine solche Extended Detection & Response-Lösung mit proaktiven Maßnahmen zur Gefahrensuche und -abwehr gehörte auch zur Lösung, für die sich das [Klinikum Landshut](#)³³ entschied. Das komplette Bundle wurde stufenweise samt Tests und Schulungen implementiert.



Viele Unternehmen stehen angesichts der aktuellen Bedrohungslage, aber auch im Hinblick auf rechtliche Regelungen wie der NIS2-Richtlinie und Anforderungen von Cyberversicherungen, vor der Herausforderung, den Schutz ihrer digitalen Infrastruktur anzuheben. Während Extended Detection and Response (XDR) Lösungen wie ESET Inspect hierbei immer mehr zur geforderten Standardausrüstung der IT-Sicherheit avancieren, stellen sich viele Unternehmen die Frage, wie sie eine solche Lösung verwalten sollen. Unsere MDR-Services schaffen hier Abhilfe und bieten Unternehmen jeder Größe Unterstützung beim operativen Betrieb Ihrer ESET Inspect Instanz. Je nach Bedarf und finanziellen Ressourcen haben sie die Möglichkeit, zwischen einem KI-gestützten schlanken und einem umfassenden kundenspezifischen MDR-Service zu wählen.

Die Vorteile der MDR-Services von ESET liegen auf der Hand

- **Geschwindigkeit:** MDR-Services von ESET identifizieren auffällige Aktivitäten und Anomalien innerhalb einer IT-Infrastruktur. Ein Großteil der Erkennungs- und Reaktionsprozesse setzt auf KI und läuft automatisiert ab. Das ermöglicht eine umgehende Reaktion auf mögliche Sicherheitsvorfälle: Von Erkennung bis zur Behebung vergehen in der Regel durchschnittlich sechs Minuten.
- **Personalersparnis und Senkung von Langzeitkosten:** Sicherheitsfachkräfte werden von ESET gestellt und kommen nur zur Überprüfung sowie zur Optimierung der Abläufe zum Einsatz. Damit sparen sich Kliniken teure Fachkräfte, die im Schichtdienst arbeiten und sich regelmäßige weiterbilden müssen.
- **Geringe Investition in Hard- und Software:** Dank des Cloud-Betriebs bleiben die Lösungen stets auf dem aktuellen Stand und bedürfen keiner aufwändigen Wartung.
- **Erfüllung von Compliance- und Cyberversicherungs-Anforderungen:** Die MDR-Services von ESET unterstützen bei der Umsetzung von Versicherungsanforderungen, von rechtlichen Regelungen wie der NIS-2-Richtlinie und dank des umfangreichen, individuell anpassbaren Reportings auch bei der Einhaltung von Berichtspflichten im Falle einer Systemkompromittierung.

Zur Case Study von einem unserer zufriedenen Kunden:

Klinikum Landshut: Wenn IT-Security auf Visite geht



Cyberbedrohungen und Cybergesetze – auch in komplexen Klinikumgebungen zu meistern

Immer mehr und besser, zudem immer effizienter erstellt und wirkungsvoller durch den Einsatz von KI – die Anzahl und die destruktive Qualität von Cyberattacken hat im Gesundheitsbereich rasant zugenommen. Insbesondere Ransomware ist zu einer massiven Bedrohung geworden. Im Fokus der Angriffe stehen Krankenhäuser, die eine herausragende Stellung in der allgemeinen Versorgung einnehmen und hochsensible Daten verwalten. Als Reaktion auf die wachsende Gefahr hat die EU durch die NIS-2-Richtlinie die geltenden Bestimmungen für Cybersecurity verschärft und bringt damit Kliniken in Zugzwang.

Ihre hohen Anforderungen lassen sich in den heterogenen IT-Infrastrukturen von Krankenhäusern teils nur schwer umsetzen. Abhilfe schaffen hier spezialisierte IT-Security-Unternehmen wie ESET mit zertifizierten Lösungen, die DSGVO- und NIS-2-konform sind. Sie können sie mit Sicherheitsprogrammen wirksam vor Ransomware schützen sowie mit ihren breit gefächerten Komplettlösungen die IT-Systeme von Kliniken nach den Anforderungen von NIS 2 aufrüsten, ohne den Betrieb zu stören und die Beschäftigten in Anspruch zu nehmen. Eine effektive Ergänzung sind zudem die KI-basierten, automatisierten MDR-Services: ESET übernimmt hier als Dienstleister für das Krankenhaus den operativen Betrieb seiner Sicherheitslösung und spart ihm damit (lebens-)wichtige Ressourcen: Zeit, Geld und Personal.

ESET – IT-Security made in Europe

Cyberangriffe verhindern, bevor sie passieren – darin ist der IT-Sicherheitshersteller ESET ein weltweit führender Spezialist. Ob Client (Endpoint, Server, Mobilgeräte) oder Cloud-Schutz – durch die Kombination aus KI und menschlicher Expertise sichert ESET Unternehmen, kritische Infrastrukturen und Privatpersonen effektiv ab. Die Technologien „Made in EU“ sorgen für zuverlässige Erkennung und Reaktion, extrem sichere Verschlüsselung und Multi-Faktor-Authentifizierung. Das Unternehmen besitzt mehr als 35 Jahre Erfahrung und bietet ein breites Portfolio an zertifizierten State-of-the-Art Security-Lösungen. ESET verfügt über weltweite Forschungs- und Entwicklungszentren und ein starkes internationales Partnernetzwerk in 178 Ländern und Regionen. Als europäisches Unternehmen mit Hauptsitz in Bratislava (Slowakei) bietet es entscheidende Vorteile:

- Strenge Einhaltung der DSGVO
- Hohe digitale Souveränität
- „No Backdoor“-Garantie: Die ESET Lösungen haben keine versteckten Zugänge, was die Sicherheit gegenüber nicht-europäischen Anbietern erhöht.
- Lokaler Support für die DACH-Region aus Jena



- Verwaltung – Kaufmännische und organisatorische IT-Systeme wie bspw. Patientenaufnahme, Abrechnung und ERP
- Verwaltungs- und Arztbereich – Hybride Überschneidungsbereiche wie Patienten- und Qualitätsmanagement sowie Abrechnung/Fallpauschale
- Arztbereich – Medizinische Fachsysteme (KIS, PACS, Labor, OP-Dokumentation) mit hoher Verfügbarkeit und Geräteanbindung

Abb. 5: Darstellung einer komplexen Klinikumgebung, ESET Deutschland GmbH

IT-Sicherheit ist Vertrauenssache

Ihre IT-Sicherheit im Fokus

- Passgenaue IT-Sicherheit für alle Unternehmensgrößen und -anforderungen
- Volle Kontrolle über Ihre Daten dank transparenter (Sample-)Analysen innerhalb der EU
- Einzigartige Geschwindigkeit bei der Analyse von eingehenden Warnmeldungen
- Breite Abdeckung gesetzlicher Anforderungen (u. a. NIS2, DSGVO)
- Verwaltung der Schutzlösungen für alle gängigen Betriebssysteme via zentraler Management-Konsole (Cloud oder On-Premises)
- Flexibilität – Kombination beliebiger Betriebssysteme (Windows, macOS, Linux) und Geräte (Clients, Server, Mobilgeräte) entsprechend der Bedürfnisse

Vorteile für Ihr Krankenhaus

- Überall verfügbar – vollautomatischer Schutz der gesamten Krankenhaus-Infrastruktur
- Mitarbeitende entlasten und Ressourcen schonen dank umfassenden MDR-Services
- Eigenes Security Operations Center (SOC) in Deutschland mit hochqualifiziertem, erfahrenem Team als Teil von ESETs globalem Netzwerk
- Zertifizierte Sicherheitslösungen für zuverlässigen Schutz (z. B. ISO und Common Criteria)
- Hoher Automatisierungsgrad durch Schwachstellen- und Patch-Management sowie dynamische Gruppen
- Schnelle und professionelle Hilfe dank lokalem Kunden-Support für Deutschland, Österreich und die Schweiz



„Als Security-Hersteller bieten wir moderne Lösungen, Dienstleistungen und Konzepte an, mit denen Unternehmen und Verwaltungen eine Cyberresilienz auf höchstem Niveau gestalten können.“

— Holger Suhl, Country Manager DACH,
ESET Deutschland GmbH

Quellenverzeichnis

- 1 https://www.bka.de/DE/AktuelleInformationen/StatistikenLagebilder/Lagebilder/Cybercrime/2024/CC_2024.html
- 2 <https://medien.bsi.bund.de/lagebericht/de/index.html>
- 3 https://kommunalwiki.boell.de/index.php/Cyberangriffe_auf_Krankenh%C3%A4user#cite_note-2
- 4 [https://www.enisa.europa.eu/sites/default/files/publications/Health Threat Landscape.pdf](https://www.enisa.europa.eu/sites/default/files/publications/Health%20Threat%20Landscape.pdf)
- 5 https://kommunalwiki.boell.de/index.php/Cyberangriffe_auf_Krankenh%C3%A4user#2025
- 6 <https://www.aok.de/pp/gg/gesundheitswesen/interview-cyberkriminalitaet-gesundheitswesen>
- 7 https://www.dsgvo-portal.de/sicherheitsvorfaelle/ransomware_angriff_bezirkskliniken-mittel-franken-4143.php
- 8 https://www.dsgvo-portal.de/sicherheitsvorfaelle/ransomware_angriff_klinikenverbund-im-4253.php
- 9 https://www.dsgvo-portal.de/sicherheitsvorfaelle/ransomware_angriff_wertachkliniken-bobingen-6447.php
- 10 <https://www.ndr.de/nachrichten/mecklenburg-vorpommern/hackerangriff-auf-it-systeme-an-ameos-kliniken,ameoskliniken-100.html>
- 11 <https://www.bitkom.org/Presse/Presseinformation/Cybersicherheit-Bundestag-NIS2>
- 12 <https://www.heise.de/hintergrund/Cyberangriffe-auf-Krankenhaeuser-Ransomware-kann-Patientenleben-gefaehrden-9608151.html>
- 13 <https://www.datenschutz-notizen.de/fehlendes-berechtigungskonzept-im-krankenhaus-ein-bussgeld-bewaehrtes-risiko-0823168/>
- 14 <https://www.aerztezeitung.de/Wirtschaft/Klinik-wird-fuer-Datenpanne-bestaft-404679.html>
- 15 https://www.dkgev.de/fileadmin/default/Mediapool/2_Themen/2.1_Digitalisierung_Daten/2.1.4._IT-Sicherheit_und_technischer_Datenschutz/2.1.4.3._IT-Sicherheit_im_Krankenhaus_75c/GF-Info-75c-SGB-V_v098.pdf
- 16 <https://www.dkgev.de/themen/digitalisierung-daten/informationssicherheit-und-technischer-datenschutz/informationssicherheit-im-krankenhaus/>
- 17 <https://de.wikipedia.org/wiki/NIS-2-Richtlinie>
- 18 https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2025/251113_NIS-2-Umsetzungsgesetz.html
- 19 <https://www.bmi.bund.de/SharedDocs/pressemitteilungen/DE/2025/09/kritis-dg-kabinett.html>
- 20 https://www.gesetze-im-internet.de/bsig_2025/_30.html
- 21 https://www.bsi.bund.de/DE/Themen/Regulierte-Wirtschaft/NIS-2-regulierte-Unternehmen/NIS-2-Pflichten/nis-2-pflichten_node.html
- 22 https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/NIS-2/nis-2-geschaeftsleitungsschulung.pdf?__blob=publicationFile&v=3
- 23 https://www.bka.de/DE/AktuelleInformationen/StatistikenLagebilder/Lagebilder/Cybercrime/2024/CC_2024.html
- 24 https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Analysen-und-Prognosen/Ransomware-Angriffe/ransomware_angriffe_node.html
- 25 https://www.bka.de/DE/AktuelleInformationen/StatistikenLagebilder/Lagebilder/Cybercrime/2024/CC_2024.html
- 26 <https://go.eset.com/eset-dach/eset-studie-de-made-in-eu>
- 27 <https://www.verfassungsschutz.de/SharedDocs/kurzmeldungen/DE/2025/2025-09-18-studie-bitkom.html>
- 28 <https://go.eset.com/eset-dach/flyer-nis2-richtlinien-eset-loesungen>
- 29 <https://www.din.de/de/meta/suche/63612!search?query=iso+9001>
- 30 <https://www.din.de/de/meta/suche/62730!search?query=27001>
- 31 https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Zero-Trust/zero-trust_node.html
- 32 <https://www.eset.com/at/business/services/managed-detection-and-response>
- 33 https://web-assets.eset.com/fileadmin/ESET/DACH/Docs/Business/Case_Studies/Case_Study_Klinikum-Landshut_2025_WEB.pdf

Abbilungsverzeichnis

Abbildung 1: Schematische Darstellung der Kliniken mit mindestens einem Sicherheitsvorfall in Deutschland, ESET Deutschland GmbH; Quelle: <https://www.aok.de/pp/gg/gesundheitsystem/interview-cyberkriminalitaet-gesundheitswesen>

Abbildung 2: Kosten eines Cybervorfalls im DACH-Gesundheitswesen, DKI, BSI, NCSC Schweiz, ENISA, Analogie zu europäischen Healthcare-Kosten;

Quellen:
<https://www.bitkom.org/Presse/Presseinformation/Wirtschaft-ruft-nach-deutscher-Cloud>

<https://www.eset.com/at/about/presse/pressemitteilungen/pressemitteilungen/eset-umfrage-mehrheit-deutscher-unternehmen-setzt-bei-der-it-sicherheit-auf-made-in-eu/>

<https://www.krankenhaus-it.de/item.5099/gesundheitswesen-durch-cyberangriffe-geschaedigt.html>

<https://www.imprivata.com/de/blog/hackerangriffe-auf-krankenhaeuser-wie-koennen-sich-krankenhaeuser-besser-schuetzen>

<https://www.europeanfinancialreview.com/gartner-why-digital-sovereignty-is-now-every-cios-survival-strategy/>

Abbildung 3: Vereinfachte Darstellung einer Klinikumgebung, ESET Deutschland GmbH

Abbildung 4: Infografik zur Ransomware-Behebung, ESET Deutschland GmbH

Abbildung 5: Darstellung einer komplexen Klinikumgebung, ESET Deutschland GmbH

3 VON ÜBER 500.000 ZUFRIEDENEN KUNDEN



**CHAMPION
PARTNER**

Seit 2019 ein starkes Team
auf dem Platz und digital



Seit 2022 durch ESET geschützt
Mehr als 1.450 Postfächer



ISP Security Partner seit 2008
2 Millionen Kunden

BEWÄHRT



ESET wurde das Vertrauensiegel
„IT Security made in EU“ verliehen



Unsere Lösungen sind nach den
Qualitäts- und Informations-
sicherheitsstandards ISO 9001:2015
und ISO/IEC 27001:2022 zertifiziert

ESET IN ZAHLEN

110.000.000+

**Geschützte Nutzer
weltweit**

178

**Länder &
Regionen**

500.000+

**Geschützte
Unternehmen**

12

**Forschungs- und
Entwicklungs-
zentren weltweit**



eset® **BLOG**

ESET Deutschland GmbH
Spitzweidenweg 32 | 07743 Jena | Tel.: +49 3641 3114 200



[ESET.DE/HEALTHCARE](https://www.eset.de/healthcare)

