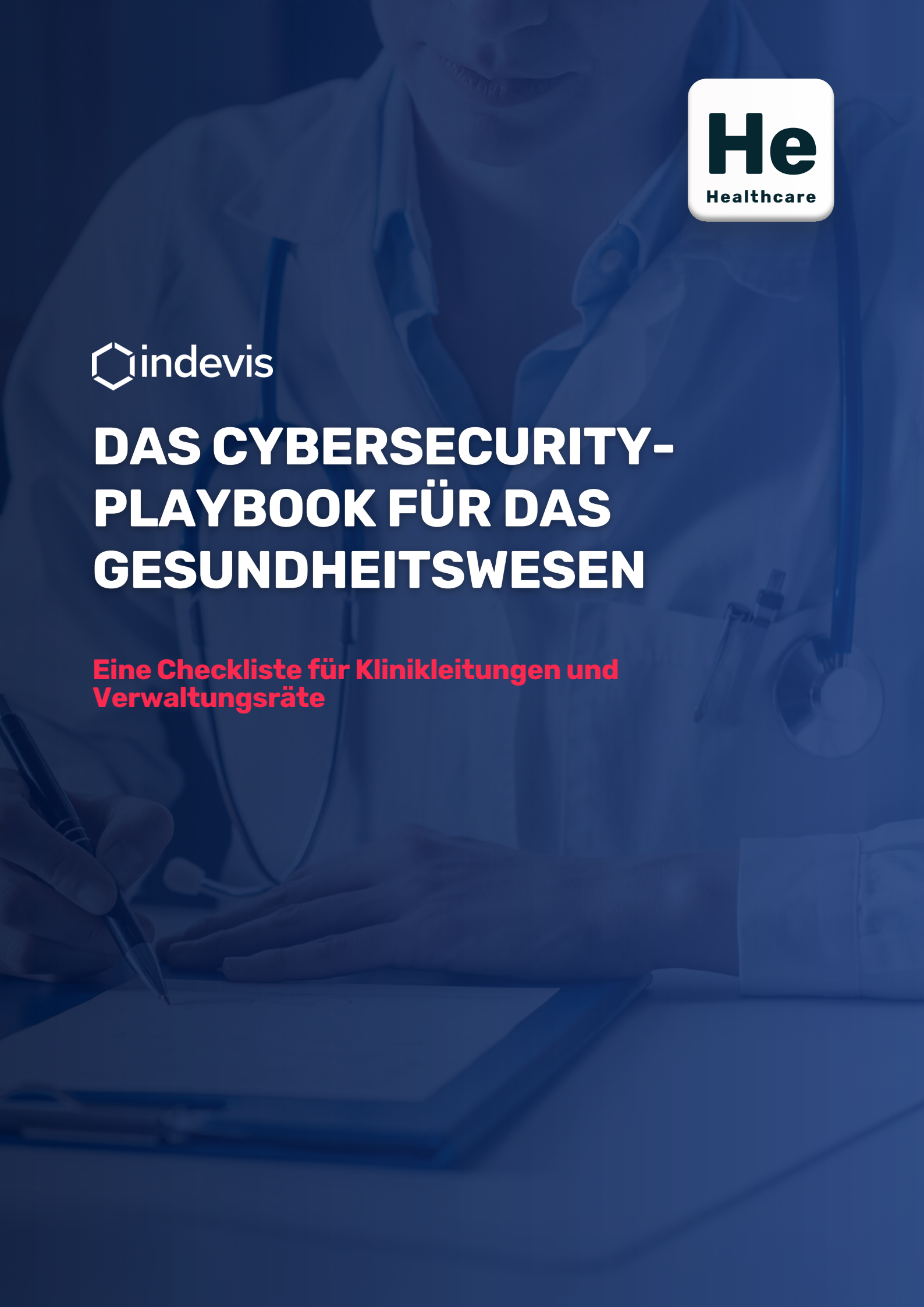

indevis

DAS CYBERSECURITY-PLAYBOOK FÜR DAS GESUNDHEITSWESEN

Eine Checkliste für Klinikleitungen und Verwaltungsräte

Warum dieses Playbook?

Ein Cyberangriff kann in Sekunden vernichten, wofür Sie Jahre gearbeitet haben.
Im Gesundheitswesen steht damit mehr auf dem Spiel als Reputation und wirtschaftliche Stabilität: Es geht um die Sicherheit von Patientinnen und Patienten.

Laut dem IBM Cost of Data Breach Report 2025[1] bleibt Healthcare der am stärksten betroffene Sektor. Im Schnitt verursachte ein Vorfall **6,36 Mio. Euro** Schaden – bereits das 14. Jahr in Folge mit den höchsten Kosten aller Branchen. Angreifer wissen genau, warum sie Kliniken, Labore und Praxen ins Visier nehmen: Patientendaten sind eine Goldgrube. Sie werden für Identitätsdiebstahl, Versicherungsbetrug oder andere Formen der Finanzkriminalität gezielt ausgenutzt.
Besonders alarmierend: Kein anderer Sektor braucht so lange, um Angriffe zu erkennen und einzudämmen. Im Gesundheitswesen dauert es durchschnittlich **279 Tage**, bis ein Vorfall unter Kontrolle ist – mehr als fünf Wochen länger als im weltweiten Durchschnitt. In dieser Zeit können Angreifer Systeme lahmlegen, Daten entwenden und Vertrauen irreparabel zerstören.

Das Fazit ist eindeutig: Cybersecurity im Healthcare-Sektor ist keine Option, sondern eine klinische Notwendigkeit.

Für Klinikleitungen und Verwaltungsräte gilt: Mangelnde Cyber-Resilienz ist ein existenzielles Risiko für Patienten, Mitarbeitende und die Institution selbst.

Die Incident-Response- und Threat-Intelligence-Teams von indevis haben hunderte Angriffe analysiert und daraus die wichtigsten Lehren gezogen – einschließlich Maßnahmen, die sich Unternehmen und Organisationen im Nachhinein gewünscht hätten. Dieses Playbook fasst diese Erkenntnisse zusammen und bietet eine praxisorientierte Anleitung, wie sich Healthcare-Einrichtungen auf Cyber-Vorfälle vorbereiten, sie bewältigen und überstehen können.

Neben einer fünfstufigen Checkliste, die Ihnen hilft, Cyber-Resilienz systematisch aufzubauen, erhalten Sie mit der Cyber-Sicherheitsampel ein Instrument zur schnellen Bewertung des Sicherheitsstatus Ihrer Einrichtung.

Versorgungskontinuität sichern: Cybersecurity als Pflichtaufgabe im Healthcare-Sektor

Cybersecurity ist längst mehr als ein IT-Thema – sie ist ein Schlüsselfaktor für Versorgungssicherheit und Patienten-wohl. Besonders Angriffe auf kritische Infra-strukturen nehmen zu.
Fehlende Sicherheitsmaßnahmen führen nicht nur zu finanziellen Schäden, sondern können den Klinikbetrieb lahmlegen – mit unmittelbaren Folgen für die medi-zinische Versorgung. Laut dem Ponemon Healthcare Cybersecurity Report 2024[2] berichteten 56 % der Einrichtungen von **schlechteren Behandlungs-ergebnissen** durch verzögerte Eingriffe, 28 % sogar von erhöhter **Patientensterblichkeit**.

Beispiele aus der Praxis bestätigen das Bild: Im Juli 2025 wurde das AMEOS-Kliniknetzwerk mit **über 100 Einrichtungen** in Deutschland Opfer eines Cyberangriffs – sämtliche IT-Systeme mussten heruntergefahren werden. Kommunikation, Dokumentation und Bild-gebungssysteme fielen aus, was die Versorgung massiv behinderte.[3] Im Februar 2025 traf es die LUP-Kliniken in Ludwigslust und Hagenow – **zentrale Systeme wurden verschlüsselt**, die Klinik erpresst – mit der Folge, dass Abläufe drastisch gestört wurden und die Versorgung unter großem Druck stand.[4]

69 %

durchschnittlich der Einrichtungen berichten von Unterbrechungen der Patientenversorgung (Ponemon Healthcare Cybersecurity Report 2024)[2]

92 %

der Organisationen erlebten einen Cyberangriff in den letzten 12 Monaten (Ponemon Healthcare Cybersecurity Report 2024)[2]

„Einhundert Prozent Cybersicherheit gibt es nicht und wird es nie geben. Die Frage ist deswegen nicht ob, sondern wann ein erfolgreicher Cyberangriff stattfindet. Wir müssen das Cybersicherheitsniveau in Deutschland daher insgesamt substantiell erhöhen.“[9]

Claudia Plattner, BSI-Präsidentin

Cybersecurity in 5 Schritten

Cyber-Resilienz ist heute ein zentraler Pfeiler für jede Organisation im Gesundheitswesen – von Kliniken über Labore und Pflegeeinrichtungen bis hin zu Krankenkassen und Medizintechnik.
Wer Cyber-Risiken wirksam steuern will, darf sie nicht isoliert betrachten, sondern fest im im strategischen Rahmen von Governance, Compliance und Versorgungssicherheit verankern. Genau hier setzt unsere Checkliste an: Sie bietet Healthcare-Entscheidern einen klaren, praxisnahen Fahrplan, um Cyber-Resilienz strukturiert aufzubauen, Risiken zu minimieren und die Qualität der Versorgung langfristig abzusichern.

1. Cyber-Risiken in die Führungsebene integrieren

Cyber-Resilienz beginnt im Management. Damit Sicherheitsfragen nicht als reine IT-Aufgabe behandelt werden, sollten Führungsgremien im Gesundheitswesen – ob Klinikleitungen, Vorstände von Krankenkassen oder Geschäftsführungen von Laboren und Pflegeeinrichtungen – ein Governance-Modell etablieren, in dem Cyber-Risiken fester Bestandteil der Unternehmenssteuerung sind. Die Verantwortung für Cybersicherheit muss klar zugewiesen, regelmäßig überprüft und in den Entscheidungsgremien transparent gemacht werden.

Kernmaßnahmen zur Umsetzung:

Durchführung einer Cyber-Resilience- / Risikoanalyse (CRA)

- Einschätzung der Sicherheitslage mittels Threat-Led Profiling
- Gap-Analyse zur Abdeckung bestehender Risiken durch die Cyber-Versicherung
- Penetrationstests zur Validierung der Verteidigungsmechanismen
- Klassifizierung technischer Risiken nach der OWASP Top 10 Infrastructure Security Risks, z. B. unzureichende Zugangskontrollen, fehlende Netzwerksegmentierung, unsichere Standardkonfigurationen, schwaches Patch-Management
- Bewertung der identifizierten Bedrohungen anhand von Eintrittswahrscheinlichkeit und wirtschaftlichem Schaden

Einführung eines quartalsweisen Cyber-Reportings zur

- Analyse der aktuellen Bedrohungslage
- Bewertung von Erkennungsleistung und Resilienzgrad
- Aktualisierung von Notfallplänen und Reaktionsrichtlinien

2. Cyber-Resilienz-Strategie entwickeln

Eine gute Strategie erkennt nicht nur Risiken – sie priorisiert, schützt, reagiert und stellt im Ernstfall alles wieder her. Das Ziel ist eine Resilienzarchitektur, die dem Prinzip folgt: „Identify, Protect, Detect, Respond, Recover."

Vorgehensweise:

Risikoanalyse und Bedrohungsbewertung durchführen

- Risiken identifizieren und quantifizieren
- Auswirkungen auf Patientenversorgung, Finanzen und Reputation erfassen

Prioritäten und Ressourcen festlegen

- Höchste Risiken priorisieren und ressourcenschonend adressieren
- Budgetplanung mit dem Management abstimmen

Strategie mit Geschäftszielen verbinden

- Sicherheitsziele klar formulieren
- Gap-Analyse zwischen Ist- und Soll-Zustand durchführen
- Wertvollste Assets identifizieren und absichern
- Business-Continuity- und Disaster-Recovery-Pläne regelmäßig testen und aktualisieren

3. Schulungen & Awareness auf Managementebene

Kontinuierliche Schulungen stellen sicher, dass das Management und die wichtigsten Teams Cyber-Risiken besser einschätzen und im Ernstfall angemessen reagieren können.

Vorgehensweise:

- Regelmäßige Management-Trainings zu aktuellen Cyber-Bedrohungen und regulatorischen Pflichten durchführen
- Awareness-Programme für alle Mitarbeitenden etablieren, mit Fokus auf Phishing, Passwortsicherheit und Incident-Reporting
- Spezialisierte Vertiefungstrainings für Hochrisikobereiche wie IT und Finanzen anbieten
- Einen Cyber-Verantwortlichen ernennen, der Zuständigkeiten definiert und regelmäßig an die Geschäftsführung berichtet

4. Incident-Response-Bereitschaft herstellen

Eine vorbereitete und getestete Incident-Response-Strategie ermöglicht es, Schäden zu begrenzen und Ausfallzeiten zu minimieren, wenn ein Angriff eintritt.

Vorgehensweise:

- Incident-Response-Plan (IR) entwickeln und regelmäßig durch Simulationen (z. B. Tabletop-Übungen) testen
- Krisenkommunikation vorbereiten: interne und externe Kommunikationswege (Patienten, Medien, Behörden) definieren
- Externe Incident-Response-Dienste frühzeitig vertraglich sichern und in Notfallprozesse einbinden
- Nach Tests Lessons Learned dokumentieren und Pläne fortlaufend optimieren

5. Kontinuierlich überwachen und anpassen

Da sich Bedrohungen und regulatorische Anforderungen ständig ändern, muss die Cybersicherheitsstrategie laufend überprüft und angepasst werden.

Vorgehensweise:

- 24/7-Überwachung über MDR (Managed Detection and Response)/SOC (Security Operations Center)-Services etablieren, um Angriffe frühzeitig zu erkennen
- Regelmäßige Schwachstellenscans und Audits durchführen und Prioritäten dynamisch anpassen
- KPIs wie Reaktionszeit und Wiederherstellungszeit messen und verbessern
- Neue Vorgaben (z. B. NIS-2, DSGVO, IT-SiG) fortlaufend integrieren

Neue Cybersecurity-Pflichten: Was Sie wissen müssen

In der DACH-Region steigen die regulatorischen Anforderungen an Cybersicherheit – mit direkter Auswirkung auf Patientensicherheit, Versorgungsqualität und Haftungsrisiken.

Strengere Pflichten

- **NIS-2:** Gesundheitsorganisationen gelten in vielen Fällen als kritische Infrastrukturen (KRITIS). Sie sind verpflichtet, ein strukturiertes Cyber-Risikomanagement aufzubauen, präventive Maßnahmen einzuleiten und ihre IT-Systeme kontinuierlich zu überwachen.
- Im Falle eines Cyberangriffs gelten strenge Meldepflichten ähnlich wie bei der DSGVO.
- Gefordert sind einheitliche europäische Mindeststandards: u. a. technische Schutzmaßnahmen, Notfallpläne, regelmäßige Audits und Risikobewertungen.
- Die **DSGVO** regelt den Umgang mit sensiblen personenbezogenen Daten, inklusive Meldepflichten bei Datenschutzverletzungen.
- Das **IT-Sicherheitsgesetz** enthält ergänzende Anforderungen für Betreiber kritischer Infrastrukturen (KRITIS), darunter insbesondere zusätzliche Nachweis- und Meldepflichten gegenüber dem Bundesamt für Sicherheit in der Informationstechnik (BSI).

Sanktionen

Bis zu **20 Mio. €** oder 4 % Umsatz

- **Bußgelder:** Bis zu 10 Mio. Euro oder 2 % Umsatz nach NIS-2; bis zu 20 Mio. Euro oder 4 % Umsatz nach DSGVO
- **Aufsichtsmaßnahmen:** Prüfungen, Audits oder im Extremfall Betriebseinschränkungen durch Behörden
- **Reputationsrisiken:** Öffentlich gewordene Verstöße untergraben das Vertrauen von Patienten, Partnern und Kostenträgern
- **Zivilrechtliche Folgen:** Schadenersatzforderungen von Patienten, Partnern oder Gesellschaftern
- **Persönliche Haftungsfolgen:** Geschäftsführungen, Vorstände und Aufsichtsgremien haften persönlich, wenn sie ihrer Pflicht zur Umsetzung angemessener Cyber-Sicherheitsmaßnahmen nicht nachkommen.

Für Verantwortliche im Gesundheitswesen gilt: Cybersecurity ist nicht länger nur ein IT-Thema, sondern ein entscheidender Faktor für Patientensicherheit, Compliance und Vertrauen. Wer NIS-2, DSGVO und IT-SiG ignoriert, riskiert nicht nur hohe Bußgelder und persönliche Haftung, sondern auch Versorgungsausfälle, Reputationsverluste und den Wegfall öffentlicher Fördermittel oder Partnerschaften. Frühzeitige Compliance schützt vor Sanktionen, stärkt das Vertrauen von Patienten, Kostenträgern und Investoren und sichert so die Zukunftsfähigkeit und Resilienz des gesamten Gesundheitsbetriebs.

Cyber-Sicherheitsampel: Ihr 10-Punkte-Check

Die Cybersicherheitsampel ist ein kompaktes Bewertungsinstrument, um den Sicherheitsstatus von Organisationen schnell und vergleichbar zu erfassen.
Sie basiert auf 10 Kernfragen zu entscheidenden Schutzmaßnahmen.
Wichtig: Kein „✓“ ohne Nachweis akzeptieren! Nur belegte Antworten (z. B. Berichte, Policies, Screenshots) zählen in die Bewertung ein.

10-Fragen-Ampel-Check

1. Ist ein 24/7 Security Operations Center (SOC) oder Managed Detection & Response (MDR) aktiv? ☐

Nachweis: Vertrag, SLA-Berichte

2. Gibt es einen Incident-Response-Plan, der getestet wurde? ☐

Nachweis: IR-Plan, Protokoll der letzten Übung

3. Wurde in den letzten 12 Monaten ein Penetrationstest durchgeführt? ☐

Nachweis: vollständiger Report inkl. Findings

4. Liegt eine dokumentierte IT-/OT-Risikobewertung vor? ☐

Nachweis: Board-Abnahme, Gap-Analyse

5. Werden regelmäßig Awareness-Trainings für Mitarbeitende durchgeführt? ☐

Nachweis: Teilnehmerlisten, Schulungskonzepte

6. Ist Multifaktor-Authentifizierung (MFA) für kritische Systeme implementiert? ☐

Nachweis: Screenshots, Audit-Bericht

7. Ist eine Netzwerksegmentierung umgesetzt, um kritische Systeme zu isolieren? ☐

Nachweis: Architekturdiagramm

8. Existiert ein dokumentiertes Schwachstellen-Management? ☐

Nachweis: Compliance-Reports

9. Wurden Backup- und Recovery-Tests innerhalb der letzten 12 Monate durchgeführt? ☐

Nachweis: Testprotokoll, RTO/RPO

10. Besteht eine aktive und geprüfte Cyberversicherung inklusive Sublimits? ☐

Nachweis: Versicherungspolice

Bewertungssystem:

- Rot (<6 ✓): Kritisch – hohe Risiken, sofortige Maßnahmen erforderlich
- Gelb (6–8 ✓): Mittel – moderate Risiken, Handlungsbedarf, mittelfristig optimierbar
- Grün (9–10 ✓): Sehr gut – geringe Risiken, hohe Resilienz

Roadmap to Security

Cyberangriffe lassen sich nicht vollständig verhindern – aber ihre Auswirkungen können drastisch reduziert werden, wenn die richtigen Maßnahmen rechtzeitig umgesetzt werden. Unsere Roadmap to Security bietet Gesundheitseinrichtungen einen klaren, strukturierten Fahrplan, um Cyber-Resilienz aufzubauen und regulatorische Anforderungen einzuhalten.

Die Roadmap umfasst:

Sicherheitsbewertung:
Umfassende Prüfung des aktuellen Cyber-Reifegrads (inkl. IT- und Medizintechnik-Systeme)

Investitionsplanung:
5-Jahres-Plan für Cybersecurity-Maßnahmen mit CapEx/OpEx-Transparenz

Regulatorik-Check:
Identifikation relevanter Anforderungen aus NIS-2-Richtlinie

Ampelbericht & Maßnahmenplan:
Standardisierte Reifegradbewertung und priorisierte Handlungsschritte

Workshop mit Ihrem Führungsteam:
Gemeinsame Abstimmung der Maßnahmen und Verantwortlichkeiten

Integration von IT- und OT-Sicherheit:
Berücksichtigung von Produktions- und IoT-Umgebungen

Ihr Nutzen:

- Klare Faktenbasis für Investmententscheidungen
- Planungssicherheit durch transparente Kosten- und Ressourcenabschätzung.
- Standardisierte Sicherheitsstrukturen, die besonders für große Klinikverbünde und Netzwerke im Gesundheitswesen unverzichtbar sind.

Ihr Partner für Cyber-Resilienz

Die **indevis GmbH** vereint technische Stärke, operative Verlässlichkeit und rechtliche Expertise, um Unternehmen und Einrichtungen in einer zunehmend vernetzten Welt ganzheitlich zu schützen.

Unser Leistungsversprechen:

- Ein 24/7 Security Operations Center (SOC) mit Standort in Deutschland
- ISO-27001-zertifizierte Prozesse für höchste Sicherheits- und Compliance-Standards
- Incident Response & Digitale Forensik – schnelle Reaktion und Analyse im Ernstfall
- Regulatorik-Expertise: NIS-2 und DSGVO im Blick für Compliance

SOS **Notfallkontakt (24/7):** +49 (0) 89 45 24 24-112

Mehr erfahren

Für weitere Informationen besuchen Sie uns auf unserer Website - einfach den QR-Code scannen oder über:
www.indevis.de/roadmap-to-security

SCAN ME

Bereit, Ihre Einrichtung cyber-resilient zu machen?

Warten Sie nicht auf den nächsten Angriff – handeln Sie jetzt.
Ob Gap-Analyse, Ampel-Check oder Roadmap-Entwicklung – wir zeigen Ihnen, wo Ihre Einrichtung heute steht und wie Sie Cybersecurity gezielt als Schutz für Versorgungssicherheit und Patientenwohl einsetzen können.

sales@indevis.de
+49 (0) 89 45 24 24-100
indevis

Quellen

1. IBM (2025). Cost of a Data Breach Report 2025. https://www.ibm.com/de-de/reports/data-breach
2. Ponemon/Proofpoint (2024). Healthcare Cybersecurity Report 2024. https://ponemonsullivanreport.com/2024/10/the-2024-study-on-cyber-insecurity-in-healthcare-the-cost-and-impact-on-patient-safety-and-care/
3. Marie-Claire Koch (2017): Ameos-Kliniken: Cyberangriff sorgt für eingeschränkte Versorgung. In: heise online, 09.07.2025. https://www.heise.de/news/Ameos-Kliniken-Wegen-IT-Ausfall-keine-Roentgen-Laboruntersuchungen-moeglich-10481173.html
4. NDR (2025). Nach Cyberangriff auf LUP-Kliniken: Offenbar Patientendaten gestohlen, 19.02.2025. https://www.ndr.de/nachrichten/mecklenburg-vorpommern/Nach-Cyberangriff-auf-LUP-Kliniken-Offenbar-Patientendaten-gestohlen,lupkliniken102.html
5. Plattner, Claudia (2024). Pressemitteilung: BSI will die „Cybernation Deutschland“ bauen. https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2023/231010_it-sa_Cybernation.html