SECJUR

# NIS2 für die Gesundheitsbranche

Warum Krankenhäuser, Kliniken und Medizintechnik zu den kritischsten NIS2-Sektoren zählen, und wie Readiness gelingt.

Gesundheitseinrichtungen und Medizintechnikhersteller sind als **besonders wichtige Einrichtungen** in Annex 1 der NIS2-Richtlinie gelistet und unterliegen den strengsten Anforderungen des **NIS2-Umsetzungsgesetzes (NIS2UmsuCG)**. Krankenhäuser mit mehr als 50 Betten sowie Hersteller kritischer Medizinprodukte sind automatisch betroffen. Besonders exponiert: Patientendaten, medizinische IT-Systeme und vernetzte Medizintechnik.

## In diesen vier Situationen wird NIS2 für Gesundheitseinrichtungen konkret:

BETROFFENHEIT & EINSTUFUNG

### Annex 1, besonders wichtig

- Krankenhäuser, Labore, Medizintechnik und Pharma unter Annex 1
- Als besonders wichtige Einrichtungen eingestuft
- Bei Krankenhäusern unabhängig von der Unternehmensgröße
- Frühe Einordnung nach §28 NIS2UmsuCG verhindert Überraschungen

PATIENTENDATEN & DSGVO

### Zwei Regime greifen ineinander

- Gesundheitseinrichtungen verarbeiten hochsensible Patientendaten
- Datenschutzverletzungen lösen oft NIS2 und DSGVO gleichzeitig aus
- Meldepflichten nach Art. 33 DSGVO und §32 NIS2UmsuCG
- Integrierter Ansatz für Datenschutz und Informationssicherheit ist Pflicht

MEDIZINISCHE IT & GERÄTE

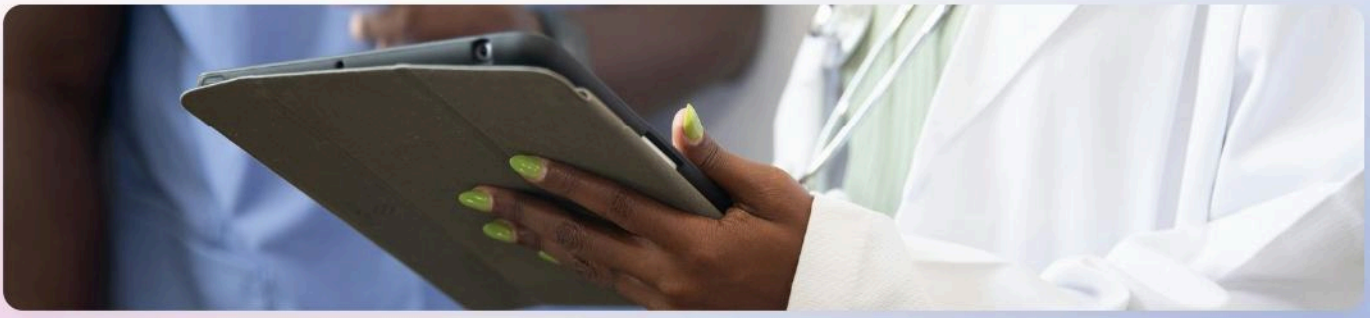
### Angriffsziel klinische Systeme

- Vernetzte Medizingeräte, KIS, PACS und LIS sind primäre Angriffsziele
- Ein Angriff auf klinische Systeme gefährdet direkt Menschenleben
- NIS2 fordert Angriffserkennung, Segmentierung, Notfallbetrieb
- Gilt ausdrücklich auch für medizinische IT

LEITUNGSHAFTUNG & BSI

### Chefsache mit Bußgeldrisiko

- Management haftet persönlich für Sicherheitsmaßnahmen (§38)
- KRITIS-Krankenhäuser: BSI-Registrierung und Prüfung alle drei Jahre
- Bußgelder bis 10 Mio. Euro oder 2 % des globalen Jahresumsatzes
- Cybersicherheit wird zur Chefsache



**Annex 1**
Gesundheitssektor als besonders wichtige Einrichtung, höchste NIS2-Pflichtklasse

**24 h**
Frist für die Erstmeldung erheblicher Sicherheitsvorfälle an BSI/Behörde

**bis 10 Mio. €**
Maximales Bußgeld für besonders wichtige Einrichtungen bei Verstößen

SECJUR

# NIS2-Readiness in 6 Schritten

Von der Betroffenheitsprüfung bis zur KRITIS-Auditfähigkeit, strukturiert und auf Kliniken, Labore und Medizintechnik zugeschnitten.

SCHRITT 01

## Betroffenheit klären

- [ ] **Einstufung** als besonders wichtige Einrichtung nach Annex 1 prüfen (§28)
- [ ] **KRITIS-Schwellenwerte** für Krankenhäuser und Labore prüfen
- [ ] **Tochtergesellschaften** und MVZ einbeziehen
- [ ] **BSI-Registrierungspflicht** für KRITIS-Betreiber klären
- [ ] **Einstufungsergebnis** schriftlich dokumentieren

SCHRITT 02

## Kritische Systeme erfassen

- [ ] **KIS, PACS, LIS** und vernetzte Medizingeräte inventarisieren
- [ ] **Schnittstellen** zu externen Laboren, Kassen und Dienstleistern dokumentieren
- [ ] **Legacy-Medizingeräte** ohne Patch-Support identifizieren
- [ ] **Verantwortlichkeiten** und Asset-Owner festlegen
- [ ] **Asset-Inventar** zentral und aktuell führen

SCHRITT 03

## Risikoanalyse & Maßnahmen

- [ ] **Bedrohungen** für klinische IT, Medizintechnik und Patientendaten bewerten
- [ ] **Netzwerksegmentierung** zwischen klinischen und administrativen Systemen
- [ ] **MFA und Zugriffskontrollen** für alle kritischen Systeme einführen
- [ ] **Maßnahmen** nach §30 Abs. 2 NIS2UmsuCG dokumentieren
- [ ] **Risiken** priorisieren und Verantwortliche zuordnen

SCHRITT 04

## Patientendaten & DSGVO

- [ ] **VVT** für Patientendaten aktualisieren
- [ ] **TOMs** für besondere Kategorien (Art. 9 DSGVO) prüfen
- [ ] **Doppelte Meldepflichten** NIS2 + DSGVO in einem Prozess zusammenführen
- [ ] **Datenschutzbeauftragten** (DSB) in ISMS-Prozesse einbinden
- [ ] **Nachweise** für beide Regime zentral ablegen

SCHRITT 05

## Vorfallsmanagement & Meldung

- [ ] **Incident-Response-Plan** für klinische IT und Medizingeräte aufbauen
- [ ] **24-Stunden-Meldekette** an BSI/Behörde einrichten und testen
- [ ] **Notbetriebskonzept** für kritische klinische Prozesse definieren
- [ ] **Meldevorlagen** für Erst- (24 h), Folge- (72 h) und Abschlussbericht
- [ ] **Verantwortliche** für den Ernstfall benennen

SCHRITT 06

## Leitung & KRITIS-Audit

- [ ] **Krankenhausleitung** und Ärztliche Direktion einbinden (§38)
- [ ] **KRITIS-Nachweisprüfung** alle 3 Jahre vorbereiten (§39 NIS2UmsuCG)
- [ ] **Awareness-Schulungen** für klinisches und administratives Personal
- [ ] **Wirksamkeitsreviews** und interne Audits einplanen
- [ ] **Kontinuierliche Verbesserung** fest verankern

SECJUR

# Häufige Stolperfallen und Quick Wins

Was Kliniken und Medizintechnikunternehmen bei NIS2 typischerweise unterschätzen, und womit sich schnell Wirkung erzielen lässt. Links die Fallen, rechts die Hebel.

STOLPERFALLE 01

## Medizingeräte als blinder Fleck

- [ ] **Vernetzte Medizintechnik** nicht als IT-Assets behandelt
- [ ] **Patch-Support** für ältere Geräte endet, Risiko wird ignoriert
- [ ] **MRT, CT und Infusionspumpen** ohne Segmentierung im Kliniknetz
- [ ] **Medizingeräte** gehören von Anfang an ins Sicherheitskonzept

QUICK WIN 01

## Netzwerksegmentierung

- [ ] **Klinische IT** von administrativen Systemen sofort trennen
- [ ] **Medizingeräte** in ein eigenes VLAN auslagern
- [ ] **Günstige Maßnahme** mit sofort spürbarer Risikoreduktion
- [ ] **Erster sichtbarer Schritt** Richtung NIS2-Readiness

STOLPERFALLE 02

## DSGVO und NIS2 getrennt gedacht

- [ ] **Zwei separate Meldeprozesse** für denselben Vorfall aufgebaut
- [ ] **DSB und IT-Sicherheitsbeauftragter** arbeiten nicht zusammen
- [ ] **Doppelter Aufwand** durch fehlende Integration der Frameworks
- [ ] **Ein Vorfall,** zwei Meldepflichten, ein gemeinsamer Prozess

QUICK WIN 02

## DSGVO-Synergie nutzen

- [ ] **Bestehende DSFA und VVT** direkt für die NIS2-Risikoanalyse verwenden
- [ ] **DSB und CISO** in einen gemeinsamen Prozess integrieren
- [ ] **Ein Framework,** doppelter Nutzen für NIS2 und DSGVO
- [ ] **Vorhandene Nachweise** gezielt wiederverwenden

STOLPERFALLE 03

## Notbetrieb nicht geprobt

- [ ] **Kein getestetes Konzept** für IT-Ausfall im laufenden Klinikbetrieb
- [ ] **Papierbasierter Notbetrieb** seit Jahren nicht aktualisiert
- [ ] **Ransomware** legt die gesamte klinische Infrastruktur lahm
- [ ] **Notbetrieb** regelmäßig üben, bevor der Ernstfall kommt

QUICK WIN 03

## Meldeprozess als 1-Seiter

- [ ] **Parallele Meldekette** NIS2 + DSGVO auf einer A4-Seite abbilden
- [ ] **Verantwortliche** für Erst-, Folge- und Abschlussmeldung benennen
- [ ] **Im medizinischen Ernstfall** enorm stressreduzierend
- [ ] **Von Unsicherheit** zu handlungsfähiger Meldekette

SECJUR

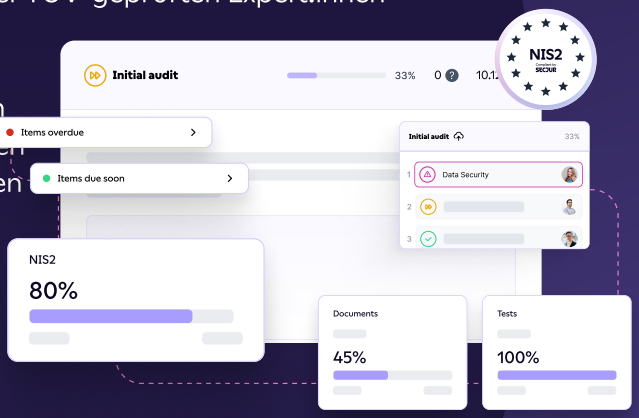
# Mit SECJUR zu 100 % NIS2-Compliance

Mit der Durchsetzung der NIS2-Richtlinie in 2026 rücken zehntausende Unternehmen neu in den regulatorischen Fokus. Die Anforderungen an Informationssicherheit, Risikomanagement und Managementverantwortung steigen spürbar – ebenso wie die Erwartungen von Aufsichtsbehörden und Geschäftspartnern.

Mit dem Digital Compliance Office von SECJUR und unseren zertifizierten Expert:innen setzen Sie die Anforderungen der NIS2-Richtlinie strukturiert und effizient um. Bestehende Sicherheits- und Governance-Strukturen werden gezielt eingebunden und systematisch weiterentwickelt.

- Aufbau und Betrieb eines NIS2-konformen ISMS inkl. Risiko- und Incident-Management
- Klare Verantwortlichkeiten, Dokumentation und Nachweise für Behörden
- Profitieren Sie von der dedizierten Erfahrung unserer TÜV-geprüften Expert:innen

Reduzieren Sie manuellen Aufwand deutlich, gewinnen Transparenz über Ihren Compliance-Status und schaffen eine belastbare Grundlage für regulatorische Prüfungen und anspruchsvolle Kundenanforderungen.




Für unsere Bestandskunden bieten wir attraktive Konditionen, um frühzeitig Klarheit zu schaffen und NIS2-Readiness planbar umzusetzen.

→ **Jetzt informieren**

Mit SECJUR zur automatisierten Compliance

**"Als Einrichtung im Gesundheitswesen mussten wir NIS2 verlässlich und prüfungssicher umsetzen. Mit SECJUR haben wir Risikoanalyse, Dokumentation und Behördennachweise zentral abgebildet, ohne unser Tagesgeschäft auszubremsen."**

**Anonym**

**Leitung IT-Sicherheit, Gesundheitswesen**

VIDEOCLINIC GSK EvoCare. St. Bernhard HOSPITAL HOMECARE viluavitartis

www.secjur.com