NIS-2 und die Caritas: Betroffenheitsanalyse, Entscheidungsbaum & Co.

Version 1.0, Stand Ende Februar 2026

Zusammengestellt von Gerhard Müller / Gerhard.Mueller@caritas-netzwerk-it.de

Inhaltsverzeichnis

Wichtige Hinweise zu diesem Dokument

Dieses Dokument dient der Orientierung und wurde von Gerhard Müller, Informatiker und Geschäftsführer vom Caritas-Netzwerk IT e. V., nach bestem Wissen und Gewissen zusammengestellt und geprüft, mit Unterstützung durch generative künstliche Intelligenz.

Das Dokument stellt keine Rechtsberatung dar, sondern hat nur informativen Charakter. Für formale juristische Beratung, insbesondere in komplexen Situationen / Rahmenbedingungen, wenden Sie sich bitte unbedingt an entsprechende Organisationen bzw. juristische Experten.

Die Refinanzierungsmöglichkeiten sind im Einzelfall und nach Bundesland unterschiedlich.

Das Caritas-Netzwerk IT e. V. / https://www.caritas-netzwerk-it.de kümmert sich unter anderem in verschiedenen Erfahrungsaustauschgruppen um (IT-)Notfallmanagement, Einführung und Nutzung von KI, Connext Vivendi, Microsoft 365 und Austausch von SoCura-Kunden (bzw. die, die es werden wollen). Die NIS-2-Thematik wurde bereits im Februar 2024 in der Erfahrungsaustauschgruppe Notfallmanagement thematisiert. Gerhard Müller & sein Kollege Mirco Beyer halten regelmäßig Vorträge und schreiben Artikel zu verschiedenen Themen rund um IT-Sicherheit inkl. NIS-2, KI, und anderen Themen, und unterstützen z.B. die IT-Leiter-Tagung im Herbst sowie organisieren für die Caritas zum wiederholten Mal einen Fachkongress Cybersecurity zusammen mit der Diakonie und V3D.

Im Anhang B finden Sie eine kurze Übersicht über den Verein, die Vereinsmitgliedschaft, die „Cyber-Feuerwehr“ und viele andere Themen.

Falls es Aktualisierungen geben sollte: Dieses Dokument ist im CariNet in der für alle offenen CariNet-Gruppe „Allgemeine Informationen zum Caritas-Netzwerk IT e. V.“ → „NIS-2 und die Caritas“ als Anhang in der jeweils aktuellsten Version verfügbar. URL für ausgedruckte Versionen:
https://ux.carinet.de/#/articles/93855732-485b-4815-9bf2-37a35ca54bcb/show

Stand: Ende Februar 2026.

1. Zusammenfassung

Das NIS-2-Umsetzungsgesetz („Gesetz zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung", kurz NIS2-RLUG, früher NIS2UmsuCG genannt) ist seit dem **6. Dezember 2025 ohne Übergangsfrist** in Kraft. Es gibt **keine pauschale Ausnahme** für gemeinnützige, kirchliche oder wohlfahrtspflegerische Träger. Die Betroffenheit richtet sich **ausschließlich** nach Sektorzugehörigkeit und Unternehmensgröße.

Auf einen Blick: Wer ist betroffen?

Einrichtungstyp	Direkt betroffen?	Einstufung
Krankenhäuser (ab 50 MA)	**JA**	Wichtig / Besonders wichtig
Reha-Kliniken (ab 50 MA)	**JA**	Wichtig / Besonders wichtig
MVZ (ab 50 MA oder >10 Mio. EUR)	**JA**	Wichtig
SoCura / ausgegl. IT (als MSP)	**JA**	Besonders wichtig
WfbM (Kfz-Zulieferer, NACE C29)	**Möglicherweise**	Prüfung erforderlich
Pflegeheime (Langzeitpflege)	Nein	Ausgenommen*
Ambulante Pflegedienste	Nein	Ausgenommen
Großküchen / Catering	Nein	Kein NIS-2-Sektor
Wäschereien	Nein	Kein NIS-2-Sektor
Kitas, Beratungsstellen	Nein	Kein NIS-2-Sektor
Rettungsdienste (Malteser)	**JA**	Anders als in ersten Aussagen des BSIs fallen Rettungsdienste DOCH unter NIS-2, siehe hier

Geschätzte Betroffenheit: Von den ca. 6.200 Caritas-Trägern dürften **300-500 Träger direkt** unter NIS-2 fallen (v.a. Krankenhausträger, Reha-Träger, IT-Dienstleister). Praktisch **alle** Träger könnten **indirekt** über Lieferketten-Anforderungen betroffen sein.

* Hinweis: Bei Komplexträgern müssen auch Pflege-IT-Systeme in den NIS-2-Scope einbezogen werden, wenn sie über gemeinsame Infrastruktur mit einem Krankenhaus verbunden sind.

2. NIS-2 im Überblick

2.1 Was ist NIS-2?

Die NIS-2-Richtlinie (EU 2022/2555) ist die europäische Richtlinie zur Netzwerk- und Informationssicherheit. Sie wurde in Deutschland durch das **NIS2-RLUG** umgesetzt, das im Wesentlichen das **BSIG (Gesetz über das Bundesamt für Sicherheit in der Informationstechnik)** novelliert.

2.2 Zeitlicher Ablauf

Datum	Ereignis
16.01.2023	NIS-2-Richtlinie EU-weit in Kraft
17.10.2024	Ursprüngliche Umsetzungsfrist (von Deutschland verfehlt)
05.12.2025	Veröffentlichung NIS2-RLUG im Bundesgesetzblatt
06.12.2025	**Inkrafttreten — OHNE Übergangsfrist**
06.01.2026	BSI-Portal für Registrierung freigeschaltet
06.03.2026	**Registrierungsfrist beim BSI**

2.3 Sektoren

Die NIS-2 erfasst **14 Sektoren** in zwei Anlagen:

Anlage 1 — Sektoren besonders wichtiger Einrichtungen (7 Sektoren): Energie, Transport und Verkehr, Finanzwesen, **Gesundheit**, Wasser, **Digitale Infrastruktur (inkl. Managed Service Provider)**, Weltraum

Anlage 2 — Sektoren wichtiger Einrichtungen (7 Sektoren): Transport und Verkehr, **Abfallbewirtschaftung**, Produktion, Herstellung und Handel mit chemischen Stoffen, **Produktion/Verarbeitung und Vertrieb von Lebensmitteln**, **Verarbeitendes Gewerbe/Herstellung von Waren**, Anbieter digitaler Dienste, Forschung

2.4 Schwellenwerte (Size-Cap-Regel)

Die Betroffenheit hängt von **Sektor + Größe** ab:

```
┌──────────────────────────────────────────────────────────────┐
│                  SCHWELLENWERTE NIS-2                        │
├──────────────────────────────────────────────────────────────┤
│                                                              │
│  BESONDERS WICHTIGE Einrichtung (Anlage-1-Sektor):           │
│  ► ab 250 Mitarbeiter                                        │
│  ► ODER: Umsatz >50 Mio. EUR UND Bilanzsumme >43 Mio. EUR    │
│                                                              │
│  WICHTIGE Einrichtung (Anlage-1- ODER Anlage-2-Sektor):      │
│  ► ab 50 Mitarbeiter                                         │
│  ► ODER: Umsatz >10 Mio. EUR UND Bilanzsumme >10 Mio. EUR    │
│                                                              │
│  KRITIS-Betreiber (z.B. Krankenhaus >30.000 Fälle/Jahr):     │
│  ► Immer besonders wichtig, größenunabhängig                 │
│                                                              │
│  Unter 50 MA UND unter 10 Mio. EUR Umsatz:                   │
│  ► Grundsätzlich NICHT betroffen (Ausnahmen: TK, DNS, KRITIS)│
│                                                              │
└──────────────────────────────────────────────────────────────┘
```

Wichtig für Caritas-Verbundstrukturen: §28 Abs. 4 BSIG enthält eine **Unabhängigkeitsklausel**: Verbundene Unternehmen werden **nicht** zusammengerechnet, wenn die Einrichtung "unter Berücksichtigung der rechtlichen, wirtschaftlichen und tatsächlichen Umstände mit Blick auf die Beschaffenheit und den Betrieb der informationstechnischen Systeme, Komponenten und Prozesse **unabhängig** ist." Dies ist für die föderale Caritas-Struktur hochrelevant — eigenständige Träger mit eigener IT können einzeln bewertet werden.

3. Die Caritas-Landschaft

3.1 Struktur in Zahlen

- **6.200** rechtlich eigenständige Träger
- **25.453** Einrichtungen und Dienste
- **739.410** hauptamtliche Mitarbeitende
- **ca. 500.000** Ehrenamtliche
- Organisiert über 27 Diözesanverbände, ~600 Orts-/Kreisverbände, 17 Fachverbände

3.2 Mitarbeitende nach Geschäftsbereich

Bereich	Mitarbeitende	NIS-2-Relevanz
Gesundheitshilfe	293.603	**HOCH**
Kinder- und Jugendhilfe	183.809	Keine
Altenhilfe	126.790	Gering (Langzeitpflege ausgenommen)
Behindertenhilfe/Psychiatrie	87.276	Differenziert
Weitere soziale Hilfen	41.320	Keine
Familienhilfe	6.612	Keine

3.3 Katholische Krankenhäuser (Primärbetroffene)

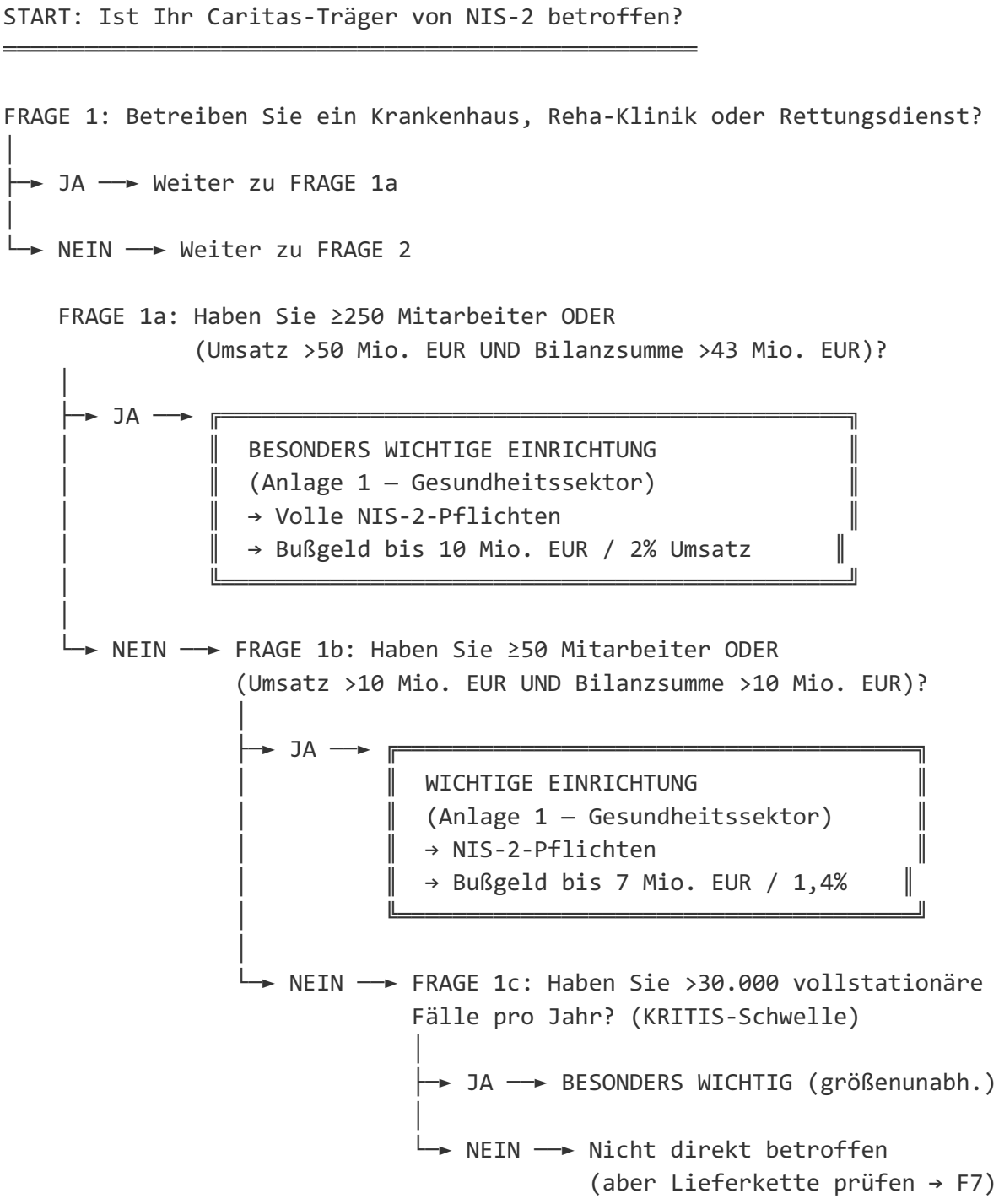
- **244 Krankenhäuser** an 320 Standorten
- **52 Reha-Einrichtungen**
- **ca. 204.000 Mitarbeitende**, **83.000 Betten**
- **Umsatzerlöse: ca. 16 Mrd. EUR jährlich**

Zahlen nach die-katholischen-krankenhaeuser.de; Größte Träger: - St. Franziskus Stiftung Münster: ~19.000 MA, ~1,6 Mrd. EUR Umsatz - Alexianer GmbH: ~34.000 MA, ca. 2 Mrd. EUR Umsatz - Contilia GmbH (Essen): ~7.500 MA, >500 Mio. EUR - BBT-Gruppe, Marienhaus Stiftung, Josefs-Gesellschaft

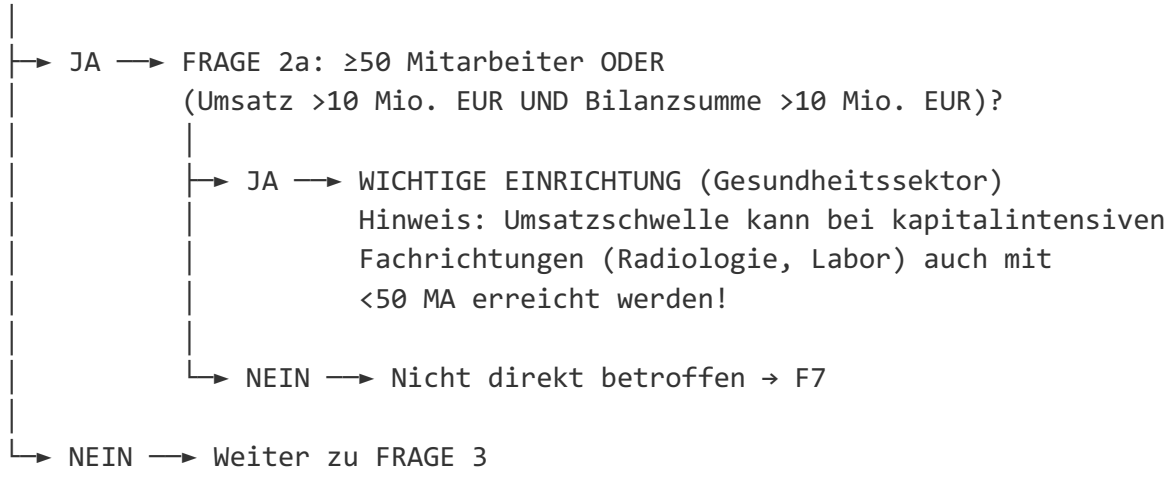
4. Entscheidungsbaum zur Selbsteinordnung

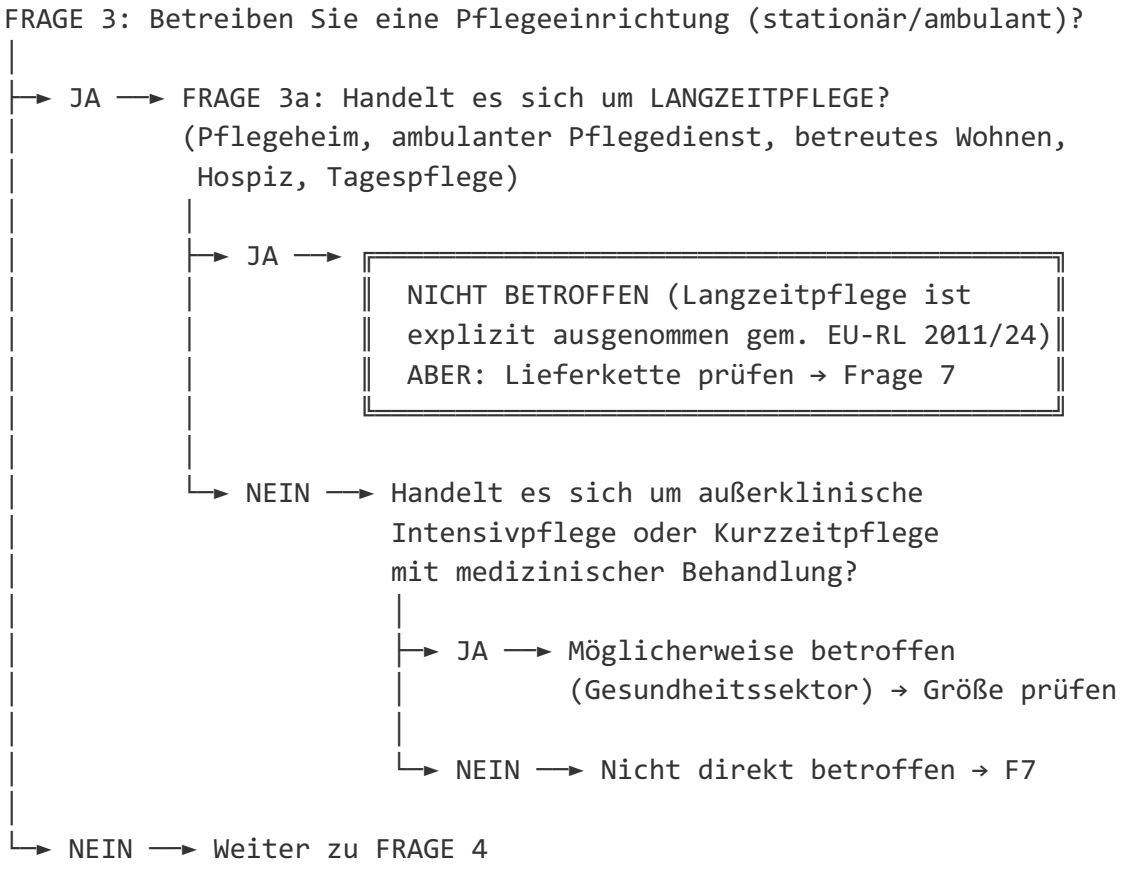
4.1 Anleitung

Gehen Sie die folgenden Fragen **der Reihe nach** durch. Die erste zutreffende Kategorie bestimmt Ihre Einstufung.

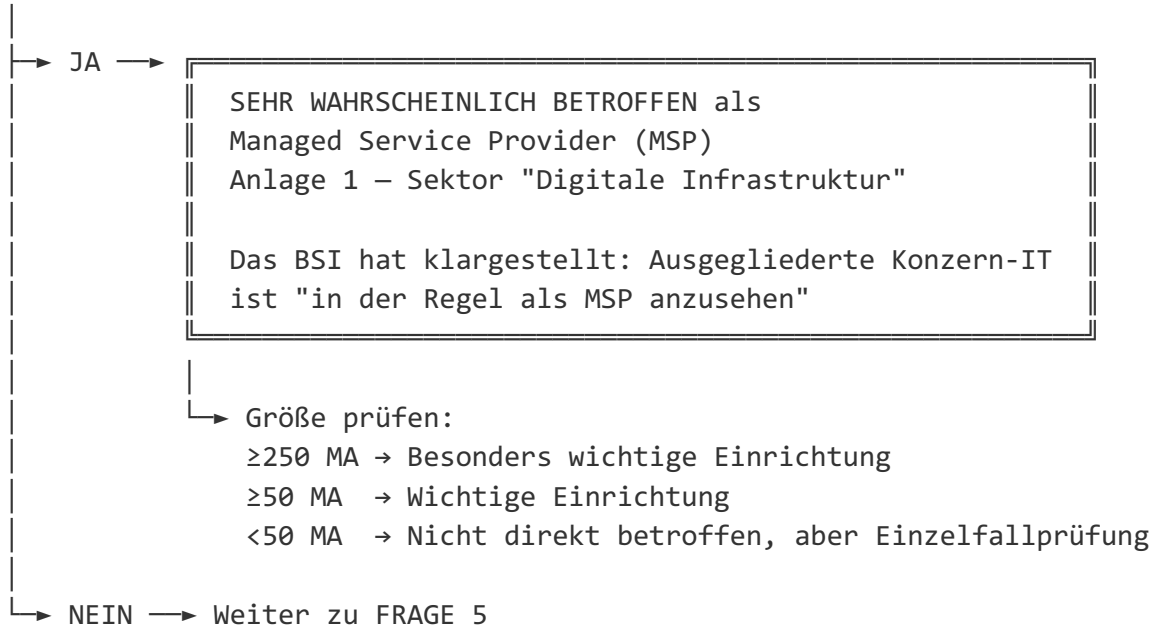


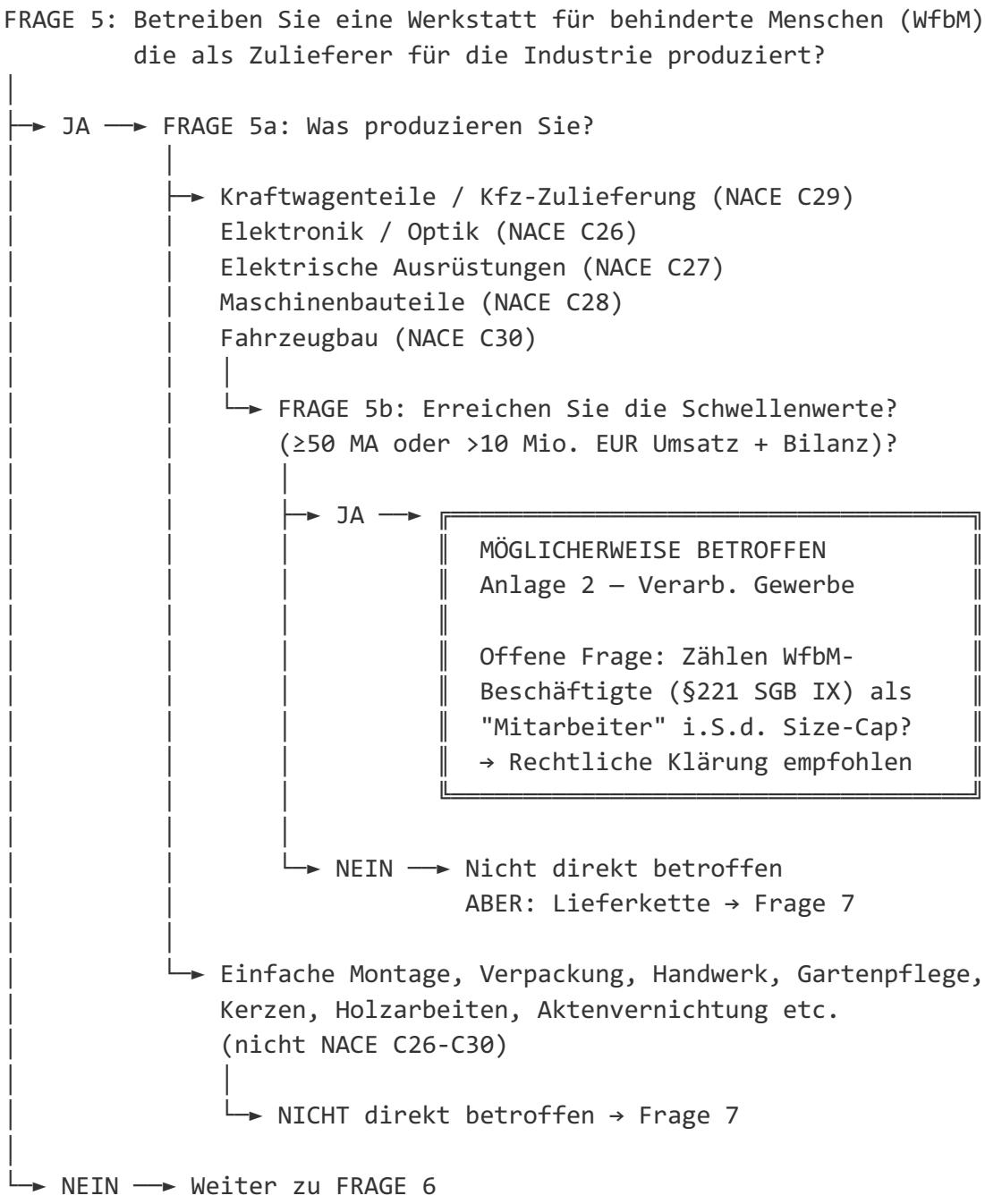
FRAGE 2: Betreiben Sie einen MVZ-Träger oder eine Frühförderstelle?




FRAGE 3: Betreiben Sie eine Pflegeeinrichtung (stationär/ambulant)?
JA → FRAGE 3a: Handelt es sich um LANGZEITPFLEGE?
(Pflegeheim, ambulanter Pflegedienst, betreutes Wohnen,
Hospiz, Tagespflege)
JA →
NICHT BETROFFEN (Langzeitpflege ist
explizit ausgenommen gem. EU-RL 2011/24)
ABER: Lieferkette prüfen → Frage 7
NEIN → Handelt es sich um außerklinische
Intensivpflege oder Kurzzeitpflege
mit medizinischer Behandlung?
JA → Möglicherweise betroffen
(Gesundheitssektor) → Größe prüfen
NEIN → Nicht direkt betroffen → F7
NEIN → Weiter zu FRAGE 4

FRAGE 4: Betreiben Sie einen IT-Dienstleister (z.B. SoCura-Modell)?
D.h. eine ausgegliederte IT-Gesellschaft, die IT-Infrastruktur
für andere Organisationen betreibt, verwaltet oder wartet?




FRAGE 5: Betreiben Sie eine Werkstatt für behinderte Menschen (WfbM), die als Zulieferer für die Industrie produziert?
JA → FRAGE 5a: Was produzieren Sie?
Kraftwagenteile / Kfz-Zulieferung (NACE C29)
Elektronik / Optik (NACE C26)
Elektrische Ausrüstungen (NACE C27)
Maschinenbauteile (NACE C28)
Fahrzeugbau (NACE C30)
FRAGE 5b: Erreichen Sie die Schwellenwerte? (≥50 MA oder >10 Mio. EUR Umsatz + Bilanz)?
JA →
MÖGLICHERWEISE BETROFFEN
Anlage 2 – Verarb. Gewerbe
Offene Frage: Zählen WfbM-Beschäftigte (§221 SGB IX) als "Mitarbeiter" i.S.d. Size-Cap?
→ Rechtliche Klärung empfohlen
NEIN → Nicht direkt betroffen
ABER: Lieferkette → Frage 7
Einfache Montage, Verpackung, Handwerk, Gartenpflege, Kerzen, Holzarbeiten, Aktenvernichtung etc. (nicht NACE C26-C30)
NICHT direkt betroffen → Frage 7
NEIN → Weiter zu FRAGE 6

FRAGE 6: Betreiben Sie eine der folgenden Einrichtungen?

├─► Großküche / Zentralküche / Catering / "Essen auf Rädern"
│   └─► ╔═══╗
│   ║ IN DER REGEL NICHT BETROFFEN   ║
│   ║   ║
│   ║ Großküchen fallen unter NACE 56 (Gastronomie),   ║
│   ║ NICHT unter "industrielle Lebensmittelproduktion". ║
│   ║ NIS-2 Lebensmittelsektor erfasst nur Großhandel   ║
│   ║ und industrielle Produktion/Verarbeitung.   ║
│   ║   ║
│   ║ AUSNAHME: Wenn Sie vorverpackte Lebensmittel für ║
│   ║ den Großhandel/Einzelhandel industriell herstellen ║
│   ║ → dann Einzelfallprüfung erforderlich   ║
│   ╚═══╝
│
├─► Wäscherei / Textilreinigung
│   └─► NICHT BETROFFEN
│   Wäschereien (NACE 96.01) fallen unter keinen NIS-2-Sektor.
│   → Indirekte Betroffenheit über Lieferkette möglich (F7)
│
├─► Recycling-Betrieb / Abfallwirtschaft
│   └─► NUR betroffen, wenn:
│   1. Abfallbewirtschaftung die HAUPTWIRTSCHAFTSTÄTIGKEIT ist
│   2. UND Schwellenwerte erreicht werden (≥50 MA / >10 Mio. EUR)
│   Sozialkaufhäuser: NICHT betroffen (Haupttätigkeit = Einzelhandel)
│
├─► Kita / Jugendhilfe / Beratungsstelle / Sozialstation
│   └─► NICHT BETROFFEN (kein NIS-2-Sektor)
│
└─► Eigene Energieerzeugung (BHKW, PV-Anlage)
    └─► NICHT BETROFFEN (KRITIS-Schwelle: Versorgung von
        500.000 Personen – von Caritas-Trägern nicht erreichbar)

FRAGE 7: INDIREKTE BETROFFENHEIT (Lieferkette)
Haben Sie Geschäftsbeziehungen zu NIS-2-pflichtigen Organisationen?

- Sie beliefern/bedienen ein Caritas-KRANKENHAUS (Wäscherei, Catering, Handwerker, Reinigung etc.)
  - **INDIREKT BETROFFEN**
    Das Krankenhaus MUSS gem. §30 Abs. 2 Nr. 4 BSIG Lieferkettensicherheit gewährleisten und wird IT-Sicherheitsanforderungen vertraglich an Sie weitergeben.
- Ihre WfbM liefert an NIS-2-pflichtige Industrieunternehmen (z.B. Automobilhersteller, Maschinenbauer)
  - INDIREKT BETROFFEN
    Erwartbar: Sicherheitsfragebögen, Audit-Rechte, vertragliche IT-Sicherheitsklauseln
- Sie nutzen die SoCura oder einen anderen NIS-2-pflichtigen IT-Dienstleister
  - INDIREKT BETROFFEN
    Sie müssen die Sicherheitsvorgaben des IT-Dienstleisters einhalten (z.B. MFA, Passwortrichtlinien, Meldepflichten)
- Keine relevanten Geschäftsbeziehungen
  - Aktuell nicht betroffen.
    Empfehlung: IT-Sicherheit trotzdem auf angemessenem Niveau halten (vgl. Ransomware-Angriff Caritas München 2022: 23 Mio. EUR Schaden, 2 Jahre wirtschaftliche Erholung)

4.2 Entscheidungsmatrix (Kurzform)

Frage	Ja	Nein
Krankenhaus / Reha?	→ Größe prüfen → betroffen	weiter
MVZ / Frühförderung?	→ Größe prüfen → betroffen	weiter
Langzeitpflege?	→ **ausgenommen**	weiter
Ausgegliederte IT (MSP)?	→ Größe prüfen → betroffen	weiter
WfbM mit Industrieproduktion (NACE C26-30)?	→ Größe prüfen → evtl. betroffen	weiter
Großküche / Catering?	→ i.d.R. nicht betroffen	weiter
Wäscherei?	→ nicht betroffen	weiter
Recycling (Haupttätigkeit)?	→ Größe prüfen	weiter
Lieferkette zu NIS-2-Pflichtigen?	→ indirekt betroffen	nicht betroffen
Rettungsdienst?	→ Größe prüfen → betroffen	weiter

5. Detailanalyse nach Einrichtungstyp

5.1 Krankenhäuser und Reha-Kliniken und Rettungsdienste

Rechtsgrundlage: Anlage 1 Nr. 4 BSIG — Sektor “Gesundheitswesen”, Einrichtungsart “Erbringer von Gesundheitsdienstleistungen” gem. EU-Richtlinie 2011/24/EU

Betroffenheit: Praktisch alle 244 katholischen Krankenhäuser und 52 Reha-Einrichtungen dürften betroffen sein, da die Schwellenwerte (50 MA oder 10 Mio. EUR) in aller Regel überschritten werden. Auch die Malteser sind direkt betroffen.

KRITIS-Schwelle: Krankenhäuser mit >30.000 vollstationären Fällen/Jahr gelten zusätzlich als **Betreiber kritischer Anlagen** mit verschärften Anforderungen.

5.2 Pflegeeinrichtungen (stationär und ambulant)

Ergebnis: Nicht direkt betroffen.

Die EU-Richtlinie 2011/24/EU (Patientenmobilitätsrichtlinie), auf die der Gesundheitssektor verweist, schließt Langzeitpflege in Erwägungsgrund 14 explizit aus. Das BSI hat dies bestätigt. Ausgenommen sind: - Stationäre Pflegeheime - Ambulante Pflegedienste - Betreutes Wohnen - Tagespflege - Hospizdienste

Grenzfall: Außerklinische Intensivpflege könnte betroffen sein (medizinische Behandlung im Vordergrund).

5.3 IT-Dienstleister (SoCura-Modell)

Rechtsgrundlage: Anlage 1 Nr. 6 BSIG — Sektor “Digitale Infrastruktur”, Einrichtungsart “Managed Service Provider (MSP)”

BSI-Klarstellung: “Tochterunternehmen, in denen der zentrale IT-Betrieb eines Unternehmensverbunds organisiert ist, dürften **in der Regel als MSP** anzusehen sein.”

SoCura konkret: - ~440 Mitarbeitende, Sitz in Köln - Gesellschafter: Malteser Verbund - Seit 2016/2017 aktiv am externen Markt (nicht nur interne IT) - Betreibt IT-Infrastruktur für 85.000+ Mitarbeitende des Malteser-Verbunds + externe Kunden - **Einstufung: Besonders wichtige Einrichtung** (>250 MA in Anlage-1-Sektor)

Weitere potenziell betroffene IT-Dienstleister im Caritas-Umfeld: - Jede ausgegliederte IT-Gesellschaft eines Diözesanverbands oder Krankenhausträgers - Jeder IT-Dienstleister, der aktiv für Dritte am Markt IT-Systeme betreibt/verwaltet - **Nicht betroffen:** Reine IT-Beratung ohne tatsächlichen Zugriff auf Kundensysteme

5.4 Werkstätten für behinderte Menschen (WfbM)

Rechtsgrundlage (potenziell): Anlage 2 Nr. 5 BSIG — Sektor “Verarbeitendes Gewerbe”

Nur betroffen, wenn **beide** Bedingungen erfüllt sind: 1. Die Produktion fällt unter NACE C26–C30 (Elektronik, Elektrik, Maschinenbau, Kfz-Teile, Fahrzeugbau) 2. Die Schwellenwerte werden erreicht (≥50 MA oder >10 Mio. EUR)

Offene Rechtsfrage: Ob WfbM-Beschäftigte im arbeitnehmerähnlichen Rechtsverhältnis (§221 SGB IX) als “Mitarbeiter” im Sinne der EU-KMU-Definition (2003/361/EG) zählen, ist **nicht abschließend geklärt**. Eine rechtliche Klärung wird empfohlen.

Beispiel: Die CBW GmbH (Caritas-Betriebs- und Werkstätten, Raum Aachen) produziert als Zulieferer für die Automobilindustrie. Falls sie Kfz-Teile unter NACE C29 herstellt und die Schwellenwerte erreicht → potenzielle NIS-2-Betroffenheit.

5.5 Großküchen, Catering, "Essen auf Rädern"

Ergebnis: In der Regel nicht betroffen.

Der NIS-2-Lebensmittelsektor (Anlage 2 Nr. 4) erfasst nur **Großhandel** und **industrielle Produktion/Verarbeitung**. Großküchen fallen unter **NACE 56 (Gastronomie)**, nicht unter NACE 10 (Herstellung von Nahrungsmitteln). Das BSI bestätigt: "Hotel-Restaurants, Restaurants und Gastronomiebetriebe zählen in der Regel nicht als wichtige Einrichtungen."

Ausnahme: Wenn eine Caritas-Küche industriell vorverpackte Lebensmittel für den Großhandel/Einzelhandel produziert (z.B. Tiefkühlkost-Linie) → Einzelfallprüfung.

5.6 Wäschereien

Ergebnis: Nicht betroffen.

Wäschereien (NACE 96.01) fallen unter **keinen** der 18 NIS-2-Sektoren. Lediglich über den Lieferketteneffekt können Anforderungen entstehen, wenn NIS-2-pflichtige Krankenhäuser beliefert werden.

5.7 Abfallwirtschaft / Recycling

Rechtsgrundlage: Anlage 2 Nr. 2 BSIG — Sektor "Abfallbewirtschaftung"

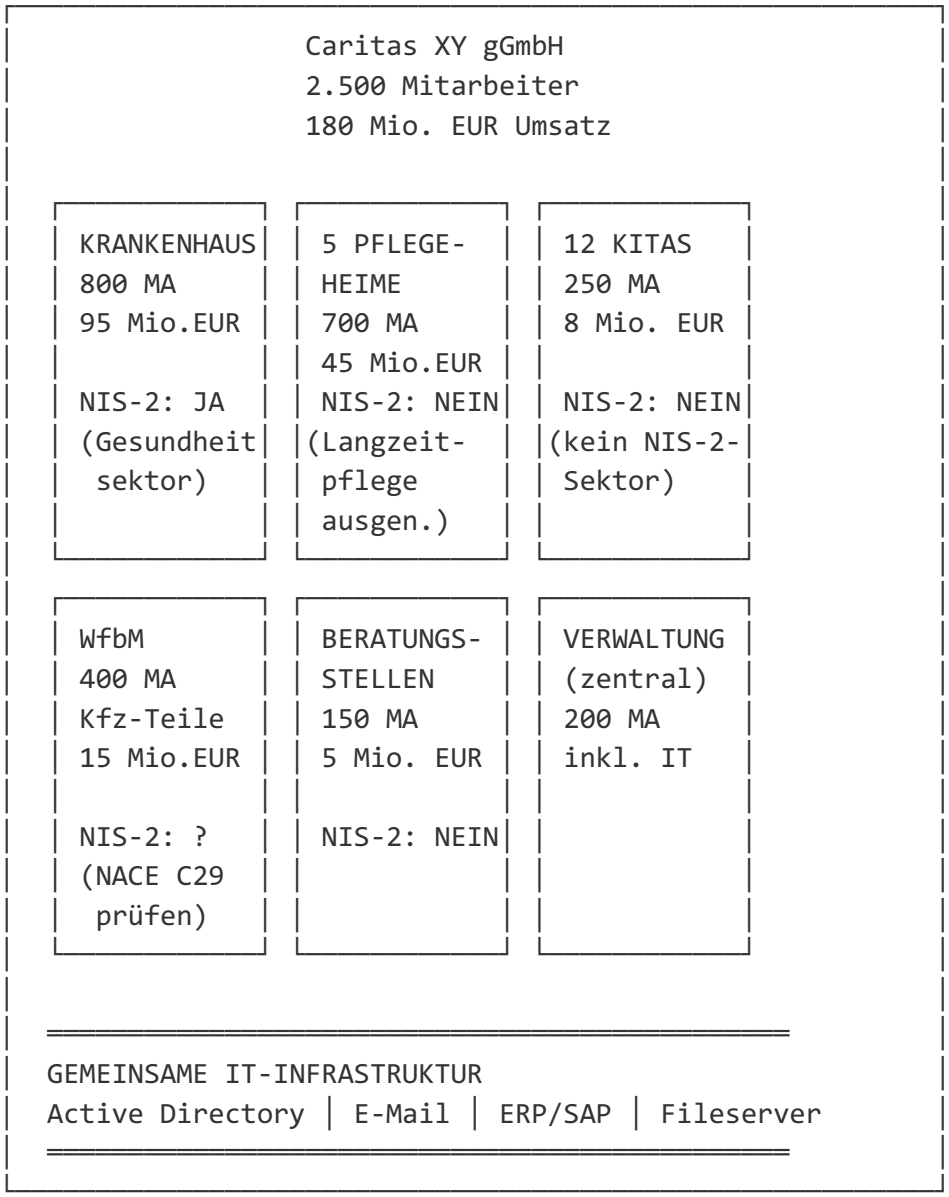
Nur betroffen, wenn Abfallbewirtschaftung die **Hauptwirtschaftstätigkeit** ist UND Schwellenwerte erreicht werden. Sozialkaufhäuser (Einzelhandel als Haupttätigkeit) sind **nicht** betroffen.

6. Komplexträger: Die zentrale Herausforderung

6.1 Was ist ein Komplexträger?

In der Caritas-Landschaft ist der **Komplexträger** der Regelfall, nicht die Ausnahme. Ein Komplexträger vereint unter **einer einzigen Rechtsform** (z.B. einer gGmbH) mehrere Geschäftsbereiche:

Typischer Caritas-Komplexträger (eine gGmbH):



Das Problem: Das Krankenhaus löst die NIS-2-Betroffenheit aus — aber was passiert mit den Pflegeheimen, Kitas und der Werkstatt, die alle Teil derselben juristischen Person sind?

6.2 Die Kernregel: NIS-2 erfasst die gesamte Rechtseinheit

NIS-2 verfolgt einen "entity-based approach" — der Bezugspunkt ist die **juristische Person** (Legaleinheit), nicht die einzelne Einrichtung oder Betriebsstätte.

> §28 BSIG spricht von: *"juristischen Personen, die anderen natürlichen oder juristischen Personen entgeltlich Waren oder Dienstleistungen anbieten und einer in den Anlagen 1 und 2 des BSIG aufgeführten Einrichtungsart zuzuordnen sind"*

Das bedeutet konkret:

```
┌──────────────────────────────────────────────────────┐
│  KONSEQUENZ FÜR KOMPLEXTRÄGER                        │
│                                                      │
│  Wenn die Caritas XY gGmbH wegen des Krankenhauses   │
│  unter NIS-2 fällt, dann:                            │
│                                                      │
│  ► Die gesamte gGmbH ist "NIS-2-Einrichtung"         │
│  ► Die Registrierung beim BSI erfolgt für die gGmbH  │
│  ► Die Geschäftsleitung der gGmbH haftet persönlich  │
│  ► Alle Pflichten (§30, §32, §38 BSIG) gelten        │
│    für die gesamte juristische Person                │
│                                                      │
│  Es gibt KEINE "Teilbereichsregistrierung"           │
│  nur für das Krankenhaus!                            │
└──────────────────────────────────────────────────────┘
```

Quelle: OpenKRITIS — Geltungsbereich bei NIS2-Einrichtungen

6.3 Schwellenwertberechnung: Die gesamte gGmbH zählt

Die Schwellenwerte (50/250 MA, 10/50 Mio. EUR) werden für die **gesamte Rechtseinheit** berechnet — nicht nur für den Krankenhausbereich. Das BSI bestätigt in den FAQ:

> *"Bezieht sich die Anzahl der Beschäftigten sowie die Höhe des Umsatzvolumens auf einen einzelnen (Filial-) Betrieb oder unter Umständen auf das gesamte Unternehmen?"* — **Antwort: Auf das gesamte Unternehmen.**

Praktische Auswirkung:

Szenario	Nur Krankenhaus	Gesamte gGmbH	Einstufung
Mitarbeiter	80	2.500	**Besonders wichtig** (statt nur "wichtig")
Umsatz	25 Mio. EUR	180 Mio. EUR	**Besonders wichtig**

Das Krankenhaus allein hätte vielleicht nur 80 MA und wäre "wichtige Einrichtung". Durch die Gesamtbetrachtung der gGmbH (2.500 MA) wird der Komplexträger zur **"besonders wichtigen Einrichtung"** — mit strengerer Aufsicht und höheren Bußgeldern (bis 10 Mio. EUR statt 7 Mio. EUR).

6.4 Scope der Pflichten: Wie weit reicht NIS-2 innerhalb des Komplexträgers?

Dies ist die **praktisch wichtigste und zugleich am wenigsten geklärte Frage**.

Was der Gesetzestext sagt

§30 Abs. 1 BSIG verpflichtet zu Maßnahmen für: > *"informationstechnische Systeme, Komponenten und Prozesse, die sie **für die Erbringung ihrer Dienste** nutzen"*

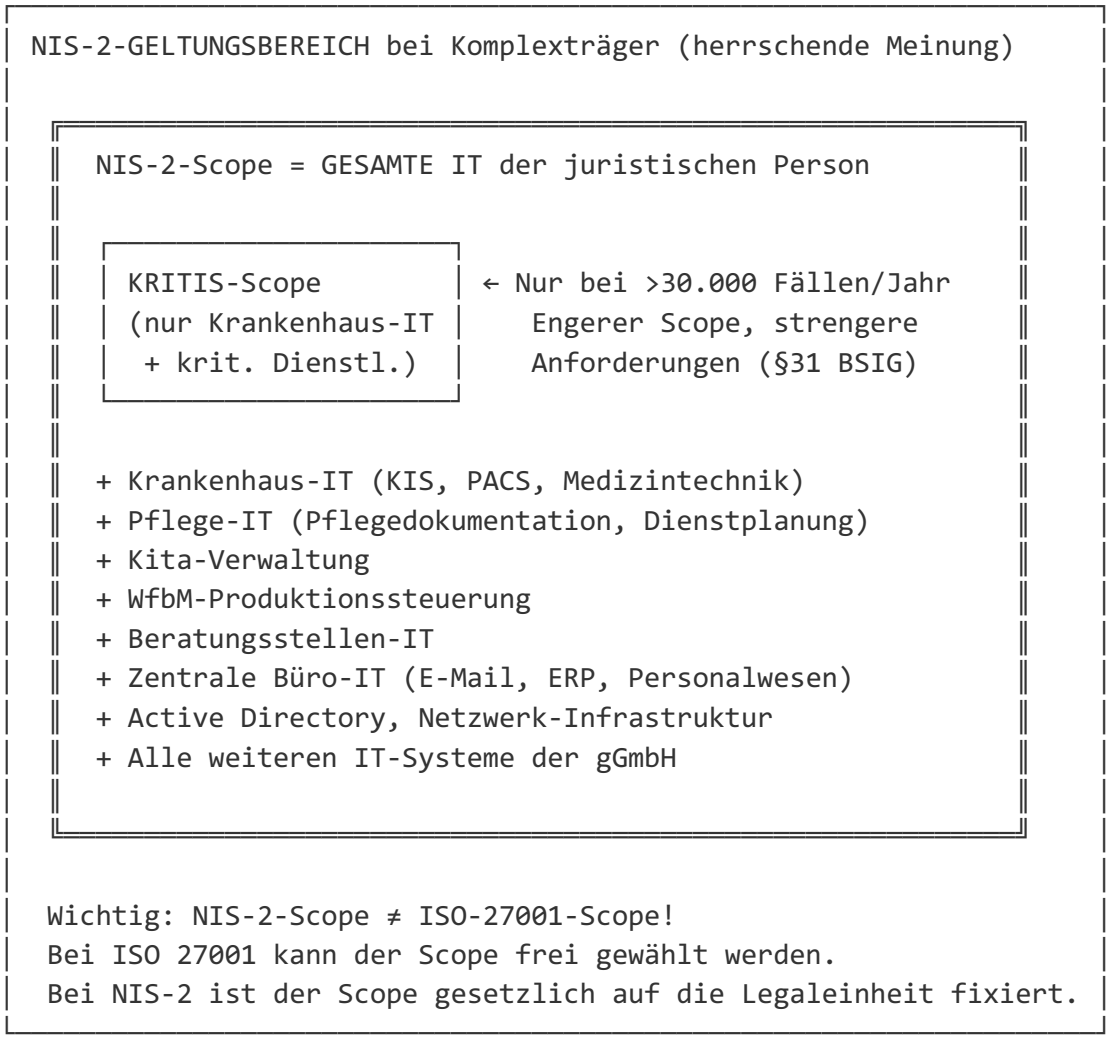
Was "Dienste" bedeutet (weite Auslegung — herrschende Meinung)

Der Gesetzgeber und das BSI interpretieren "Dienste" **sehr weit**. OpenKRITIS stellt klar:

> *"Mit den Diensten meint der Gesetzgeber sämtliche Aktivitäten der Einrichtung, für die IT-Systeme eingesetzt werden, dies beinhaltet beispielsweise auch **Büro-IT** oder andere IT-Systeme, die durch die Einrichtung betrieben werden."*

Und explizit: > *"…sollen alle IT-Systeme einer Einrichtung einer Regulierung unterliegen"*

Konsequenz: Der Scope umfasst ALLE IT-Systeme der gGmbH



Unterschied zu KRITIS: Unter dem alten KRITIS-Regime galt ein **anlagenbezogener** Ansatz — nur die IT für die kritische Dienstleistung musste geschützt werden. NIS-2 hat diesen Ansatz durch den **einrichtungsbezogenen** Ansatz ersetzt. Der KRITIS-Scope (§31 BSIG) existiert als **engere Teilmenge** innerhalb des weiteren NIS-2-Scopes weiter.

Hinweis: Die Darstellung hier ist die vorherrschende, aber nicht unumstrittene Meinung. Es gibt auch juristische Stimmen (z.B. Noerr, CMS), die argumentieren, dass der Scope durch §30 Abs. 1 BSIG ("Systeme,

die sie für die Erbringung ihrer Dienste nutzen") begrenzbar sein könnte. Die Darstellung hier ist also die dominante **Rechtsauffassung**, keine gesetzliche Gewissheit.

6.5 Das Verhältnismäßigkeitsprinzip: Differenzierung ja, Ausschluss nein

§30 Abs. 1 BSIG fordert **"verhältnismäßige"** Maßnahmen. Das Verhältnismäßigkeitsprinzip ist allerdings **keine Scope-Begrenzung**, sondern ein **Maßstab für die Intensität** der Maßnahmen.

```
Verhältnismäßigkeit = Risikodifferenzierte Maßnahmenintensität
═══════════════════════════════════════════════════════════════

  Krankenhaus-IT          ████████████████████████ Höchste Intensität
  (KIS, Medizintechnik)   Grund: Direkte Patientengefährdung

  Zentrale IT             ████████████████████████  Sehr hohe Intensität
  (AD, E-Mail, ERP)       Grund: Kompromittierung betrifft alles

  Pflege-IT               ████████████████          Hohe Intensität
  (Dokumentation)         Grund: Sensible Gesundheitsdaten

  WfbM-Produktions-IT     ████████████              Mittlere Intensität
  (Maschinensteuerung)    Grund: Keine direkte Patientengefährdung

  Kita-Verwaltung         ██████████                Moderate Intensität
  (Anmeldungen, Planung)  Grund: Personenbezogene Daten, aber
                                 kein "zwingender betrieblicher
                                 Zusammenhang" mit Gesundheitsdienst

  Beratungsstellen-IT     ████████                  Basis-Intensität
  (Terminplanung)         Grund: Geringste Verknüpfung mit
                                 reguliertem Dienst
```

Entscheidend: Auch die Kita-IT muss in die **Risikoanalyse** einbezogen werden. Sie muss nicht das gleiche Sicherheitsniveau wie das KIS erreichen, darf aber **nicht vollständig ignoriert** werden.

Das BSI nennt als Kriterium: > *"ob die Maßnahme(n) Dienste schützt, die in einem zwingenden betrieblichen Zusammenhang zu den Waren und Dienstleistungen stehen (welche die NIS-2 Betroffenheit bedingen)"*

6.6 Das Problem der gemeinsamen IT-Infrastruktur

In der Praxis ist gemeinsame IT bei Komplexträgern der **Normalfall**, nicht die Ausnahme. Das verschärft die Lage erheblich:

```
PROBLEM: Geteilte IT = Unteilbarer Scope
═══════════════════════════════════════

  Krankenhaus  ─┐
  Pflegeheime  ─┤
  Kitas        ─┼──► Gemeinsames Active Directory
  WfbM         ─┤    Gemeinsames E-Mail-System
  Beratung     ─┤    Gemeinsames ERP (SAP)
```

```
Verwaltung   ─┘     Gemeinsames Netzwerk
                    Gemeinsames Rechenzentrum

→ Kompromittierung des AD = Kompromittierung ALLER Bereiche
→ Ransomware in der Kita-IT → Lateral Movement → KIS betroffen
→ Scope-Begrenzung technisch UNMÖGLICH
```

Konsequenz: Bei gemeinsamer IT-Infrastruktur erstreckt sich der NIS-2-Scope **zwingend** auf alle verbundenen Systeme. Ein Sicherheitsvorfall in der Kita-IT, der über das gemeinsame AD das Krankenhaus erreicht, ist **meldepflichtig** (24h-Frühwarnung an BSI).

Praxisbeispiel Caritas München 2022: Der Ransomware-Angriff (BlackCat/ALPHV) auf den Caritasverband München und Oberbayern traf über die gemeinsame IT-Infrastruktur alle 350+ Einrichtungen gleichzeitig — 23 Mio. EUR Schaden, 2 Jahre Erholung.

6.7 Die "Vernachlässigbarkeitsregel" (§28 Abs. 3 BSIG) — hilft sie Komplexträgern?

§28 Abs. 3 BSIG enthält eine Regel, die auf den ersten Blick wie ein Ausweg wirkt:

> *"Bei der Zuordnung zu einer der Einrichtungsarten nach den Anlagen 1 und 2 können solche Geschäftstätigkeiten unberücksichtigt bleiben, die im Hinblick auf die gesamte Geschäftstätigkeit der Einrichtung **vernachlässigbar** sind."*

Aber Achtung — die Regel wirkt UMGEKEHRT als erhofft:

```
Was die Vernachlässigbarkeitsregel NICHT kann:
═══════════════════════════════════════════════

  ✗ "Unser Krankenhaus ist nur 30% unserer gGmbH,
     also können wir es als 'vernachlässigbar' ignorieren
     und die gGmbH fällt nicht unter NIS-2."

  → FALSCH! Die Regel erlaubt nur, eine WINZIGE regulierte
    Tätigkeit zu ignorieren – nicht eine substanzielle.

  → Bei 30% Umsatzanteil und expliziter Nennung in der
    Satzung ist das Krankenhaus NICHT vernachlässigbar.

Was die Vernachlässigbarkeitsregel KANN:
═══════════════════════════════════════════

  ✓ "Unsere gGmbH betreibt primär 20 Pflegeheime (95% des
     Umsatzes) und hat ein winziges Labor (5%), das technisch
     als Gesundheitsdienstleister zählen könnte."

  → MÖGLICHERWEISE: Wenn das Labor einen vernachlässigbaren
    Anteil hat und NICHT in der Satzung steht, könnte die
    Gesamteinrichtung von NIS-2 ausgenommen sein.
```

Bewertungskriterien (laut Gesetzesbegründung): - Anteil der Mitarbeiter im regulierten Bereich - Umsatzanteil des regulierten Bereichs - Bilanzsummenanteil - **Gegenindiz:** Nennung in Gesellschaftervertrag, Satzung oder Gründungsdokument

EU-Rechtsrisiko: Mehrere Kanzleien (u.a. Heuking, GvW) weisen darauf hin, dass §28 Abs. 3 BSIG **keine Grundlage in der NIS-2-Richtlinie** hat und möglicherweise **europarechtswidrig** ist.

Quellen: - GvW — NIS-2 und die Vernachlässigbarkeit - Heuking — Scope for Corporate Groups

6.8 Strategien zur Scope-Begrenzung

Strategie A: Gesellschaftsrechtliche Ausgliederung (wirksamste Option)

```
VORHER: Ein Rechtsträger für alles
═══════════════════════════════════

  Caritas XY gGmbH
  ├── Krankenhaus (NIS-2: JA)
  ├── Pflegeheime (NIS-2: NEIN)
  ├── Kitas (NIS-2: NEIN)
  └── Alles teilt sich IT

  → Gesamte gGmbH = NIS-2-Einrichtung
  → 2.500 MA → "Besonders wichtige Einrichtung"
  → Scope: ALLE IT-Systeme

NACHHER: Getrennte Rechtsträger
═══════════════════════════════

  Caritas XY Holding gGmbH (kein NIS-2-Sektor)
  ├── Caritas Krankenhaus gGmbH (NIS-2: JA)
  │    └── 800 MA → "Besonders wichtig" (Anlage 1)
  │    └── EIGENE IT-Infrastruktur
  │    └── Scope: Nur Krankenhaus-IT
  │
  ├── Caritas Pflege & Soziales gGmbH (NIS-2: NEIN)
  │    └── 1.200 MA, aber kein NIS-2-Sektor
  │    └── EIGENE IT-Infrastruktur
  │
  └── Caritas Kinder & Familie gGmbH (NIS-2: NEIN)
       └── 500 MA, aber kein NIS-2-Sektor
       └── EIGENE IT-Infrastruktur
```

Voraussetzungen für die Wirksamkeit: 1. **Echte rechtliche Trennung** — eigene gGmbHs, nicht nur Betriebsstätten 2. **IT-Unabhängigkeit** — getrennte IT-Infrastruktur (eigenes AD, eigene Server, eigene E-Mail). **Ohne IT-Trennung ist die Ausgliederung wirkungslos!** 3. **Unabhängigkeitsklausel (§28 Abs. 4 BSIG)** muss greifen — sonst werden die Schwellenwerte trotzdem zusammengerechnet

Keine "Infektionswirkung": Die NIS-2-Betroffenheit der Krankenhaus-gGmbH führt **nicht** automatisch dazu, dass die Pflege-gGmbH ebenfalls unter NIS-2 fällt.

Aber Vorsicht: - Hoher organisatorischer und finanzieller Aufwand - Doppelte IT-Infrastrukturen = deutlich höhere IT-Kosten - Neue Lieferketten-Fragen: Wenn die Pflege-gGmbH Dienstleistungen für die Krankenhaus-

gGmbH erbringt, muss das Krankenhaus gem. §30 Abs. 2 Nr. 4 BSIG Lieferkettensicherheit gewährleisten → indirekte Anforderungen an die Pflege-gGmbH - EU-Rechtsunsicherheit bei der Unabhängigkeitsklausel

Strategie B: IT-Segmentierung (pragmatischer Mittelweg)

Ohne gesellschaftsrechtliche Umstrukturierung, aber mit Netztrennung:

```
Caritas XY gGmbH (eine juristische Person)
│
├── Segment "Krankenhaus"  ── Eigenes VLAN / Eigenes AD
│   → NIS-2-Maßnahmen: VOLLE Intensität
│
├── Segment "Pflege"       ── Eigenes VLAN / Trust-Beziehung
│   → NIS-2-Maßnahmen: Hohe Intensität
│
├── Segment "Kita/Soziales" ── Eigenes VLAN
│   → NIS-2-Maßnahmen: Moderate Intensität
│
└── Segment "Verwaltung"   ── Eigenes VLAN
    → NIS-2-Maßnahmen: Hohe Intensität (ERP, Personal)
```

Was Segmentierung bewirkt: - **Rechtlich:** Ändert den Scope NICHT — die gGmbH bleibt als Ganzes NIS-2-pflichtig - **Praktisch:** Ermöglicht risikodifferenzierte Maßnahmenintensität - **Bei Vorfällen:** Ein isolierter Vorfall im Kita-Segment, der das Krankenhaus NICHT betrifft, ist möglicherweise nicht meldepflichtig - **Kostenvorteil:** Günstiger als vollständige Ausgliederung mit doppelter IT

Was NIS-2 selbst fordert: Netzsegmentierung ist eine in §30 BSIG und der geplanten NIS2UmsVO vorgesehene Maßnahme — der Gesetzgeber erwartet sie also ohnehin.

Strategie C: Status quo beibehalten — gesamte IT auf NIS-2-Niveau heben

```
Caritas XY gGmbH
└── ALLE IT-Systeme → NIS-2-Compliance
    → Vorteil: Kein Umbau nötig, einheitliches Sicherheitsniveau
    → Nachteil: Höchster Aufwand, da ALLE Bereiche betroffen
    → Vorteil: Stärkstes Sicherheitsniveau insgesamt
```

Wann sinnvoll: Wenn der Komplexträger ohnehin ein hohes IT-Sicherheitsniveau anstrebt und die Kosten tragbar sind.

6.9 Die Unabhängigkeitsklausel (§28 Abs. 4 BSIG) bei Konzernstrukturen

Für Caritas-Träger, die als **Holding mit Tochtergesellschaften** organisiert sind:

```
UNABHÄNGIGKEITSKLAUSEL – Drei-Stufen-Prüfung
═══════════════════════════════════════════

§28 Abs. 4 Satz 2 BSIG: Verbundene Unternehmen werden
NICHT zusammengerechnet, wenn Unabhängigkeit besteht in:

  1. RECHTLICHE Unabhängigkeit
     ├── Eigene juristische Person?                    [✓/✗]
     ├── Keine wesentlichen Weisungsrechte in IT?      [✓/✗]
     └── Eigene Entscheidungshoheit über IT-Strategie? [✓/✗]

  2. WIRTSCHAFTLICHE Unabhängigkeit
     ├── Eigenes IT-Budget?                            [✓/✗]
     ├── Eigene IT-Beschaffung?                        [✓/✗]
     └── Kein wirtschaftlicher Zwang zur Konzern-IT?   [✓/✗]

  3. TATSÄCHLICHE Unabhängigkeit (IT-Betrieb)
     ├── Eigenes Active Directory?                     [✓/✗]
     ├── Eigene Server / eigenes Rechenzentrum?        [✓/✗]
     ├── Eigenes IT-Personal?                          [✓/✗]
     ├── Eigene E-Mail-Infrastruktur?                  [✓/✗]
     └── Keine gemeinsame Netzwerk-Infrastruktur?      [✓/✗]

  → Alle drei Ebenen müssen erfüllt sein!
  → Gemeinsame IT ist der häufigste Grund für SCHEITERN
```

Wichtige Einschränkung: Die Unabhängigkeitsklausel gilt nur für das Verhältnis zwischen **verschiedenen juristischen Personen**. Innerhalb einer einzigen gGmbH gibt es **keine Unabhängigkeit** zwischen Geschäftsbereichen.

EU-Rechtsrisiko: Die Kanzlei Heuking warnt, dass die deutsche Unabhängigkeitsklausel in der NIS-2-Richtlinie nicht vorgesehen ist und deren EU-Rechtskonformität “highly doubtful” ist.

6.10 Entscheidungsbaum für Komplexträger

```
START: Komplexträger-Analyse
═══════════════════════════

SCHRITT 1: Sektorzuordnung
   Betreiben Sie innerhalb Ihrer Rechtseinheit mindestens
   eine Tätigkeit in einem NIS-2-Sektor?
   (Krankenhaus, MVZ, Reha, IT-Dienstleistung, WfbM mit
    NACE C26-C30, Abfallwirtschaft als Haupttätigkeit)
   │
   ├─► NEIN → Nicht direkt betroffen (nur Lieferkette prüfen)
   │
   └─► JA → Weiter zu Schritt 2

SCHRITT 2: Vernachlässigbarkeit prüfen (§28 Abs. 3 BSIG)
   Ist die regulierte Tätigkeit "vernachlässigbar" gemessen
   an der Gesamttätigkeit der Rechtseinheit?
   │
   ├─► Umsatzanteil < 5% UND
   │   Mitarbeiteranteil < 5% UND
   │   Nicht in Satzung/Gesellschaftervertrag genannt
   │   → Möglicherweise vernachlässigbar → juristische Prüfung
   │     (ACHTUNG: EU-Rechtskonformität umstritten!)
   │
   └─► Umsatzanteil ≥ 5% ODER
       In Satzung genannt
       → NICHT vernachlässigbar → Weiter zu Schritt 3

SCHRITT 3: Schwellenwerte der GESAMTEN Rechtseinheit
   (Alle MA + Umsätze der gesamten gGmbH!)
   │
   ├─► ≥250 MA ODER (>50 Mio. EUR Umsatz UND >43 Mio. EUR Bilanz)
   │   UND Tätigkeit in Anlage-1-Sektor
   │   → BESONDERS WICHTIGE EINRICHTUNG
   │     Bußgeld bis 10 Mio. EUR / 2% Umsatz
   │     BSI-Aufsicht: aktive Kontrolle
   │
   ├─► ≥50 MA ODER (>10 Mio. EUR Umsatz UND >10 Mio. EUR Bilanz)
   │   → WICHTIGE EINRICHTUNG
   │     Bußgeld bis 7 Mio. EUR / 1,4% Umsatz
   │     BSI-Aufsicht: anlassbezogen
   │
   └─► Unter den Schwellenwerten
       → Grundsätzlich nicht betroffen
         (Ausnahme: KRITIS-Betreiber, TK-Anbieter)

SCHRITT 4: Scope bestimmen
```

```
    │
    ├─► Gemeinsame IT für alle Bereiche?
    │   → Scope = GESAMTE IT der Rechtseinheit
    │   → Handlungsoptionen:
    │     a) Alles auf NIS-2-Niveau heben
    │     b) Netzwerksegmentierung einführen
    │     c) Gesellschaftsrechtliche Ausgliederung prüfen
    │
    └─► Getrennte IT pro Geschäftsbereich?
        → Scope = Formal die gesamte Rechtseinheit,
          aber Verhältnismäßigkeit ermöglicht
          risikodifferenzierte Maßnahmenintensität

SCHRITT 5: Strategie wählen
    │
    ├─► OPTION A: Ausgliederung des Krankenhauses
    │   in eigene gGmbH MIT eigener IT
    │   → Engster Scope, höchster Umstellungsaufwand
    │   → Neue Lieferketten-Themen
    │
    ├─► OPTION B: IT-Segmentierung OHNE Ausgliederung
    │   → Scope bleibt die gGmbH, aber differenzierte Maßnahmen
    │   → Pragmatischer Mittelweg
    │
    └─► OPTION C: Gesamte IT auf NIS-2-Niveau
        → Kein Umbau, einheitliches Sicherheitsniveau
        → Höchste Kosten, aber stärkstes Sicherheitsniveau
```

6.11 Typische Komplexträger-Konstellationen und ihre Bewertung

Konstellation	Einstufung	Scope	Empfehlung
Eine gGmbH: Krankenhaus + 5 Pflegeheime + 10 Kitas	Besonders wichtig (Anlage 1, >250 MA gesamt)	Gesamte IT der gGmbH	Segmentierung oder Ausgliederung KH
Holding + Krankenhaus-gGmbH + Pflege-gGmbH (gemeinsame IT)	KH-gGmbH betroffen; Pflege-gGmbH: Schwellenwerte werden zusammengerechnet (gemeinsame IT = keine Unabhängigkeit)	Faktisch die gesamte IT	IT trennen oder gemeinsam auf NIS-2-Niveau
Holding + Krankenhaus-gGmbH (eigene IT) + Pflege-gGmbH (eigene IT)	Nur KH-gGmbH betroffen; Pflege-gGmbH kann Unabhängigkeit geltend machen	Nur IT der KH-gGmbH	Idealszenario, aber teuer
Eine gGmbH: Nur Pflegeheime + Kitas	Nicht betroffen (Langzeitpflege ausgenommen, Kitas kein Sektor)	—	Lieferkette prüfen
Eine gGmbH: Krankenhaus + WfbM (Kfz-Zulieferung)	Besonders wichtig (Gesundheit Anlage 1); WfbM möglicherweise zusätzlich über Anlage 2	Gesamte IT	Doppelte Sektorzuordnung prüfen
Eine gGmbH: 20 Pflegeheime + 1 kleines Labor	Vernachlässigbarkeit prüfen: Wenn Labor <5% Umsatz und nicht in Satzung → möglicherweise nicht betroffen	—	Juristische Einzelfallprüfung

6.12 Offene Rechtsfragen und regulatorische Lücken

Das Komplexträger-Thema ist ein **blinder Fleck** der NIS-2-Regulierung:

1. **Keine BSI-Guidance** speziell für Komplexträger
2. **Keine Rechtsprechung** zur Vernachlässigbarkeit (der Begriff ist nicht definiert)
3. **Keine Branchenstandards (B3S)** für die Sozialwirtschaft
4. **EU-Rechtsrisiko** bei der Vernachlässigbarkeitsregel und der Unabhängigkeitsklausel
5. **Unklar:** Zählen WfbM-Beschäftigte (§221 SGB IX) als “Mitarbeiter” für die Schwellenwerte?
6. **Unklar:** Refinanzierung der NIS-2-Compliance-Kosten in der Sozialwirtschaft

Die **FINSOZ** erkennt das Problem explizit an: > *“Eine pauschale Antwort ist insbesondere bei Trägern und Einrichtungen nicht möglich, die als Komplexträger mit unterschiedlichen Leistungsangeboten in Pflege, Betreuung, Eingliederungshilfe, medizinischer Versorgung und weiteren Tätigkeitsfeldern tätig sind.”*

6.13 Handlungsempfehlungen für Komplexträger — Sofortmaßnahmen

SOFORT (bis 06.03.2026):
═══════════════════════

□ 1. Betroffenheitsprüfung durchführen
→ BSI-Tool: betroffenheitspruefung-nis-2.bsi.de
→ Pro juristischer Person, nicht pro Einrichtung
→ Alle MA und Umsätze der gesamten Rechtseinheit zählen!

□ 2. Registrierung beim BSI
→ Frist: 06.03.2026 (in wenigen Wochen!)
→ Die gesamte gGmbH registriert sich, nicht nur das KH
→ Portal: mein-unternehmenskonto.de (ELSTER-Zertifikat)

□ 3. Geschäftsleitung informieren
→ Persönliche Haftung ab sofort!
→ Schulungspflicht nach §38 BSIG
→ Cybersicherheit = Chefsache

KURZFRISTIG (Q1-Q2 2026):
═══════════════════════

□ 4. IT-Asset-Inventar erstellen
→ Alle IT-Systeme der gesamten Rechtseinheit erfassen
→ Abhängigkeiten zwischen Bereichen dokumentieren

□ 5. Risikoanalyse durchführen
→ Risikodifferenziert nach Geschäftsbereichen
→ Krankenhaus-IT: höchste Priorität
→ Gemeinsame Infrastruktur: kritisch

□ 6. Meldeprozess etablieren
→ 24h-Frühwarnung bei erheblichen Vorfällen
→ Zuständigkeiten klären: Wer meldet an BSI?

MITTELFRISTIG (2026):
═══════════════════

□ 7. Strategische Entscheidung: Scope-Begrenzung?
→ Juristische Prüfung: Ausgliederung sinnvoll?
→ IT-Architektur: Segmentierung möglich?
→ Kosten-Nutzen-Analyse

□ 8. Maßnahmenumsetzung nach §30 BSIG
→ 10 Mindestmaßnahmen implementieren
→ Verhältnismäßig = risikodifferenziert
→ Dokumentation der Entscheidungsgrundlagen

Quellen für dieses Kapitel: - OpenKRITIS — Geltungsbereich bei NIS2-Einrichtungen und KRITIS-Betreibern - BSI — Allgemeine FAQ zu NIS-2 - BSI — Risikomanagementmaßnahmen - GvW — NIS-2 und die

Vernachlässigbarkeit - Heuking — Scope for Corporate Groups - Freshfields — Germany implements NIS2 - FINSOZ — Orientierungshilfe NIS-2 für Sozialwirtschaft - §28 BSIG — Gesetzestext - §30 BSIG — Gesetzestext

7. Indirekte Betroffenheit: Der Lieferketteneffekt

7.1 Gesetzliche Grundlage

§30 Abs. 2 Nr. 4 BSIG verpflichtet NIS-2-regulierte Einrichtungen zur **“Sicherheit der Lieferkette”**, einschließlich sicherheitsbezogener Aspekte der Beziehungen zu unmittelbaren Anbietern und Diensteanbietern.

7.2 Was bedeutet das für Caritas-Träger?

Auch Träger, die **selbst nicht** unter NIS-2 fallen, werden betroffen, wenn sie Geschäftsbeziehungen zu NIS-2-pflichtigen Organisationen unterhalten:

Ihr Caritas-Betrieb	Ihr NIS-2-pflichtiger Partner	Was auf Sie zukommt
Ambulanter Pflegedienst	Krankenhaus	IT-Sicherheitsnachweise bei digitalen Schnittstellen
Wäscherei	Krankenhaus	Vertragliche IT-Sicherheitsklauseln
WfbM (Zulieferer)	Automobilhersteller	Sicherheitsfragebögen, Audit-Rechte
Catering	Krankenhaus	IT-Sicherheitsanforderungen im Vertrag
Jeder Caritas-Träger	SoCura (als MSP)	Einhaltung von SoCura-Sicherheitsvorgaben

7.3 Typische Anforderungen an Zulieferer

NIS-2-pflichtige Kunden werden zunehmend verlangen: - **Sicherheitsfragebögen** mit Nachweispflicht - **Dokumentierte IT-Sicherheitsprozesse** und -kontrollen - **ISO 27001** oder vergleichbare Zertifizierungen - **Meldepflichten** bei Sicherheitsvorfällen (oft 24h) - **Audit- und Kontrollrechte** des Kunden - **MFA**, Verschlüsselung, Patch-Management

7.4 Praxisempfehlung

Auch ohne direkte NIS-2-Betroffenheit sollte jeder Caritas-Träger: 1. Eine **Bestandsaufnahme** der eigenen IT-Sicherheit durchführen 2. Prüfen, welche Geschäftspartner NIS-2-pflichtig sind 3. Sich auf **vertragliche Anforderungen** vorbereiten 4. Das **IT-Sicherheitsniveau** proaktiv anheben

8. Was NIS-2 konkret bedeutet: Alle Pflichten im Detail

8.1 Übersicht der Pflichtenbereiche

Wenn ein Caritas-Träger unter NIS-2 fällt, treffen ihn **vier Pflichtenbereiche** gleichzeitig — alle seit dem 06.12.2025 **ohne Übergangsfrist** in Kraft:

8.2 Registrierung beim BSI (§§33-34 BSIG)

Frist: 6. März 2026 — in wenigen Tagen!

Was	Detail
Portal	BSI-Registrierungsportal (über MUK = Mein Unternehmenskonto)
Authentifizierung	ELSTER-Organisationszertifikat erforderlich
Angaben	Name, Rechtsform, Handelsregisternummer, Anschrift, Kontaktdaten, öffentliche IP-Adressbereiche, relevanter Sektor
Wer registriert	Die gesamte juristische Person (bei Komplexträgern: die gGmbH, nicht nur das Krankenhaus)
Aktualisierung	Bei Änderungen unverzüglich, mindestens jährliche Bestätigung

Was	Detail
Bei Nicht-Registrierung	Bußgeld bis 500.000 EUR (KRITIS ggf. höher)

Praxishinweis: Viele Caritas-Träger haben noch kein ELSTER-Organisationszertifikat. Die Beantragung dauert mindestens einige Tage — **sofort beantragen!**

In der Praxis wird das BSI zunächst den Registrierungsprozess priorisieren und bei der Durchsetzung der Risikomanagement-Pflichten eine gewisse Anlaufzeit de facto gewähren — auch wenn es dafür keine gesetzliche Grundlage gibt.

8.3 Risikomanagement — Die 10 Mindestmaßnahmen (§30 BSIG) im Detail

§30 BSIG verlangt **"verhältnismäßige technische, operative und organisatorische Maßnahmen"** nach dem **Stand der Technik**. Der Gesetzgeber hat 10 Mindestmaßnahmen definiert. Für jede Maßnahme folgt: Was ist gefordert? Was bedeutet das praktisch für einen Caritas-Träger? Und was kostet es?

Maßnahme 1: Risikoanalyse und Sicherheitskonzepte

Was ist gefordert: Systematische Identifikation, Analyse und Bewertung von Risiken für die Netz- und Informationssicherheit. Erstellung eines Konzepts für Informationssicherheit.

Was das praktisch bedeutet: - **ISMS aufbauen** (Information Security Management System) — entweder nach ISO 27001, BSI IT-Grundschutz oder dem branchenspezifischen Sicherheitsstandard (B3S) für die medizinische Versorgung - **Asset-Inventar** erstellen: Alle IT-Systeme, Anwendungen, Netzwerke, Datenflüsse erfassen - **Risikoregister** führen: Für jedes Asset Bedrohungen, Schwachstellen und Auswirkungen bewerten - **Risikobehandlungsplan** erstellen: Für jedes Risiko entscheiden — vermeiden, reduzieren, übertragen, akzeptieren - **Regelmäßige Überprüfung** (mindestens jährlich, nach Vorfällen sofort)

Typischer Ist-Zustand bei Caritas-Trägern: - Kein formales ISMS vorhanden - Kein systematisches Asset-Inventar - Risikoanalysen höchstens informell ("der IT-Leiter weiß Bescheid") - Kein dokumentiertes Sicherheitskonzept

Aufwand:

Position	Einmalig	Jährlich
ISMS-Aufbau (externe Beratung)	60.000-120.000 EUR	
ISMS-Pflege und Weiterentwicklung		20.000-40.000 EUR
ISO-27001-Zertifizierung (optional, aber empfohlen)	15.000-30.000 EUR	10.000-15.000 EUR (Überwachungsaudit)
Oder: B3S-Konformitätsprüfung	10.000-20.000 EUR	10.000 EUR

Interne Arbeitszeit (Projektteam)	200-400 Personentage	50-100 Personentage

Maßnahme 2: Bewältigung von Sicherheitsvorfällen (Incident Response)

Was ist gefordert: Fähigkeit, Sicherheitsvorfälle zu erkennen, zu analysieren, einzudämmen und zu bewältigen. Muss mit den Meldepflichten (§32) verzahnt sein.

Was das praktisch bedeutet: - **Incident-Response-Plan** erstellen und testen - **CSIRT** (Computer Security Incident Response Team) aufbauen oder extern beauftragen - **24/7-Erreichbarkeit** sicherstellen (wegen 24h-Meldefrist!) - **Forensische Fähigkeiten** vorhalten oder vertraglich sichern - **Eskalationswege** definieren (IT → Geschäftsleitung → BSI) - **Regelmäßige Übungen** (Tabletop Exercises, mindestens 1x/Jahr)

Typischer Ist-Zustand bei Caritas-Trägern: - Kein formaler Incident-Response-Plan - Keine 24/7-Bereitschaft - Im Ernstfall: "Rufen wir den IT-Dienstleister an" - Keine forensischen Fähigkeiten - Keine Übungen

Aufwand:

Position	Einmalig	Jährlich
IR-Plan erstellen	5.000-15.000 EUR	3.000 EUR (Aktualisierung)
Caritas-Netzwerk IT „Cyber-Feuerwehr" / Mitgliedschaft		5.000-25.000 EUR (je nach Größe)
Alternativ: Externer IR-Retainer		30.000-80.000 EUR
Tabletop Exercise (1x/Jahr)		5.000-10.000 EUR
Forensik-Tools (bei interner Capability)	10.000 EUR	5.000 EUR (Lizenzen)

Empfehlung: Das **Caritas-Netzwerk IT** bietet einen gemeinsamen Incident-Response-Service mit 24/7-Hotline und bis zu 100 Stunden Expertenhilfe pro Vorfall — deutlich günstiger als ein eigener IR-Retainer.

Maßnahme 3: Business Continuity Management (BCM)

Was ist gefordert: Aufrechterhaltung und Wiederherstellung des Betriebs, einschließlich Backup-Management, Disaster Recovery und Krisenmanagement.

Was das praktisch bedeutet: - **Business Impact Analyse (BIA):** Welche Prozesse sind kritisch? Wie lange darf der Ausfall maximal dauern? - **Backup-Strategie** nach 3-2-1-Regel: 3 Kopien, 2 verschiedene Medien, 1 offsite/air-gapped - **Disaster-Recovery-Plan:** Wie werden Systeme wiederhergestellt? In welcher

Reihenfolge? - **Krisenmanagement:** Krisenstab, Kommunikationswege, Notfallhandbuch (auch in Papierform!) - **Regelmäßige Tests:** Backup-Restore-Tests (mindestens quartalsweise), DR-Tests (jährlich)

Typischer Ist-Zustand bei Caritas-Trägern: - Backups vorhanden, aber oft nicht getestet - Keine air-gapped oder immutable Backups (→ Ransomware-Risiko!) - Kein formaler DR-Plan - Kein Krisenmanagement-Prozess - Caritas München 2022: Ransomware → 23 Mio. EUR Schaden

Aufwand:

Position	Einmalig	Jährlich
BIA + BCM-Konzept	15.000-30.000 EUR	5.000 EUR (Pflege
Backup-Infrastruktur-Upgrade (air-gapped, immutable)	30.000-100.000 EUR	10.000-30.000 EUR
Disaster-Recovery-Standort / Cloud-DR	20.000-50.000 EUR	20.000-60.000 EUR
DR-Test (1x/Jahr)		5.000-15.000 EUR
Notfallhandbuch erstellen	5.000 EUR	2.000 EUR (Pflege)

Maßnahme 4: Sicherheit der Lieferkette

Was ist gefordert: Sicherheitsbezogene Aspekte der Beziehungen zu unmittelbaren Anbietern und Diensteanbietern, einschließlich Bewertung des allgemeinen Sicherheitsniveaus der Anbieter.

Was das praktisch bedeutet: - **Inventar aller IT-Dienstleister und -Lieferanten** erstellen - **Risikobewertung** jedes Dienstleisters (Fragebogen, Zertifikate, SLAs) - **Vertragliche Sicherheitsklauseln** in allen IT-Verträgen (Audit-Rechte, Meldepflichten, Sicherheitsstandards) - **Regelmäßige Überprüfung** (mindestens jährlich) - **Besondere Aufmerksamkeit** für: SoCura/IT-Dienstleister, Cloud-Anbieter, Softwareanbieter, Fernwartungszugänge

Typischer Ist-Zustand bei Caritas-Trägern: - Kein Dienstleisterverzeichnis - Verträge ohne IT-Sicherheitsklauseln - Keine Risikobewertung von Lieferanten - Fernwartungszugänge ohne Kontrolle

Aufwand:

Position	Einmalig	Jährlich
Dienstleister-Inventar + Erstbewertung	10.000-25.000 EUR	
Lieferanten-Assessment-Tool (Software)	5.000 EUR	3.000-10.000 EUR
Vertragsanpassungen (Rechtsberatung)	10.000-20.000 EUR	5.000 EUR
Jährliche Neubewertung (intern)		20-40 Personentage

Maßnahme 5: Sichere Beschaffung, Entwicklung und Wartung von IT-Systemen

Was ist gefordert: Sicherheit bei Erwerb, Entwicklung und Wartung von Netz- und Informationssystemen, einschließlich Management und Offenlegung von Schwachstellen.

Was das praktisch bedeutet: - **Patch-Management-Prozess:** Kritische Patches innerhalb von 72h, alle Patches innerhalb von 30 Tagen - **Schwachstellenmanagement:** Regelmäßige Vulnerability Scans (mindestens monatlich) - **Sichere Konfiguration:** Härtung aller Systeme nach CIS Benchmarks oder BSI-Empfehlungen - **Change Management:** Dokumentierte Freigabeprozesse für IT-Änderungen - **End-of-Life-Management:** Keine Systeme ohne Sicherheitsupdates im Betrieb

Typischer Ist-Zustand bei Caritas-Trägern: - Patches werden “irgendwann” eingespielt - Kein Vulnerability Scanning - Windows-Server mit Standardkonfiguration - Alte Systeme (Windows Server 2012, XP-Clients in der Medizintechnik) noch im Netz - Kein formales Change Management

Aufwand:

Position	Einmalig	Jährlich
Patch-Management-System (z.B. WSUS, SCCM, Intune)	5.000-20.000 EUR	5.000-15.000 EUR
Vulnerability Scanner (Tenable, Qualys etc.)	5.000 EUR	15.000-40.000 EUR
Systemhärtung (Erstdurchlauf)	20.000-50.000 EUR	
End-of-Life-Systeme ablösen	50.000-200.000 EUR	
Change-Management-Prozess	5.000 EUR	Personalaufwand

Maßnahme 6: Bewertung der Wirksamkeit von Maßnahmen

Was ist gefordert: Konzepte und Verfahren zur Bewertung der Wirksamkeit der Risikomanagementmaßnahmen.

Was das praktisch bedeutet: - **Interne Audits** (mindestens jährlich) - **Penetrationstests** (mindestens jährlich, bei KRITIS häufiger) - **Kennzahlen (KPIs)** für IT-Sicherheit definieren und messen - **Management-Reviews** (Vorstellung der Ergebnisse vor der Geschäftsleitung)

Aufwand:

Position	Einmalig	Jährlich
Penetrationstest (extern)		15.000-40.000 EUR

Interner Audit (eigene oder Diözesanverband-Ressourcen)		10.000-20.000 EUR
KPI-Dashboard aufbauen	5.000 EUR	2.000 EUR
Red-Team-Assessment (optional, für KRITIS)		30.000-60.000 EUR

Maßnahme 7: Cyberhygiene und Schulungen

Was ist gefordert: Grundlegende Verfahren der Cyberhygiene und Schulungen im Bereich der Sicherheit von Netz- und Informationssystemen.

Was das praktisch bedeutet: - **Awareness-Schulungen für ALLE Mitarbeitenden** (inkl. Pflege, Kita, Werkstatt) - **Phishing-Simulationen** (regelmäßig, mindestens quartalsweise) - **Passwortrichtlinien** (Mindestlänge, Komplexität, keine Wiederverwendung) - **Clean-Desk-Policy** und Bildschirmsperren - **Spezialschulungen** für IT-Personal - **Geschäftsleitungsschulungen** (§38 BSIG — gesonderte Pflicht!)

Typischer Ist-Zustand bei Caritas-Trägern: - Keine systematischen Awareness-Schulungen - Passwörter: “Caritas2024” oder Post-its am Monitor - Kein Phishing-Training - Geteilte Accounts (“Station3-PC”) - Geschäftsleitung: “IT-Sicherheit ist Sache der IT-Abteilung”

Aufwand:

Position	Einmalig	Jährlich
E-Learning-Plattform (z.B. SoSafe)	5.000 EUR (Setup)	10.000-30.000 EUR (nach Nutzeranzahl)
Phishing-Simulationen		Im E-Learning enthalten
Geschäftsleitungsschulung (§38 BSIG)		2.000-5.000 EUR
IT-Fachschulungen (CISSP, CompTIA Sec+)		5.000-15.000 EUR
Rollout-Aufwand (alle MA schulen, Schichtdienst!)	20.000-40.000 EUR	

Sonderproblem Caritas: Viele Mitarbeitende arbeiten im Schichtdienst, in der Pflege, in Werkstätten oder in Kitas — sie sitzen **nicht am PC**. Schulungskonzepte müssen das berücksichtigen (z.B. Kurzvideos auf dem Smartphone, Präsenzschulungen in Teamzeiten).

Maßnahme 8: Kryptografie und Verschlüsselung

Was ist gefordert: Konzepte und Verfahren für den Einsatz von Kryptografie und, wo angemessen, von Verschlüsselung.

Was das praktisch bedeutet: - **Verschlüsselung "at rest":** Festplattenverschlüsselung (BitLocker, FileVault) auf allen Endgeräten - **Verschlüsselung "in transit":** TLS 1.2+ für alle Verbindungen, VPN für Fernzugriff - **E-Mail-Verschlüsselung:** Mindestens Transportverschlüsselung, idealerweise S/MIME oder Gateway-Verschlüsselung - **WLAN-Verschlüsselung:** WPA3 oder mindestens WPA2-Enterprise - **Schlüsselmanagement:** Wer verwaltet die Schlüssel? Backup der Schlüssel?

Typischer Ist-Zustand bei Caritas-Trägern: - Keine Festplattenverschlüsselung auf Notebooks - Offene WLANs oder WPA2-Personal mit geteiltem Passwort - E-Mails unverschlüsselt - USB-Sticks ohne Verschlüsselung

Aufwand:

Position	Einmalig	Jährlich
BitLocker-Rollout (alle Endgeräte)	5.000-15.000 EUR	
E-Mail-Gateway-Verschlüsselung	5.000-10.000 EUR	3.000-8.000 EUR
VPN-Erneuerung (falls veraltet)	10.000-30.000 EUR	5.000-10.000 EUR
WLAN-Upgrade auf WPA2-Enterprise/WPA3	10.000-40.000 EUR	
PKI / Zertifikatsmanagement	5.000-15.000 EUR	3.000-5.000 EUR

Maßnahme 9: Personalsicherheit, Zugriffskontrolle, Asset-Management

Was ist gefordert: Sicherheit des Personals, Konzepte für die Zugriffskontrolle und Management von Anlagen (Assets).

Was das praktisch bedeutet: - **Identity & Access Management (IAM):** Wer hat Zugriff auf was? Least-Privilege-Prinzip! - **Privileged Access Management (PAM):** Admin-Zugänge besonders schützen - **Joiner-Mover-Leaver-Prozess:** Bei Eintritt → Rechte vergeben. Bei Wechsel → Rechte anpassen. Bei Austritt → Rechte sofort entziehen! - **Asset-Management:** Vollständiges Inventar aller Hardware, Software, Daten - **Personalsicherheit:** Verpflichtungserklärungen, Sicherheitsüberprüfungen für kritische Rollen

Typischer Ist-Zustand bei Caritas-Trägern: - "Alle haben Adminrechte, weil es sonst nicht geht" - Kein Offboarding-Prozess (Ex-Mitarbeiter haben noch Zugang) - Kein vollständiges IT-Asset-Register - Shared Accounts auf Stationen ("PflegePC-Station3")

Aufwand:

Position	Einmalig	Jährlich
IAM-System (z.B. Azure AD P1/P2, Okta)	10.000-30.000 EUR	15.000-50.000 EUR
PAM-System (z.B. CyberArk, BeyondTrust)	15.000-40.000 EUR	10.000-25.000 EUR
Asset-Management-Tool (z.B. CMDB)	5.000-15.000 EUR	5.000-10.000 EUR
Aufräumen bestehender Rechte (Erstdurchlauf)	20.000-50.000 EUR	
Joiner-Mover-Leaver-Prozess etablieren	5.000 EUR	Personalaufwand

Maßnahme 10: Multi-Faktor-Authentifizierung (MFA) und gesicherte Kommunikation

Was ist gefordert: Verwendung von Lösungen zur Multi-Faktor-Authentifizierung oder kontinuierlichen Authentifizierung, gesicherte Sprach-, Video- und Textkommunikation sowie gesicherte Notfallkommunikationssysteme.

Was das praktisch bedeutet: - **MFA für ALLE Benutzer** — nicht nur für Admins, sondern für jeden Login - **MFA-Methoden:** Hardware-Token (FIDO2), Authenticator-App, Smartcard — **keine SMS!** (unsicher) - **Gesicherte Kommunikation:** Verschlüsselte Messenger für interne Kommunikation (nicht WhatsApp!) - **Notfallkommunikation:** Out-of-Band-Kommunikation, die auch bei IT-Ausfall funktioniert (z.B. Mobiltelefon-Kette, Satellitentelefon für Krisenstab)

Typischer Ist-Zustand bei Caritas-Trägern: - Keine MFA — nirgendwo - Passwort "Caritas2024" für alle - WhatsApp als Hauptkommunikationsmittel - Bei IT-Ausfall: keine Kommunikationsmöglichkeit (siehe Caritas München 2022)

Aufwand:

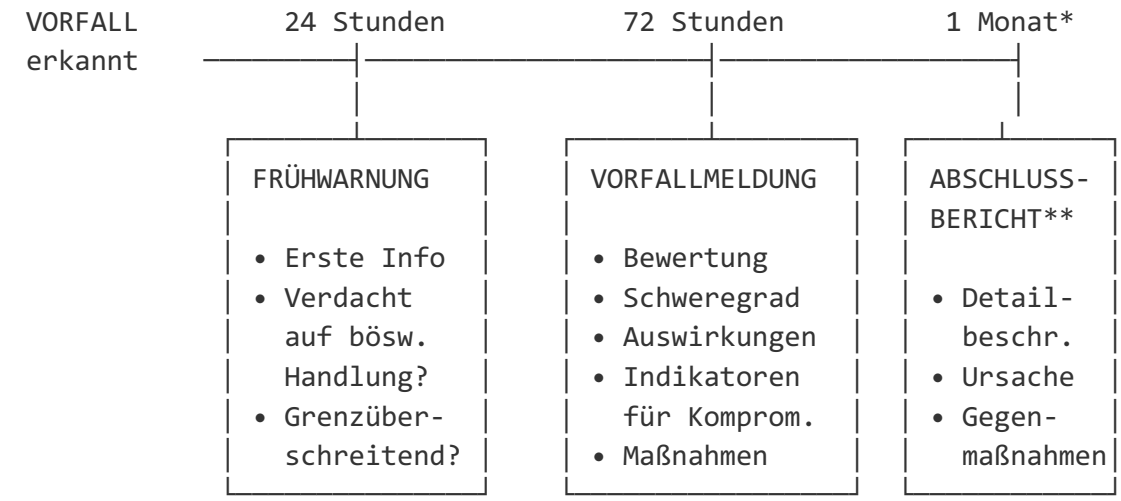
Position	Einmalig	Jährlich
MFA-Rollout (Hardware-Token für alle, z.B. YubiKey)	20.000-60.000 EUR (bei 2.500 MA: ~10 EUR/Token + Rollout)	5.000-10.000 EUR (Ersatz, neue MA)
Alternativ: Microsoft Authenticator (bei M365)	5.000 EUR (Rollout)	Im M365-Lizenzpreis
Sicherer Messenger (z.B. Threema Work, Signal)	5.000 EUR	5.000-15.000 EUR
Notfallkommunikation (Mobiltelefone, Krisenstab)	3.000-10.000 EUR	2.000 EUR

Sonderproblem Caritas — MFA im Schichtdienst: Pflegekräfte und Werkstattmitarbeiter teilen sich PCs und wechseln häufig. MFA darf den Arbeitsablauf nicht blockieren. Lösungen: Smartcard am Namensschild, Tap-and-Go mit FIDO2-Token, Fast User Switching.

8.4 Meldepflichten (§32 BSIG) — Der Dreistufenprozess

Bei “erheblichen Sicherheitsvorfällen” müssen drei Meldungen an das BSI erfolgen:

MELDEPFLICHTEN — DREISTUFIG



Meldeweg: BSI-Meldeportal (online)
Wer meldet: Benannte Kontaktstelle (§33 Abs. 2 BSIG)
Erreichbarkeit: 24/7 — auch am Wochenende!
*1 Monat nach der Vorfallmeldung
**2 Wenn Vorfall noch andauert: Fortschrittbericht

Was ist ein “erheblicher Sicherheitsvorfall”?

Ein Vorfall gilt als erheblich, wenn er: - **schwerwiegende Betriebsstörungen** der Dienste verursacht hat oder verursachen kann, **ODER** - **finanzielle Verluste** für die Einrichtung verursacht hat oder verursachen kann, **ODER** - **andere natürliche oder juristische Personen** durch erhebliche materielle oder immaterielle Schäden beeinträchtigt hat oder beeinträchtigen kann

Für Krankenhäuser besonders relevant: Jeder Vorfall, der potenziell die Patientenversorgung beeinträchtigt, dürfte als “erheblich” gelten.

Organisatorische Voraussetzungen: - **24/7-Erreichbarkeit** einer Person, die Vorfälle bewerten und melden kann - **Klare Eskalationswege:** IT-Mitarbeiter → IT-Leitung → CISO → Geschäftsleitung → BSI - **Vorformulierte Meldetexte** (Templates für Frühwarnung und Vorfallmeldung) - **Regelmäßige Übungen** des Meldeprozesses

8.5 Governance und Geschäftsleiterhaftung (§38 BSIG)

Dies ist der Bereich, der Vorstände und Geschäftsführer **persönlich** am unmittelbarsten betrifft:

GESCHÄFTSLEITERPFLICHTEN NACH §38 BSIG

1. UMSETZUNGS- UND ÜBERWACHUNGSPFLICHT (§38 Abs. 1)
   Die Geschäftsleitung MUSS die Risikomanagement-maßnahmen nach §30 BSIG umsetzen und ihre Umsetzung überwachen.
   → Nicht delegierbar, nicht auf den IT-Leiter abschiebbar
   → Dokumentierte Umsetzungsentscheidung erforderlich
   → Regelmäßige Berichte des CISO/ISB
   → Management-Reviews (mindestens halbjährlich)
   → Kenntnis des aktuellen Sicherheitsstatus

   Hinweis: Die EU-NIS-2-Richtlinie (Art. 20) spricht von "billigen" (approve); der deutsche Gesetzgeber hat dies zu "umsetzen und überwachen" verschärft – die GL muss also nicht nur abnicken, sondern aktiv die Umsetzung betreiben.

2. SCHULUNGSPFLICHT (§38 Abs. 3)
   Geschäftsleiter MÜSSEN regelmäßig an Schulungen teilnehmen, um ausreichende Kenntnisse und Fähigkeiten zur Erkennung und Bewertung von Risiken zu erwerben.
   → Empfehlung: Alle 2-3 Jahre, nach Vorfällen sofort
   → Z.B. IHK-Akademie, TÜV, etc.

3. PERSÖNLICHE HAFTUNG (§38 Abs. 2)
   • Innenhaftung: GL haftet ihrer Einrichtung für schuldhaft verursachte Schäden
   • Haftung nach gesellschaftsrechtlichen Grundsätzen (GmbHG §43 – Sorgfalt eines ordentlichen Geschäftsmannes)
   • Haftung mit PRIVATVERMÖGEN bei Pflichtverletzung (z.B. Nichtumsetzung trotz Kenntnis der Pflichten)

Wichtiger Unterschied zum Regierungsentwurf:
Das ursprünglich geplante Verzichtsverbot (Verbot des Verzichts auf Schadensersatzansprüche) wurde im Gesetzgebungsverfahren GESTRICHEN. Es gelten die allgemeinen gesellschaftsrechtlichen Regeln.
→ Bei einer gGmbH: §43 Abs. 3 GmbHG – Verzicht oder Vergleich nur mit Zustimmung der Gesellschafter und nicht vor Ablauf von 3 Jahren nach Entstehung des Anspruchs (wenn keine Gläubigerbeeinträchtigung).
→ In der Praxis bleibt die Haftung dennoch scharf.

⚠ Bei Bußgeld von 10 Mio. EUR: Die GL haftet persönlich gegenüber der gGmbH für den entstandenen Schaden!

8.6 KRITIS-Zusatzpflichten (§31 BSIG) — Falls Krankenhaus >30.000 Fälle/Jahr

Wenn das Krankenhaus die KRITIS-Schwelle überschreitet (>30.000 vollstationäre Fälle/Jahr), kommen **zusätzlich** zu allen NIS-2-Pflichten:

Pflicht	Detail	Kosten
Systeme zur Angriffserkennung (SzA)	SIEM + SOC mit 24/7-Monitoring, Protokollierung, Anomalieerkennung	80.000-250.000 EUR/Jahr
Nachweispflicht alle 3 Jahre	Audit durch BSI-anerkannte Prüfer (§39 BSIG)	30.000-80.000 EUR pro Audit
Verschärfte Meldepflichten	Wie NIS-2, aber BSI kann zusätzliche Informationen verlangen	Personalaufwand
BSI-Aufsicht	Aktive Kontrolle (nicht nur anlassbezogen wie bei “wichtigen Einrichtungen”)	—

9. Umsetzungskosten: Was es wirklich kostet

9.1 Gesamtkostenübersicht für einen Caritas-Komplexträger

Referenzszenario: Caritas-gGmbH mit Krankenhaus, 5 Pflegeheimen, 12 Kitas, WfbM, Beratungsstellen. 2.500 Mitarbeitende, 180 Mio. EUR Umsatz. Gemeinsame IT-Infrastruktur. Bisheriger IT-Sicherheitsstatus: grundlegend.

```
GESAMTKOSTEN NIS-2-UMSETZUNG – REALISTISCHE SCHÄTZUNG
═══════════════════════════════════════════════════════

EINMALIGE INVESTITIONSKOSTEN:
─────────────────────────────

  ISMS-Aufbau (Beratung + intern)                120.000 EUR
  Netzwerksegmentierung (Hardware + Umbau)       200.000 EUR
  Firewall-Erneuerung / NGFW                      80.000 EUR
  Endpoint Detection & Response (Rollout)         50.000 EUR
  Backup-Infrastruktur (air-gapped, immutable)    60.000 EUR
  MFA-Rollout (alle Mitarbeitenden)               30.000 EUR
  IAM/PAM-System                                  40.000 EUR
  Verschlüsselung (BitLocker, WLAN, VPN)          30.000 EUR
  Vulnerability Scanner + Systemhärtung           40.000 EUR
  End-of-Life-Systeme ablösen                    100.000 EUR
  Prozessdokumentation + Notfallhandbuch          30.000 EUR
  BSI-Registrierung + Erstaudit                   20.000 EUR
  Projektmanagement (intern)                      50.000 EUR
  ──────────────────────────────────────────────────────────
  SUMME EINMALIG:                              ca. 850.000 EUR
  (Spanne: 500.000 - 1.200.000 EUR)

JÄHRLICHE LAUFENDE KOSTEN:
──────────────────────────

  CISO / ISB (1 Vollzeitstelle, 70-120k Gehalt)   100.000 EUR
  IT-Security-Analyst (0,5 VZÄ)                    40.000 EUR
  Security-Lizenzen (EDR, SIEM, Firewall, IAM)    150.000 EUR
  Managed SOC / Monitoring                         80.000 EUR
  Penetrationstests (2x/Jahr)                      30.000 EUR
  Awareness-Schulungen (alle MA)                   25.000 EUR
  Geschäftsleitungsschulung (§38)                   3.000 EUR
  BSI-Konformitätsprüfungen / Audits               15.000 EUR
  Incident-Response-Bereitschaft                   25.000 EUR
  Cyber-Versicherung                               30.000 EUR
  Patch-/Schwachstellenmanagement                  15.000 EUR
  Lieferkettenmanagement                           10.000 EUR
  ISMS-Pflege und Dokumentation                    15.000 EUR
  ──────────────────────────────────────────────────────────
  SUMME JÄHRLICH:                               ca. 538.000 EUR
  (Spanne: 350.000 - 800.000 EUR)
```

9.2 Personalkosten — Die größte laufende Belastung

Rolle	Vollzeit/Teilzeit	Bruttogehalt (inkl. AG-Anteil)	Alternativ extern
CISO / ISB	1,0 VZÄ (ab 1.000 MA unverzichtbar)	85.000-130.000 EUR/Jahr	Externer ISB: 40.000-80.000 EUR/Jahr (weniger Präsenz)
IT-Security-Analyst	0,5-1,0 VZÄ	55.000-80.000 EUR/Jahr	Managed SOC: 60.000-120.000 EUR/Jahr
IT-Security-Engineer	0,5 VZÄ	50.000-70.000 EUR/Jahr	Projektbasiert
Datenschutzbeauftragter	oft schon vorhanden	—	Synergien mit CISO

Problem: Fachkräftemangel. IT-Sicherheitsfachkräfte sind auf dem Arbeitsmarkt extrem knapp. Die Caritas-Vergütung (AVR) liegt unter dem Marktniveau der IT-Branche/IT-Experten. Empfehlung: Kombination aus interner Basisrolle + externer Unterstützung.

9.3 Kostenvergleich: Compliance vs. Nicht-Compliance

```
WAS KOSTET MEHR?
═══════════════

NIS-2-Compliance (jährlich):                ca.   540.000 EUR
──────────────────────────────────────────────────────────────

                                                    vs.

Nicht-Compliance:
├── Bußgeld (bis 10 Mio. EUR / 2% Umsatz)      10.000.000 EUR
├── Ransomware-Schaden (vgl. Caritas München)  23.000.000 EUR
├── Betriebsunterbrechung (Wochen-Monate)      unkalkulierbar
├── Reputationsschaden                         unkalkulierbar
├── Persönliche GL-Haftung                     Privatvermögen
└── Bußgeld bei Nicht-Registrierung               500.000 EUR
                                              ──────────────────
                                              bis zu 33.500.000+ EUR
```

9.4 Was die Bundesregierung geschätzt hat — und warum das zu wenig ist

Die Bundesregierung hat im Gesetzgebungsverfahren folgende Kosten geschätzt:

Kennzahl	Regierungsschätzung	Realistische Schätzung (ohne Basis-IT)
Erfüllungsaufwand pro Einrichtung (einmalig)	37.060 EUR	500.000-1.200.000 EUR
Erfüllungsaufwand pro Einrichtung (jährlich)	209.000 EUR	350.000-800.000 EUR

Warum die Regierungsschätzung zu niedrig ist: 1. Sie geht von einem **bestehenden Grundniveau** an IT-Sicherheit aus 2. Sie mittelt über alle 29.000 betroffenen Einrichtungen (inkl. große Konzerne mit

bestehenden ISMS) 3. Sie berücksichtigt **nicht** den Investitionsstau in der Sozialwirtschaft 4. Sie berücksichtigt **nicht** die Komplexträger-Problematik

10. Refinanzierung: Wer bezahlt das?

10.1 Das Grundproblem

Die Sozialwirtschaft unterscheidet sich fundamental von der gewerblichen Wirtschaft: Sie kann Kosten **nicht über Preise weitergeben**. Caritas-Träger sind abhängig von **administrierten Preisen**, die durch Kostenträger festgelegt oder verhandelt werden:

Leistungsbereich	Kostenträger	Rechtsgrundlage
Krankenhausbehandlung	Krankenkassen (DRG) + Länder (Investitionen)	KHG, KHEntgG
Stationäre Pflege	Pflegekassen + Sozialhilfeträger	SGB XI (§§84-85)
Ambulante Pflege	Pflegekassen	SGB XI, SGB V
Eingliederungshilfe	Eingliederungshilfeträger	SGB IX (§§123-125)
Kinder- und Jugendhilfe	Jugendämter	SGB VIII (§§78a-g)

Das NIS-2-Dilemma: Der Gesetzgeber hat eine Pflicht geschaffen, deren Nichteinhaltung mit bis zu 10 Mio. EUR bestraft wird — aber **keine Finanzierungsregelung** vorgesehen. Es gibt **keine politische Zusage** zur Refinanzierung.

10.2 Refinanzierung im Krankenhausbereich

Duale Finanzierung

```
DUALE FINANZIERUNG — WO FALLEN NIS-2-KOSTEN HIN?
═══════════════════════════════════════════════

  Länder (KHG §9)                Krankenkassen (DRG)
  Investitionskosten              Betriebskosten
  ├── Firewalls (Hardware)       ├── CISO-Gehalt
  ├── Netzwerktechnik            ├── Security-Lizenzen
  ├── Server                     ├── SOC-Dienstleistung
  ├── Netzwerksegmentierung      ├── Schulungen
  └── IT-Erstausstattung         ├── Penetrationstests
                                 └── Incident Response

  PROBLEM: Investitionsstau      PROBLEM: Kein IT-Sicherheits-
  von 30+ Mrd. EUR!              zuschlag in DRG-Fallpauschalen!
  Länder können regulären        InEK-Kalkulation erfasst IT-
  Bedarf nicht decken.           Kosten nur pauschal mit
                                 2-3 Jahren Verzögerung.
```

KHZG — Praktisch aufgebraucht

Das Krankenhauszukunftsgesetz stellte 4,3 Mrd. EUR bereit (davon IT-Sicherheit als Fördertatbestand 10). **Stand Februar 2026:** Von 2,952 Mrd. EUR Bundesmitteln wurden 2,938 Mrd. EUR bewilligt — der Fonds ist **leer**.

Krankenhäuser, die KHZG-Mittel für IT-Sicherheit genutzt haben, profitieren bei der NIS-2-Umsetzung von Synergieeffekten (ISMS-Aufbau, Netzwerksegmentierung). Wer die KHZG-Mittel nicht für IT-Sicherheit verwendet hat, steht jetzt schlechter da.

Krankenhaustransformationsfonds (KHTF) — ab 2026

Der KHTF (50 Mrd. EUR bis 2035) ist der wichtigste zukünftige Finanzierungsweg. IT-Sicherheit ist **explizit förderfähig** in den Fördertatbeständen 1-5 der KHTFV. **Aber:** Nur als Teil von Strukturmaßnahmen, nicht als eigenständiger Fördertatbestand. Und: **Betriebskosten bleiben nicht förderfähig** — nur Investitionen.

DKG-Kritik

Die Deutsche Krankenhausgesellschaft hat in vier Stellungnahmen (2023-2025) die fehlende Refinanzierung scharf kritisiert: > *"Krankenhäuser haben derzeit keinerlei Refinanzierungsmöglichkeiten der aus Digitalisierungsmaßnahmen entstehenden Kosten."*

10.3 Refinanzierung im Pflegebereich

Pflegeeinrichtungen sind direkt nicht NIS-2-betroffen — aber bei Komplexträgern mit gemeinsamer IT muss die Pflege-IT ebenfalls geschützt werden.

Pflegesatzverhandlungen (§§84-85 SGB XI)

IT-Sicherheitskosten können als **Sachkosten** in Pflegesatzverhandlungen eingebracht werden:

```
PFLEGESATZ-KALKULATION MIT NIS-2-KOSTEN
═══════════════════════════════════════

Sachkosten / Betriebsaufwand:
├── Verwaltungsbedarf
│   ├── IT-Kosten (Hardware, Software, Lizenzen)
│   ├── [NEU] IT-Sicherheitslizenzen
│   ├── [NEU] Managed Security Services
│   └── [NEU] BSI-konforme Schulungen
├── Versicherungen
│   └── [NEU] Cyber-Versicherung
├── Externe Beratung
│   └── [NEU] ISMS-Beratung, Audit-Kosten
└── Personalkosten Verwaltung
    └── [NEU] Anteiliger CISO / IT-Sicherheitspersonal
```

Herausforderung: Pflegekassen nutzen den "externen Vergleich" — wenn andere Einrichtungen die NIS-2-Kosten noch nicht eingepreist haben, gelten sie als "überdurchschnittlich". Bei Ablehnung: **Schiedsstelle** (§76 SGB XI), dann Sozialgericht.

Digitalisierungsförderung §8 Abs. 8 SGB XI

- Förderhöhe: Bis 40%, max. **12.000 EUR pro Einrichtung**
- IT-Sicherheit ist **explizit förderfähig**
- Laufzeit: Bis 2030
- Bewertung: **Ein Tropfen auf den heißen Stein** — aber für Einzelmaßnahmen nutzbar (MFA-Hardware, Schulungen)

10.4 Refinanzierung in der Eingliederungshilfe

IT-Sicherheitskosten können als **Sachkosten** in Vergütungsvereinbarungen nach §125 SGB IX eingebracht werden. Das stärkste Argument: **betriebsnotwendige Kosten** (§125 Abs. 3 SGB IX) — die IT-Sicherheitsinfrastruktur gehört zur betriebsnotwendigen Ausstattung.

10.5 Refinanzierung in der Kinder- und Jugendhilfe

IT-Kosten sind in der Jugendhilfe als Teil der **Gemeinkosten** (Overhead) anerkannt (§78c SGB VIII). IT-Sicherheitskosten können in die nächste Entgeltverhandlung eingebracht werden.

10.6 Das zentrale Argument: Gesetzliche Pflicht = nicht disponibel

NIS-2-Compliance ist eine gesetzliche Pflicht. Ein Kostenträger kann die Refinanzierung gesetzlich zwingender Kosten nicht dauerhaft verweigern.

Gesetzliche Pflicht	Wurde refinanziert?	Mechanismus
Brandschutz	Ja	Investitionen: Land. Laufend: Entgelt
DSGVO (2018)	Teilweise	Sukzessive in Sachkosten einkalkuliert
Hygieneverordnung	Ja	Hygienezuschläge
Arbeitssicherheit	Ja	Als Gemeinkosten anerkannt
Mindestlohn	Ja	Automatische Entgeltanpassung
NIS-2 (2025)	**Offen**	Kein Förderprogramm, kein Zuschlag

Rechtsweg bei Ablehnung: 1. Pflegekasse lehnt ab → **Schiedsstelle** (§76 SGB XI) → Sozialgericht 2. Eingliederungshilfeträger lehnt ab → Klage nach SGB IX 3. Jugendamt lehnt ab → Klage nach SGB VIII 4. Krankenhaus → Keine direkte Durchsetzbarkeit bei DRG. Investitionsförderung: Antrag beim Land

10.7 Die Gemeinkostenumlage — Das wichtigste interne Instrument

Für Komplexträger ist die Gemeinkostenumlage das zentrale Instrument:

```
GEMEINKOSTENUMLAGE IT-SICHERHEIT (Beispiel)
═══════════════════════════════════════════

Zentrale IT-Sicherheitskosten:                538.000 EUR/Jahr

Umlage nach Mitarbeiter-Anteil:
  Krankenhaus     (32% = 800 MA)    →  172.160 EUR  → DRG
  Pflegeheime     (28% = 700 MA)    →  150.640 EUR  → Pflegesatz
  WfbM            (16% = 400 MA)    →   86.080 EUR  → EGH-Vereinbarung
  Kitas           (10% = 250 MA)    →   53.800 EUR  → Jugendhilfe-Entgelt
  Beratung        (6%  = 150 MA)    →   32.280 EUR  → Zuschüsse/Eigenmittel
  Verwaltung      (8%  = 200 MA)    →   43.040 EUR  → Umlage auf alle

KOSTEN PRO MITARBEITER:              215 EUR/Jahr
KOSTEN PRO PFLEGEPLATZ (500 Plätze): 301 EUR/Jahr = 0,82 EUR/Tag
```

0,82 EUR pro Pflegeplatz und Tag — das ist die Größenordnung, die in Pflegesatzverhandlungen argumentiert werden muss. Zum Vergleich: Ein Pflegetag kostet durchschnittlich 90-150 EUR.

10.8 Kooperationsmodelle — Kosten drastisch senken

Maßnahme	Einzelträger	10 Träger gemeinsam	Ersparnis
CISO (Vollzeit)	100.000 EUR/Jahr	10.000 EUR/Träger	90%
ISMS-Aufbau	80.000 EUR	15.000 EUR/Träger	81%
SOC/SIEM	120.000 EUR/Jahr	18.000 EUR/Träger	85%
Penetrationstest	25.000 EUR	5.000 EUR/Träger	80%
Awareness-Schulungen	15.000 EUR/Jahr	3.000 EUR/Träger	80%

Schlüsselrolle: - **Caritas-Netzwerk IT:** 150 Mitgliedsorganisationen, 24/7-IR-Service, gemeinsame Beschaffung - **SoCura:** ISO-27001-zertifiziert, IT-Infrastruktur für 85.000+ Nutzer, NIS-2-compliant - **Diözesanverbände:** Koordination gemeinsamer ISMS-Vorlagen, geteilter CISO, Rahmenverträge

10.9 Förderprogramme — Was verfügbar ist

Programm	Verfügbarkeit	Förderung	Bewertung
KHZG (FT 10)	Aufgebraucht	—	Zu spät
KHTF (ab 2026)	Ab 2026, 50 Mrd. EUR	IT im Kontext von Strukturmaßnahmen	Wichtigster Weg für KH
§8 Abs. 8 SGB XI	Bis 2030	Max. 12.000 EUR/Einrichtung	Tropfen auf heißen Stein
rückenwind3 (ESF+)	Laufend	Bis 800.000 EUR/Projekt (50-70%)	Relevant für Sozialwirtschaft
BAFA Unternehmensberatung	Laufend	50-80%, max. 2.800 EUR	Für ISMS-Erstberatung
KfW Digitalisierung	Laufend	Kredit + 3-5% Tilgungszuschuss	Für gGmbH prüfen
Landesförderung	Länderabhängig	3.000-30.000 EUR	Meist nur gewerbliche KMU
EU Digital Europe	Calls laufend	Verschiedene	Eher Forschung, kaum operativ

10.10 Musterargumentation für Kostenträgerverhandlungen

Gegenüber Pflegekassen:

> **1.** Das NIS2-RLUG (in Kraft seit 06.12.2025) verpflichtet unseren Gesamtträger als “besonders wichtige Einrichtung” zur Umsetzung umfassender IT-Sicherheitsmaßnahmen (§30 BSIG).
>
> **2.** Die NIS-2-Pflichten erstrecken sich auf **alle IT-Systeme der juristischen Person** — einschließlich der Pflege-IT, die über gemeinsame Infrastruktur mit dem Krankenhaus verbunden ist.
>
> **3.** Nicht-Compliance führt zu Bußgeldern bis 10 Mio. EUR und persönlicher Geschäftsleiterhaftung.

> **4.** Diese Kosten sind **nicht disponibel** — vergleichbar mit Brandschutz und Hygieneverordnung, die ebenfalls als Sachkosten anerkannt werden.
>
> **5.** Kostenposition: Anteilige IT-Sicherheitskosten gemäß Gemeinkostenumlage: **0,82 EUR pro Pflegeplatz und Tag** (bei 500 Plätzen = 150.640 EUR/Jahr).
>
> **Rechtsgrundlage:** §84 Abs. 2 SGB XI — Pflegesätze müssen leistungsgerecht sein und dem Pflegeheim bei wirtschaftlicher Betriebsführung ermöglichen, seine Aufwendungen zu finanzieren.

Am besten durchsetzbare Kostenpositionen:

```
GUT DURCHSETZBAR:
├── IT-Sicherheitsschulungen (wie andere Pflichtschulungen)
├── Cyber-Versicherung (wie Betriebshaftpflicht)
├── Software-Lizenzen (wie andere IT-Sachkosten)
├── Externe Audits (wie Wirtschaftsprüfung)
└── Anteiliges CISO-Gehalt (wie Datenschutzbeauftragter)

MITTEL DURCHSETZBAR:
├── Managed Security Services
└── Penetrationstests

SCHWER DURCHSETZBAR:
├── Hardware-Investitionen (→ Investitionsschiene)
├── Netzwerk-Segmentierung (→ Einmalinvestition)
└── ISMS-Gesamtprojekt (→ auf mehrere Jahre verteilen)
```

10.11 Empfohlener Zeitplan für Kostenträgerverhandlungen

```
SOFORT (Feb/März 2026):
├── NIS-2-Kosten kalkulieren (siehe Musterkalkulation)
├── Umlageschlüssel festlegen und dokumentieren
├── Kostenträger schriftlich informieren
└── Nächste Verhandlungsrunde vorbereiten

Q2 2026:
├── Pflegesatzverhandlungen: IT-Sicherheit als Sachkosten einbringen
├── Leistungsvereinbarungen EGH: Betriebsnotwendige Sachkosten
├── Jugendhilfe-Entgelte: Gemeinkosten/Overhead
└── KHTF-Antrag vorbereiten (IT-Sicherheit im Kontext Strukturmaßnahme)

Q3/Q4 2026:
├── Verhandlungen führen
├── Bei Ablehnung: Schiedsstelle / Klage vorbereiten
└── Ergebnisse dokumentieren

LAUFEND:
├── Kostenentwicklung dokumentieren (Nachweispflicht!)
├── Rechnungen, Verträge, Audit-Berichte sammeln
└── Benchmarking mit anderen Caritas-Trägern
```

11. Fristen und Sanktionen

11.1 Aktuelle Fristen

Frist	Was
Seit 06.12.2025	Alle Pflichten gelten (Risikomanagement, Meldepflichten, Governance)
Bis 06.03.2026	Registrierung beim BSI
Laufend	Meldepflichten bei erheblichen Vorfällen (24h/72h/1 Monat)

11.2 Bußgelder

Kategorie	Höchstbetrag
Besonders wichtige Einrichtungen	Bis **10 Mio. EUR** oder **2%** des weltweiten Jahresumsatzes
Wichtige Einrichtungen	Bis **7 Mio. EUR** oder **1,4%** des weltweiten Jahresumsatzes
Nicht-Registrierung	Bis **500.000 EUR** (KRITIS-Krankenhäuser: Bis zu 1 Mio EUR)
Meldepflichtverletzung	Bis **500.000 EUR** (KRITIS-Krankenhäuser: Bis zu 1 Mio EUR)

11.3 Persönliche Geschäftsleiterhaftung

- Geschäftsleiter haften **mit ihrem Privatvermögen** gegenüber der Einrichtung für schuldhaft verursachte Schäden (§38 Abs. 2 BSIG)
- Haftung richtet sich nach dem jeweiligen Gesellschaftsrecht (bei gGmbH: §43 GmbHG — Sorgfalt eines ordentlichen Geschäftsmannes)
- Umsetzungs- und Überwachungspflicht ist **nicht delegierbar** — auch nicht an den IT-Leiter oder CISO (§38 Abs. 1 BSIG)
- Hinweis: Das im Regierungsentwurf enthaltene Verzichtsverbot wurde im Gesetzgebungsverfahren gestrichen. Es gelten die allgemeinen gesellschaftsrechtlichen Regeln (bei gGmbH: §43 Abs. 3 GmbHG — Verzicht/Vergleich nur eingeschränkt möglich).
- D&O-Versicherung kann das Risiko nur **teilweise abfangen** (bei Vorsatz/grober Fahrlässigkeit keine Deckung)

12. Praktischer Leitfaden: Was ist bei NIS-2-Betroffenheit zu tun?

Dieses Kapitel richtet sich an Caritas-Träger, die festgestellt haben (oder vermuten), dass sie unter NIS-2 fallen. Es gibt einen konkreten, praxisnahen Fahrplan — von der Registrierung über die ersten 90 Tage bis zum vollständigen ISMS = Informationssicherheitsmanagementsystem-Aufbau.

12.1 Sofortmaßnahme: BSI-Registrierung

12.1.1 Registrierungspflicht und Frist

Alle betroffenen Einrichtungen müssen sich **innerhalb von 3 Monaten** nach Inkrafttreten des Gesetzes beim BSI registrieren. NIS-2 ist am 06.12.2025 in Kraft getreten — die **Registrierungsfrist läuft damit am 06.03.2026 ab**.

> ***Achtung:*** *Wer die Registrierung versäumt, riskiert bereits ein Bußgeld von bis zu* ***500.000 EUR*** *(§65 BSIG, KRITIS-Einrichtungen auch höher). Die Registrierung ist keine freiwillige Betroffenheitsanzeige — es handelt sich um eine* ***gesetzliche Pflicht zur Selbstidentifikation****.*

Einrichtungen, die erst nach dem 06.12.2025 die Schwellenwerte überschreiten (z.B. durch Wachstum oder Umstrukturierung), müssen sich innerhalb von 3 Monaten ab dem Zeitpunkt registrieren, ab dem sie die Voraussetzungen erfüllen.

12.1.2 Schritt 1: "Mein Unternehmenskonto" (MUK) einrichten

Bevor Sie sich im BSI-Portal registrieren können, benötigen Sie ein **Unternehmenskonto über den ELSTER-Dienst**.

Was ist MUK? "Mein Unternehmenskonto" ist ein bundesweites Servicekonto für Unternehmen, das über die ELSTER-Infrastruktur der Finanzverwaltung läuft. Es dient als Authentifizierungsmechanismus für verschiedene Behördenportale — darunter nun auch das BSI-Portal.

Schritt-für-Schritt-Anleitung:

1. **Website aufrufen:** https://www.mein-unternehmenskonto.de
    - Registrierungsseite: https://www.mein-unternehmenskonto.de/registrierung
2. **Voraussetzung prüfen:** Sie benötigen eine **deutsche Steuernummer** Ihrer Organisation
3. **ELSTER Organisationszertifikat beantragen:**
    - Jede Person, die im BSI-Portal arbeiten soll, benötigt ein **eigenes ELSTER Organisationszertifikat**
    - Die Beantragung ist **kostenlos**
    - Pro Organisation sind bis zu 5.000 Zertifikate möglich
    - Sie erhalten zunächst eine E-Mail mit Grunddaten
    - **Wichtig:** Der **postalische Aktivierungsbrief** benötigt **mindestens 5 Werktage** — planen Sie diesen Vorlauf ein!
4. **Erste/r Registrierende/r wird Administrator/in:**
    - Die Person, die sich als erste registriert, erhält den Status "Verwalter"
    - Diese Person kann anschließend weitere Benutzer einladen und deren Berechtigungen verwalten

Empfehlung für Caritas-Träger: Registrieren Sie mindestens **zwei Personen** — idealerweise den/die IT-Sicherheitsbeauftragte/n und eine Vertretung. So stellen Sie sicher, dass die Meldewege auch bei Urlaub oder Krankheit funktionieren.

> ***Weitere Informationen des BSI zum MUK-Prozess:***
> https://www.bsi.bund.de/DE/Themen/Regulierte-Wirtschaft/NIS-2-regulierte-Unternehmen/NIS-2-MUK/MUK_node.html

12.1.3 Schritt 2: Im BSI-Portal registrieren

Das BSI-Portal ist seit dem **06.01.2026** aktiv und ist die zentrale Plattform für Registrierung, Vorfallsmeldungen und Kommunikation mit dem BSI.

Portal-URL: https://portal.bsi.bund.de

Anmeldung: 1. Rufen Sie https://portal.bsi.bund.de auf 2. Klicken Sie auf **"Mit MUK anmelden"** 3. Sie werden zum ELSTER-Login weitergeleitet 4. Laden Sie Ihr ELSTER Organisationszertifikat hoch und geben Sie Ihr Passwort ein 5. Nach der Authentifizierung werden Ihre Unternehmensdaten automatisch aus ELSTER übernommen

Welche Daten werden bei der Registrierung abgefragt?

Kategorie	Benötigte Daten	Hinweise
Stammdaten	Name, Adresse, Rechtsform	Werden aus ELSTER übernommen
Website	URL der Organisation	Optional
Status	Bundesbehörde, Körperschaft, Verein?	Für Caritas-Träger: meist gGmbH, e. V. oder KdöR
KRITIS-Status	Bestehende KRITIS-Registrierung?	Nur bei Krankenhäusern mit ≥30.000 vollstat. Fällen/Jahr
Unternehmensgröße	Mitarbeiterzahl, Jahresumsatz, Jahresbilanzsumme	Entscheidend für Einstufung als bwE oder wE
Sektor & Branche	Sektorauswahl (Dropdown), Branche, Einrichtungsart	Für Caritas-Krankenhäuser: "Gesundheitswesen" → "Erbringer von Gesundheitsdienstleistungen"
EU-Mitgliedstaaten	Alle EU-Staaten, in denen Dienste erbracht werden	Für die meisten Caritas-Träger: nur Deutschland
Zuständige Behörden	Aufsichtsbehörden (vollständige Namen)	Z.B. Gesundheitsamt, Heimaufsicht etc.
Einstufung	bwE (besonders wichtige Einrichtung) oder wE (wichtige Einrichtung)	Wird automatisch vorgeschlagen, kann aber eigenverantwortlich korrigiert werden
Kontaktstelle	Organisationseinheit/Abteilung, Adresse, 1-2 Telefonnummern (international, z.B. +49…), E-Mail-Adresse	**Empfehlung:** Verwenden Sie eine **Funktions-Mailbox** (z.B. it-sicherheit@caritas-xy.de), keine persönliche Adresse
Kontaktperson	Namentliche Ansprechperson für regulatorische Angelegenheiten	Mehrere Kontakte mit definierten Rollen möglich

Kategorie	Benötigte Daten	Hinweise
Öffentliche IP-Bereiche	Alle öffentlichen IPv4- und IPv6-Adressbereiche in CIDR-Notation	Mit beschreibenden Bezeichnungen versehen

> ***Wichtig:*** *Alle Änderungen an den registrierten Daten müssen* ***innerhalb von zwei Wochen*** *im Portal aktualisiert werden (§33 Abs. 5 BSIG).*

Detaillierte BSI-Registrierungsanleitung: https://www.bsi.bund.de/DE/Themen/Regulierte-Wirtschaft/NIS-2-regulierte-Unternehmen/NIS-2-Anleitung-Registrierung/Anleitung-Registrierung_node.html

12.1.4 Betroffenheitsprüfung: Bin ich überhaupt betroffen?

Falls noch Unsicherheit über die eigene Betroffenheit besteht, stellt das BSI ein **kostenloses, anonymes Online-Tool** zur Verfügung:

BSI-Betroffenheitsprüfung: https://betroffenheitspruefung-nis-2.bsi.de/

- Fragebogenbasiert, orientiert an den BSIG-Anlagen 1 und 2
- Prüft Sektor, Unternehmensgröße und Dienstearten
- Ergebnis ist **nicht rechtsverbindlich** und ersetzt nicht die offizielle Selbstidentifikation
- Als Entscheidungshilfe aber sehr empfehlenswert

Hinweis: für die Freie Wohlfahrt ist dieses Tool nicht spezifisch genug und kennt z.B. nicht die Ausnahmen für Pflege und die Herausforderungen von Komplexträgern – Antworten daher sehr mit Vorsicht bewerten.

Zusätzlich steht der **FitNIS2-Navigator** von “Deutschland sicher im Netz” zur Verfügung — ein modulares Tool, das nicht nur die Betroffenheit prüft, sondern auch bestehende IT-Sicherheitsmaßnahmen gegen NIS-2-Anforderungen abgleicht und konkrete Umsetzungsempfehlungen liefert.

12.2 Meldepflichten: Was melden, wie melden, wann melden?

12.2.1 Dreistufiges Meldeverfahren bei erheblichen Sicherheitsvorfällen

NIS-2 führt ein **dreistufiges Meldeverfahren** ein, das bewusst auf “Schnelligkeit vor Vollständigkeit” setzt — lieber schnell eine unvollständige Erstmeldung als zu spät eine vollständige.

Meldung	Frist	Was muss gemeldet werden?
Frühwarnung (Erstmeldung)	**24 Stunden** nach Kenntniserlangung	Dass ein erheblicher Vorfall eingetreten ist; Verdacht auf rechtswidrige/böswillige Handlung; mögliche grenzüberschreitende Auswirkungen
Folgemeldung (Update)	**72 Stunden** nach Kenntniserlangung	Erste Bewertung des Vorfalls: Schweregrad, Auswirkungen; Indikatoren für Kompromittierung (IoC); ergriffene Sofortmaßnahmen
Abschlussmeldung	**1 Monat** nach der Übermittlung der Folgemeldung	Detaillierte Beschreibung; Art der Bedrohung und Grundursache; alle ergriffenen und geplanten Abhilfemaßnahmen;

Meldung	Frist	Was muss gemeldet werden?
		grenzüberschreitende Auswirkungen

> ***Downloadbare BSI-Hilfen:*** - Meldepflicht One-Pager (PDF) — *ideales Aushang-Dokument für die IT-Abteilung* - Meldeprozess-Diagramm (PDF) — *Flussdiagramm des Meldeprozesses*

12.2.2 Was ist ein "erheblicher Sicherheitsvorfall"?

Ein Sicherheitsvorfall gilt als **erheblich** (§2 Nr. 11 BSIG), wenn er:

- **Schwerwiegende Betriebsstörungen** verursacht hat oder verursachen kann, **ODER**
- **Finanzielle Verluste** für die Einrichtung verursacht hat oder verursachen kann, **ODER**
- **Andere Personen** durch erhebliche materielle oder immaterielle Schäden beeinträchtigt hat oder beeinträchtigen kann

Praxisbeispiele für Caritas-Träger:

Situation	Erheblich?	Begründung
Ransomware verschlüsselt KIS (Krankenhausinformationssystem)	**JA**	Schwerwiegende Betriebsstörung, Patientengefährdung
Datenexfiltration von Patienten-/Klientendaten	**JA**	Erheblicher immaterieller Schaden für Betroffene
Ausfall der Pflegedokumentation für >4 Stunden	**JA**	Betriebsstörung, potenzielle Versorgungsgefährdung
Phishing-Mail an Mitarbeiter, keine Kompromittierung	Nein	Kein Schaden eingetreten oder zu erwarten
Kompromittierung eines VPN-Zugangs mit Zugriff auf Kernsysteme	**JA**	Potenzielle schwerwiegende Auswirkungen
Fehlgeschlagener Angriff, automatisch abgewehrt	Nein	Kein erheblicher Schaden, aber ggf. als "Beinahevorfall" intern dokumentieren

12.2.3 Wo und wie melden?

Nach Registrierung im BSI-Portal: - Melden Sie sich unter https://portal.bsi.bund.de an - Klicken Sie auf die rote Schaltfläche **"Sicherheitsvorfall melden"** - Füllen Sie das Formular aus (siehe unten)

Vor Abschluss der BSI-Portal-Registrierung: - Nutzen Sie das Online-Formular für Meldungen ohne Registrierung: https://mip2.bsi.bund.de/de/meldungen/meldung-ohne-registrierung-erstellen/?meldestelle=10&formular=32

Parallel ggf. erforderlich: - **Datenschutzmeldung an die Aufsichtsbehörde** (Art. 33 DSGVO), wenn personenbezogene Daten betroffen sind — Frist: ebenfalls 72 Stunden - **Information der Betroffenen** (Art. 34 DSGVO), wenn hohes Risiko für Betroffene besteht - Bei KRITIS-Einrichtungen: **Unterrichtung der Dienstempfänger**, wenn der Vorfall deren Dienste beeinträchtigen kann

Was das Meldeformular im BSI-Portal abfragt:

1. **Vorfallklassifikation:** Erheblicher Sicherheitsvorfall / Sicherheitsvorfall / Beinahevorfall
2. **Beschreibung:** Freitext zu Störung, Auswirkung, Dauer, Ursache
3. **Schweregrad** (Farbschema):
   - 🔴 Rot: Vollständiger Ausfall
   - 🟠 Orange: Beeinträchtigung
   - 🟡 Gelb: Anomalie ohne unmittelbare Auswirkung
   - ⚪ Grau: Keine Anomalie feststellbar
4. **Zeitverlauf:** Wann aufgetreten, ob andauernd, wann entdeckt
5. **Geografische Auswirkung:** Grenzüberschreitend? Betroffene Länder?
6. **Ursachenbewertung:** Böswillige Absicht? Unter Kontrolle? Externe Dienstleister eingebunden?
7. **Gegenmaßnahmen:** Technische und organisatorische Maßnahmen
8. **Kontakt:** Name, Telefon, E-Mail der meldenden Person (muss für BSI-Rückfragen erreichbar sein)

> ***BSI-Anleitung zur Vorfallmeldung (Schritt-für-Schritt):***
> https://www.bsi.bund.de/DE/Themen/Regulierte-Wirtschaft/NIS-2-regulierte-Unternehmen/NIS-2-Anleitung-Meldung/Anleitung-Meldung_node.html

12.2.4 Praxistipp: Meldeprozess intern vorbereiten

Damit die Fristen eingehalten werden können, muss der Meldeprozess **vor dem Vorfall** etabliert sein:

Empfohlene Sofortmaßnahmen:

1. **Meldeweg-Dokument erstellen:** Wer meldet was wann an wen?
2. **BSI-Portal-Zugänge einrichten:** Mindestens 2 Personen mit Zugang
3. **Notfall-Kontaktliste:** IT-Leitung, ISB, Geschäftsführung, externer IT-Dienstleister, Datenschutzbeauftragter — mit privaten Mobilnummern für Wochenenden
4. **Vorausgefüllte Meldeformulare:** Basisdaten der Organisation vorhalten
5. **Vertretungsregelungen:** Was passiert nachts, am Wochenende, im Urlaub?
6. **Übungen:** Mindestens einmal jährlich den Meldeprozess durchspielen (Tabletop Exercise)

12.3 Geschäftsleitungsschulung: Pflicht, nicht Kür

12.3.1 Gesetzliche Grundlage

§38 Abs. 3 BSIG verpflichtet Geschäftsleitungen zur **regelmäßigen Teilnahme an Schulungen** (Empfehlung: alle 2-3 Jahre) zu Informationssicherheit und Risikomanagement. Dies gilt für **alle natürlichen Personen**, die nach Gesetz, Satzung oder Gesellschaftsvertrag zur Führung und Vertretung berechtigt sind — also:

- Geschäftsführer/innen (GmbH, gGmbH)
- Vorstände (e. V., Stiftung)
- Geschäftsführende Gesellschafter
- Alle Mitglieder der Geschäftsleitung

12.3.2 Was die Schulung umfassen muss

Das BSI hat eine **Handreichung für Geschäftsleitungsschulungen** veröffentlicht, die Mindestinhalte definiert:

Vorbereitende Inhalte: - NIS-2-Regulierungskontext: Warum gibt es dieses Gesetz? - Betroffenheitsanalyse: Warum fällt unsere Organisation darunter?

Kerninhalte: - Pflichten der Geschäftsleitung nach §38 BSIG - Die 10 Risikomanagementmaßnahmen nach §30 BSIG - Melde- und Unterrichtungspflichten (§32 BSIG) - Registrierungspflicht (§33 BSIG) - Haftungsrisiken bei Pflichtverletzung - Aktuelle Bedrohungslage und branchenspezifische Risiken

Ergänzende Inhalte: - Branchenspezifische Standards (z.B. B3S Krankenhaus) - Zusammenspiel mit DSGVO und anderen Regulierungen - Praxisbeispiele (z.B. der Ransomware-Angriff auf die Caritas München 2022)

> ***BSI-Handreichung zur Geschäftsleitungsschulung (PDF):***
> https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/NIS-2/nis-2-geschaeftsleitungsschulung.pdf

12.3.3 Haftungsrisiken — warum man das ernst nehmen muss

Die persönliche Geschäftsleiterhaftung ist eine der schärfsten Regelungen der NIS-2:

- **Persönliche Haftung** mit dem Privatvermögen für schuldhaft verursachte Schäden (§38 Abs. 2 BSIG i.V.m. §43 GmbHG)
- Haftung bei **Vorsatz UND Fahrlässigkeit** — auch leichte Fahrlässigkeit genügt (nach §43 GmbHG)
- **Beweislastumkehr**: Der Geschäftsführer muss nachweisen, dass er pflichtgemäß gehandelt hat (§93 Abs. 2 S. 2 AktG analog / §43 Abs. 2 GmbHG nach h.M.)
- **Verzicht auf Schadensersatzansprüche nur eingeschränkt möglich**: Das im Regierungsentwurf vorgesehene absolute Verzichtsverbot wurde im Gesetzgebungsverfahren gestrichen. Es gelten die allgemeinen Regeln: Bei der gGmbH ist ein Verzicht nach §43 Abs. 3 S. 2 GmbHG erst nach 3 Jahren möglich und nur, wenn die Gesellschafter zustimmen und keine Gläubigerbenachteiligung vorliegt. In der Praxis bleibt die Haftung damit sehr scharf.
- **D&O-Versicherung** deckt nur bedingt — bei Vorsatz oder grober Fahrlässigkeit greift sie nicht

> ***Praxistipp für Caritas-Träger:*** *Dokumentieren Sie die Teilnahme an der Schulung mit Zertifikat, Datum und Inhaltsbeschreibung. Im Haftungsfall ist die Dokumentation Ihr wichtigstes Verteidigungsinstrument.*

12.3.4 Wo kann man sich schulen lassen? Beispiele

Anbieter	Format	Dauer	Kosten	Link
IHK Akademie München — ISB/ISO (IHK)	Präsenz / Online	5 Tage	2.350 EUR	ihk-akademie-muenchen.de
IHK Akademie München — Cyber Security Advisor	Live Online	~100 Stunden	2.490 EUR	ihk-akademie-muenchen.de
IHK Mittelfranken — NIS-2-Beauftragter	Präsenz (Nürnberg)	3 Tage	1.600 EUR	ihk-akademie-mittelfranken.de
BIHK Webinar-Reihe IT-Sicherheit	Online (kostenlos!)	Je 60-90 Min.	Kostenlos	bihk.de/itsicherheit

Anbieter	Format	Dauer	Kosten	Link
TÜV SÜD, TÜV NORD	Präsenz / Online	1-3 Tage	800-2.500 EUR	tuev-sued.de
Externe Berater vor Ort	Inhouse	Individuell	Individuell	Solidaris, Althammer & Kill u.a.

> ***Kostenlose Einstiegsmöglichkeit:*** *Die BIHK-Webinar-Reihe "IT-Sicherheit" (8. Staffel, ab 16.03.2026) behandelt NIS-2-Themen ausführlich — ideal als Erstorientierung für Geschäftsleitungen. Alle vergangenen Webinare sind als PDF und YouTube-Video verfügbar.*

12.4 IT-Sicherheitsbeauftragte/n benennen

12.4.1 Warum ein/e ISB unverzichtbar ist

Obwohl NIS-2 die Rolle eines "IT-Sicherheitsbeauftragten" (ISB) nicht namentlich vorschreibt, ergibt sich aus den umfangreichen Pflichten die **praktische Notwendigkeit** einer dedizierten Stelle. Ohne ISB ist eine systematische NIS-2-Umsetzung nicht realistisch.

12.4.2 Aufgabenprofil

- Aufbau, Betrieb und Weiterentwicklung des ISMS
- Durchführung und Koordination von Risikoanalysen
- Koordination aller Sicherheitsmaßnahmen
- Ansprechperson für BSI und Aufsichtsbehörden
- Regelmäßige Berichterstattung an die Geschäftsführung
- Koordination der Meldepflichten (24h/72h/1 Monat)
- Planung und Überwachung von Schulungsmaßnahmen
- Steuerung interner und externer Audits
- Lieferanten-Sicherheitsbewertungen

12.4.3 Organisatorische Einordnung

- **Direkte Berichtslinie an die Geschäftsführung** — der ISB darf nicht dem IT-Leiter unterstellt sein (Interessenkonflikt: IT-Betrieb vs. IT-Sicherheit)
- **Unabhängig von der IT-Abteilung** — auch wenn eine enge Zusammenarbeit notwendig ist
- **Mindestens 0,5-1,0 VZÄ** als dedizierte Kapazität (je nach Organisationsgröße)
- **Stellvertreterregelung** ist zwingend erforderlich (s. Meldepflichten)

12.4.4 Intern oder extern?

Variante	Vorteile	Nachteile	Kosten (ca.)
Interner ISB (eigener Mitarbeiter)	Kennt die Organisation, schnelle Reaktion, dauerhaft präsent	Muss qualifiziert werden, Kapazität gebunden	60.000-90.000 EUR/Jahr (Personalkosten)
Externer ISB (Berater/Dienstleister)	Sofort verfügbar, hohe Expertise, unabhängig	Weniger Organisationskenntnis, begrenzte Verfügbarkeit	30.000-60.000 EUR/Jahr (Rahmenvertrag)
Kombination (intern + externe Unterstützung)	Best of both worlds	Höhere Gesamtkosten	80.000-120.000 EUR/Jahr

Empfehlung für Caritas-Träger: Für die Einführungsphase empfiehlt sich eine **Kombination**: Ein/e interne/r Mitarbeiter/in wird zum ISB weiterqualifiziert (z.B. über die IHK-Zertifizierung, 5 Tage) und erhält in den ersten 12-18 Monaten **externe Beratungsunterstützung** für den ISMS-Aufbau.

12.5 ISMS-Aufbau: Welches Framework wählen?

12.5.1 Die drei relevanten Optionen

Für die Umsetzung der NIS-2-Anforderungen brauchen Sie ein **Informationssicherheits-Managementsystem (ISMS)**. Drei Frameworks sind für Caritas-Träger relevant:

Kriterium	ISO/IEC 27001	BSI IT-Grundschutz	CISIS12
Ansatz	Flexibel, risikobasiert	Strukturiert, maßnahmenbasiert	12 konkrete Schritte
Dokumentationsumfang	Ca. 100 Seiten Norm	Über 350 Seiten Kataloge	Reduziert, 12-Schritte-Modell
Internationale Anerkennung	Hoch (weltweit)	Primär Deutschland	Primär Deutschland
Zertifizierung durch	Akkreditierte Auditoren (TÜV, DQS etc.)	BSI selbst	IT-Sicherheitscluster e. V.
Implementierungsaufwand	Mittel bis hoch	Hoch	Gering bis mittel
Kosten Zertifizierung	10.000-50.000 EUR	Höher	Niedriger
Geeignet für	Mittlere bis große Organisationen	Behördennahe Orgs., KRITIS	KMU, Einstiegsorganisationen

12.5.2 Empfehlung nach Trägergröße

Große Caritas-Träger (Diözesanverbände, große Krankenhausträger, >250 MA): → **ISO 27001** oder "ISO 27001 auf Basis von IT-Grundschutz" (Kombination beider Ansätze)

Mittlere Caritas-Träger (50-250 Mitarbeiter, einzelne Krankenhäuser, größere Komplexträger): → **ISO 27001** — flexibler, kostengünstiger, international anerkannt

Kleinere Einrichtungen (als Einstieg, indirekt betroffene Träger): → **CISIS12** (https://cisis12.de/) — speziell für KMU und Kommunen entwickelt, 12 konkrete Schritte, niedrigere Kosten, vom IT-Planungsrat empfohlen

Wenn KRITIS-Relevanz besteht (Krankenhäuser mit ≥30.000 vollstationären Fällen/Jahr): → **BSI IT-Grundschutz** in Verbindung mit dem **B3S Krankenhaus** (branchenspezifischer Sicherheitsstandard der DKG)

12.5.3 Typischer Zeitplan ISO 27001

Phase	Dauer	Aktivitäten
1. Projektstart & Scoping	1-2 Monate	Managemententscheidung, Scope-Definition, Gap-Analyse, Projektplan, Budgetfreigabe
2. Risikobewertung	1-3 Monate	Asset-Inventar erstellen, Bedrohungsanalyse, Risikobehandlungsplan
3. ISMS-Dokumentation	2-4 Monate	Policies erstellen, Verfahren dokumentieren, Statement of Applicability (SoA)
4. Implementierung	3-6 Monate	Technische und organisatorische Maßnahmen umsetzen, Schulungen durchführen

Phase	Dauer	Aktivitäten
5. Internes Audit	1 Monat	Internes Audit, Management Review, Korrekturmaßnahmen
6. Zertifizierungsaudit	1-2 Monate	Stage 1 (Dokumentenprüfung), Stage 2 (Vor-Ort-Audit)
Gesamt	**9-18 Monate**	

12.5.4 Kostenrahmen ISMS-Aufbau und Zertifizierung

Kostenkategorie	Kleine Org. (50-100 MA)	Mittlere Org. (100-500 MA)	Große Org. (500+ MA)
Beratung/Vorbereitung	15.000-30.000 EUR	40.000-80.000 EUR	80.000-150.000+ EUR
Zertifizierungsaudit	6.000-14.000 EUR	15.000-30.000 EUR	30.000-50.000 EUR
Jährliche Überwachungsaudits	4.000-8.000 EUR	8.000-15.000 EUR	15.000-25.000 EUR
Rezertifizierung (alle 3 Jahre)	~70% des Erstaudits	~70% des Erstaudits	~70% des Erstaudits
ISMS-Tools (Software)	3.000-10.000 EUR/Jahr	10.000-30.000 EUR/Jahr	30.000-60.000 EUR/Jahr
Gesamt Erstjahr	**25.000-55.000 EUR**	**65.000-130.000 EUR**	**140.000-250.000+ EUR**

12.6 Der 90-Tage-Fahrplan: Erste konkrete Schritte

Phase 1: Tage 1-30 — Grundlagen und Analyse

Nr.	Maßnahme	Verantwortlich	Ergebnis
1	**Betroffenheitsanalyse** dokumentieren: Entscheidung "Wir fallen unter NIS-2" schriftlich fixieren, Einstufung als bwE oder wE	Geschäftsführung + Rechtsabteilung	Dokumentierte Einstufung
2	**BSI-Registrierung** abschließen: MUK einrichten → BSI-Portal registrieren (Frist 06.03.2026!)	IT-Leitung	Registrierung bestätigt
3	**Geschäftsleitungsschulung** terminieren und buchen	Geschäftsführung	Schulungstermin steht
4	**ISB benennen** (intern oder extern), Stellenbeschreibung und Berichtslinie festlegen	Geschäftsführung	ISB benannt, Stellenprofil dokumentiert
5	**Quick-Wins umsetzen:** MFA für Admin-Konten und VPN sofort aktivieren	IT-Abteilung	MFA aktiv für kritische Zugänge
6	**IT-Asset-Bestandsaufnahme** starten: Alle Systeme, Server, Anwendungen, Cloud-Dienste erfassen	IT-Abteilung	Erste Asset-Liste (80% Vollständigkeit)
7	**Meldeprozess etablieren:** Notfall-Kontaktliste, Meldeweg-Dokument, BSI-Portal-Zugänge für 2 Personen	ISB	Meldeprozess-Dokument erstellt

Phase 2: Tage 31-60 — Strukturaufbau

Nr.	Maßnahme	Verantwortlich	Ergebnis
8	**Gap-Analyse** durchführen: Ist-Zustand vs. §30 BSIG systematisch abgleichen	ISB + ggf. externer Berater	Gap-Report mit priorisiertem Maßnahmenplan
9	**Risikoanalyse** starten: Kritische Assets und Prozesse identifizieren und bewerten	ISB + Fachbereiche	Erste Risikobewertungsmatrix
10	**ISMS-Framework** entscheiden: ISO 27001 vs. IT-Grundschutz vs. CISIS12	Geschäftsführung + ISB	Entscheidung dokumentiert
11	**Informationssicherheitsleitlinie** erstellen und von Geschäftsleitung verabschieden	ISB + Geschäftsleitung	Verabschiedete Leitlinie (1-3 Seiten)
12	**Backup-Situation** auditieren: 3-2-1-Regel? Restore-Tests? Offline-Backups?	IT-Abteilung	Backup-Statusbericht mit Handlungsbedarf
13	**Incident-Response-Plan** erstellen (Entwurf): Eskalationsstufen, Rollen, Kommunikationswege	ISB + IT-Abteilung	IRP-Entwurf
14	**Lieferantenverzeichnis** erstellen: Alle IT-Dienstleister, Cloud-Anbieter, Softwarelieferanten erfassen	IT + Einkauf	Lieferantenliste mit Kritikalitätsbewertung

Phase 3: Tage 61-90 — Implementierung beginnen

Nr.	Maßnahme	Verantwortlich	Ergebnis
15	**Geschäftsleitungsschulung** durchführen	Externer Anbieter / IHK	Schulungsnachweis mit Datum und Inhalten
16	**Security-Awareness-Training** für alle Mitarbeiter starten: Phishing-Erkennung, sichere Passwörter, Meldeweg	ISB + HR	Erste Schulungsrunde dokumentiert
17	**Schwachstellen-Scan** aller von außen erreichbaren Systemen	IT / externer Dienstleister	Schwachstellenbericht mit Prioritäten
18	**Netzwerksegmentierung** planen: Medizintechnik, Verwaltung, Gäste-WLAN trennen	IT-Abteilung	Netzwerkplan mit Sicherheitszonen
19	**Business Impact Analyse (BIA):** Welche Prozesse sind geschäftskritisch? RTO/RPO festlegen	ISB + Fachbereiche	BIA-Ergebnisdokument
20	**Lieferantenverträge** prüfen: Cybersicherheitsklauseln, Meldepflichten, Audit-Rechte ergänzen	ISB + Rechtsabteilung	Muster-Vertragsklauseln erstellt
21	**12-Monats-Roadmap** erstellen: Detaillierter ISMS-Projektplan mit Meilensteinen und Verantwortlichkeiten	ISB	Projektplan freigegeben

12.7 Die 10 Pflichtmaßnahmen nach §30 BSIG — Praxisnahe Umsetzungshinweise

§30 Abs. 2 BSIG definiert **zehn Mindestmaßnahmen**, die alle betroffenen Einrichtungen umsetzen müssen. Das BSI hat dazu die Informationsreihe **#nis2know** veröffentlicht — hervorragende, kostenlose Praxishandreichungen zu jedem einzelnen Thema.

> ***Alle #nis2know-Infopakete auf einen Blick:*** https://www.bsi.bund.de/dok/nis-2-infopakete

Maßnahme 1: Risikoanalyse und Sicherheitskonzepte

Was zu tun ist: - Systematische Erfassung aller Assets (IT-Systeme, Daten, Prozesse) - Bedrohungen und Schwachstellen für jedes Asset identifizieren - Risikomatrix erstellen: Eintrittswahrscheinlichkeit × Schadenshöhe - Risikobehandlungsplan: Für jedes Risiko — Vermeiden, Vermindern, Übertragen oder Akzeptieren - Informationssicherheitsleitlinie: Vom Management verabschiedetes Grundsatzdokument - Mindestens jährliche Überprüfung, bei wesentlichen Änderungen sofort

Methoden: ISO 27005, BSI-Standard 200-3 (Risikoanalyse)

> ***BSI-Infopaket:*** NIS-2 Risikoanalyse

Maßnahme 2: Bewältigung von Sicherheitsvorfällen

Was zu tun ist: - **Incident-Response-Plan (IRP):** Vordefiniertes Drehbuch mit Eskalationsstufen - **Erkennungsfähigkeit aufbauen:** Zentrale Log-Sammlung (SIEM), Endpunkt-Überwachung (EDR/XDR), Netzwerk-Anomalieerkennung (IDS/IPS) - **Incident-Response-Team:** Rollen definieren, Erreichbarkeit sicherstellen - **Forensische Fähigkeiten:** Intern oder per Rahmenvertrag mit externem Dienstleister - **Kommunikationsplan:** Interne/externe Kommunikation, Abstimmung mit BSI-Meldepflichten - **Post-Incident-Review:** Lessons Learned, Maßnahmenanpassung

Praxistipp für kleinere Träger: Ein vollständiges SIEM ist für Organisationen mit 50-100 MA oft zu aufwändig. Starten Sie mit zentraler Log-Sammlung (z.B. Wazuh als Open-Source-Lösung) und erwägen Sie einen Managed-SIEM-Service über einen Dienstleister.

> ***BSI-Infopaket:*** NIS-2 Meldepflicht

Maßnahme 3: Business Continuity und Krisenmanagement

Was zu tun ist: - **Business Impact Analyse (BIA):** Geschäftskritische Prozesse identifizieren, RTO/RPO festlegen - **Business Continuity Plan (BCP):** Notfallplan für Aufrechterhaltung kritischer Dienste - **Disaster Recovery Plan (DRP):** Technischer Wiederherstellungsplan - **Backup-Konzept nach der 3-2-1-Regel:** - **3** Kopien der Daten - Auf **2** verschiedenen Medientypen - Davon **1** offsite/offline (gegen Ransomware!) - Verschlüsselte Backups - Regelmäßige Restore-Tests (mindestens quartalsweise, dokumentiert!) - Immutable Backups (unveränderbar für definierten Zeitraum) - **Krisenmanagement:** Krisenstab definieren, Kommunikationsketten, Entscheidungsbefugnisse - **Jährliche Notfallübungen:** Tabletop Exercises

Standard-Referenz: BSI-Standard 200-4 (Business Continuity Management), ISO 22301

> ***BSI-Infopaket:*** NIS-2 BCM

Maßnahme 4: Sicherheit der Lieferkette

Was zu tun ist: - Vollständiges **Lieferantenverzeichnis** aller IT-Dienstleister und -Zulieferer - **Risikobewertung** je Lieferant: Kritikalität, Abhängigkeit, Ersetzbarkeit - **Vertragliche Vereinbarungen** müssen enthalten: - Cybersicherheitsanforderungen an den Anbieter - Pflicht zur Meldung von Sicherheitsvorfällen - Audit-Rechte / Nachweispflichten - SLA-Definitionen für Sicherheitsaspekte - Anforderungen an Personalqualifikation - **Diversifizierung:** Keine Single Points of Failure - Mindestens jährliche Review der Lieferantenbewertung

Besonders wichtig für Caritas-Träger: Auch wenn Ihre Pflegeeinrichtung selbst nicht unter NIS-2 fällt — wenn Ihr IT-Dienstleister (z.B. SoCura) unter NIS-2 fällt, werden Sie über dessen Lieferketten-Anforderungen indirekt verpflichtet.

> ***BSI-Infopaket:*** NIS-2 Sichere Lieferkette

Maßnahme 5: Sicherheit bei Beschaffung, Entwicklung und Wartung / Schwachstellenmanagement

Was zu tun ist: - **Schwachstellen-Scanning:** Regelmäßig (mindestens monatlich) alle Systeme auf bekannte CVEs prüfen - **Patch-Management-Prozess:** - Kritische Patches: Innerhalb von **72 Stunden** - Hohe Patches: Innerhalb von **2 Wochen** - Mittlere Patches: Innerhalb von **30 Tagen** - **Netzwerksegmentierung:** Trennung kritischer Netzbereiche (Medizintechnik, Verwaltung, Gäste-WLAN) - **Restriktive Firewall-Regelwerke** mit regelmäßiger Überprüfung

> ***BSI-Infopaket:*** NIS-2 Sicherheitsmaßnahmen und Schwachstellenmanagement

Maßnahme 6: Bewertung der Wirksamkeit

Was zu tun ist: - **Interne Audits:** Mindestens jährlich - **Penetrationstests:** Jährlich durch externe Dienstleister - **KPI-Tracking:** Patchstand, Schulungsquote, Mean Time to Detect/Respond, Anzahl offener Risiken - **Management Reviews:** Quartalsbericht an Geschäftsführung - **Kontinuierlicher Verbesserungsprozess:** PDCA-Zyklus (Plan-Do-Check-Act)

Maßnahme 7: Schulungen und Sensibilisierung (Cyberhygiene)

Was zu tun ist: - **Alle Mitarbeiter** mit IT-Zugang: Security-Awareness-Training (jährlich) - **Geschäftsführung:** NIS-2-spezifische Schulung (alle 2-3 Jahre („regelmäßig"), s. Kapitel 12.3) - **IT-Personal:** Fachspezifische Sicherheitsschulungen - **Schulungsinhalte:** Phishing-Erkennung (inkl. Simulationen), sichere Passwortnutzung, Social-Engineering-Abwehr, Umgang mit mobilen Geräten, Meldewege bei Verdachtsfällen, Clean-Desk-Policy - **Dokumentation:** Durchführung und Wirksamkeit müssen nachweisbar sein

> ***BSI-Infopaket:*** NIS-2 Schulungen und Sensibilisierung

Maßnahme 8: Kryptographie und Verschlüsselung

Was zu tun ist: - **Data at Rest:** Festplattenverschlüsselung (BitLocker, FileVault), Datenbank- und Backup-Verschlüsselung - **Data in Motion:** TLS 1.2+ für alle Webanwendungen, VPN für Remote-Zugriffe, E-Mail-Verschlüsselung für sensible Kommunikation - **Schlüsselmanagement:** Sichere Erzeugung, Speicherung, Verteilung und Vernichtung von Schlüsseln - **Mindeststandards:** AES-256, RSA 2048+, SHA-256+ — veraltete Algorithmen (MD5, SHA-1, DES) sind nicht akzeptabel

BSI-Technische Richtlinien: TR-02102-1 (Kryptographische Verfahren), TR-02102-2 (TLS)

Maßnahme 9: Personalsicherheit, Zugangskontrolle, Asset-Management

Was zu tun ist: - **Rollenbasierte Zugriffskontrolle (RBAC):** Need-to-know-Prinzip konsequent umsetzen - **Privileged Access Management (PAM):** Besondere Absicherung administrativer Konten - **Regelmäßige Zugriffsrechte-Reviews:** Mindestens halbjährlich - **Onboarding/Offboarding-Prozess:** Sofortige Deaktivierung bei Austritt - **Vollständiges IT-Asset-Inventar:** Hardware, Software, Lizenzen, Cloud-Dienste - **Klassifikation:** Kritikalität und Schutzbedarf für jedes Asset - **Personalsicherheit:** Führungszeugnisse bei sensitiven Positionen, Vertraulichkeitsvereinbarungen

> *BSI-Infopaket:* NIS-2 Personalsicherheit, Zugriffskontrolle und Asset-Management

Maßnahme 10: Multi-Faktor-Authentifizierung und gesicherte Kommunikation

Was zu tun ist: - **MFA verpflichtend** einführen — Priorisierung: 1. **Sofort:** Administrative Konten, VPN-Zugänge, Cloud-Portale, E-Mail 2. **Kurzfristig:** Alle externen Zugänge, Fachapplikationen mit sensitiven Daten 3. **Mittelfristig:** Alle Benutzerkonten - **MFA-Methoden** (nach Sicherheitsstufe): - FIDO2/WebAuthn (phishing-resistent, empfohlen) - Hardware-Token (YubiKey etc.) - Authenticator Apps (Microsoft Authenticator, Google Authenticator) - SMS-basiert (Minimum, nicht empfohlen für kritische Systeme) - **Gesicherte Kommunikation:** Notfallkommunikationssysteme, verschlüsselte Sprach-/Video-/Textkommunikation

> *BSI-Infopaket:* NIS-2 MFA und gesicherte Kommunikation

12.8 BSI-Ressourcen und Tools — die komplette Übersicht

Das BSI stellt umfangreiche, kostenlose Ressourcen zur Verfügung, die speziell für NIS-2-betroffene Einrichtungen entwickelt wurden:

12.8.1 NIS-2-spezifische Ressourcen

Ressource	Beschreibung	URL
BSI-Portal	Zentrale Plattform für Registrierung und Vorfallsmeldungen	portal.bsi.bund.de
Betroffenheitsprüfung	Kostenloses Online-Tool zur Selbsteinschätzung	betroffenheitspruefung-nis-2.bsi.de
NIS-2 Starterpaket	Einstiegsseite mit allen wichtigen Links und Anleitungen	bsi.bund.de/dok/nis-2-start
“NIS-2 — was tun?”	6-Schritte-Roadmap des BSI	bsi.bund.de/dok/nis-2-was-tun
#nis2know-Infopakete	16+ themenspezifische Handreichungen zu allen Maßnahmen	bsi.bund.de/dok/nis-2-infopakete
Infopaket Gesundheit	Sektorspezifisches Paket für Gesundheitseinrichtungen	BSI Gesundheit
NIS-2 FAQ (allgemein)	Häufig gestellte Fragen	BSI FAQ
NIS-2 FAQ (sektorspezifisch)	FAQ nach Sektoren, inkl. Gesundheitswesen	BSI Sektor-FAQ

Ressource	Beschreibung	URL
Registrierungsanleitung	Schritt-für-Schritt-Anleitung	BSI Registrierung
Meldeanleitung	Schritt-für-Schritt-Anleitung Vorfallsmeldung	BSI Meldung
Geschäftsleitungsschulung	Handreichung für GL-Schulungen	BSI GL-Schulung (PDF)

12.8.2 BSI-Standards (IT-Grundschutz)

Auch wenn Sie nicht den IT-Grundschutz als ISMS-Framework wählen, sind die BSI-Standards wertvolle Methodik-Quellen:

Standard	Titel	NIS-2-Relevanz
BSI-Standard 200-1	Managementsysteme für Informationssicherheit	ISMS-Aufbau, kompatibel mit ISO 27001
BSI-Standard 200-2	IT-Grundschutz-Methodik	Drei Absicherungsstufen: Basis, Kern, Standard
BSI-Standard 200-3	Risikoanalyse auf Basis von IT-Grundschutz	Risikoanalyse-Verfahren (Maßnahme 1 & 6)
BSI-Standard 200-4	Business Continuity Management	BCM-Leitfaden (Maßnahme 3)

Besonders empfehlenswert: Der "Leitfaden zur Basis-Absicherung nach IT-Grundschutz" richtet sich speziell an **KMU und kleinere Organisationen** und ist ein idealer Einstieg.

BSI-Standards Übersicht: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/BSI-Standards/bsi-standards_node.html

12.8.3 BSI-Kontakt

Kanal	Details
BSI Service-Center	service-center@bsi.bund.de
Telefon	+49 228 99 9582-0
Adresse	Godesberger Allee 87, 53175 Bonn

12.9 IHK-Ressourcen: Praxishilfen, Schulungen und Beratung

Die Industrie- und Handelskammern bieten umfangreiche, praxisnahe Unterstützung für NIS-2 — viele Angebote sind sogar **kostenlos**.

12.9.1 Beispiel: IHK für München und Oberbayern

Ressource	Beschreibung	URL
NIS-2/KRITIS-Infoseite	Zentrale NIS-2-Informationsseite	ihk-muenchen.de NIS-2
IT-Notfallplan-Vorlage	Kostenlose Excel-Vorlagen (Dokumentenliste + Benutzer-Notfallplan)	ihk-muenchen.de Notfallplan
IT-Notfallplan für KMU	Vereinfachte Vorlage für Kleinstunternehmen	ihk-muenchen.de KMU

Ressource	Beschreibung	URL
IT-Sicherheits-Checkliste	“Stand der IT-Sicherheit ermitteln & verbessern”	ihk-muenchen.de Checkliste
Checkliste externe Beratung	Hilfe bei der Auswahl externer IT-Sicherheitsberater	ihk-muenchen.de Beratung
Positionspapier IT-Sicherheit	IHK-Vollversammlungs-Beschluss November 2024	ihk-muenchen.de Position
Kontakt: Bernhard Kux	Referent Cybersicherheit, Tel. +49 89 5116-1705	IHK München, Orleansstr. 10-12, 81669 München

12.9.2 BIHK Webinar-Reihe IT-Sicherheit (kostenlos!)

Die Bayerischen IHKs führen gemeinsam mit dem Bayerischen Staatsministerium für Digitales eine **kostenlose Webinar-Reihe** zu IT-Sicherheit und NIS-2 durch — mittlerweile in der 8. Staffel.

Website: https://www.bihk.de/itsicherheit

Ausgewählte NIS-2-relevante Termine 2026 (8. Staffel):

Datum	Thema	Referent/in
24.03.2026	NIS-2: Die Geschäftsleitung als Owner der Cyber Resilience	Marion Schultz
19.05.2026	NIS-2 Business Continuity: BIA, BCM, Notfallmanagement	Alexander Karls (Pegasus GmbH)
Termin folgt	NIS-2-Anforderungen für Lieferketten	Thorsten Krause (Rechtsanwalt)
Termin folgt	IT-Krisenmanagement: “Der Tag, an dem alles stillsteht”	Matthias Hofmann

Bereits verfügbare Aufzeichnungen (7. Staffel, 2025): - 24.06.2025: NIS-2 Comprehension & Rollout — YouTube-Video - 16.10.2025: NIS-2-Umsetzung für KMU — PDF-Unterlagen - 25.11.2025: Risikomanagement-Grundlagen — YouTube-Video

Besonders relevant für Caritas-Träger: In der 5. Staffel (22.10.2024) berichtete **Thomas Schwarz von der Caritas München-Freising** über den Ransomware-Angriff im September 2022 — ein eindrückliches Praxisbeispiel aus dem eigenen Verband. Videos und PDFs sind verfügbar.

12.9.3 IHK-Zertifizierungskurse

Kurs	Format	Dauer	Kosten	Nächste Termine
ISB/ISO (IHK) — Informationssicherheitsbeauftragte/r	Präsenz + Online	5 Tage	2.350 EUR	16.03.2026 (Ingolstadt), 22.06.2026 (Online), 14.09.2026 (Mühldorf)
Cyber Security Advisor (IHK)	Live Online	~100 Std.	2.490 EUR	Ab 01.09.2026

Kurs	Format	Dauer	Kosten	Nächste Termine
NIS-2-Beauftragter (IHK Mittelfranken)	Präsenz (Nürnberg)	3 Tage	1.600 EUR	27.-29.07.2026
Update-Seminar für ISB	München / Online	1 Tag	ab 520 EUR	Laufend

Links: - ISB/ISO IHK Akademie München - Cyber Security Advisor IHK - NIS-2-Beauftragter IHK Mittelfranken

12.9.4 CyberSicherheitsCheck für KMU

Die IHKs bieten einen **kostenlosen 60-minütigen IT-Sicherheitscheck** an — durchgeführt von digiZ-Beratern mit detaillierter Checkliste. Ergebnis ist eine visuelle Bewertung mit konkreten Optimierungsempfehlungen. Ein niedrigschwelliger Einstieg, besonders für kleinere Caritas-Einrichtungen.

12.10 Externe Unterstützung: Berater, Dienstleister, Netzwerke

12.10.1 BSI-zertifizierte IT-Sicherheitsdienstleister

Das BSI führt eine Liste zertifizierter IS-Revisions-Dienstleister. Diese haben ein anspruchsvolles Zertifizierungsverfahren durchlaufen und sind für besonders sensible Prüfungen qualifiziert:

BSI-Liste IT-Sicherheitsdienstleister

12.10.2 Spezialisierte Berater für Sozialwirtschaft

Berater	Spezialisierung	Website
Solidaris	Prüfungsgesellschaft mit Schwerpunkt Gesundheits-/Sozialwesen	solidaris.de
Althammer & Kill	Datenschutz und IT-Sicherheit im Gesundheits-/Sozialwesen	althammer-kill.de
SoCura GmbH	IT-Dienstleister für Wohlfahrt, Kirche, Gesundheitswesen; ISO-27001-zertifiziert	socura.de

12.10.3 Kostenlose Unterstützungsangebote

Angebot	Beschreibung	URL
Transferstelle Cybersicherheit im Mittelstand	Zentrales BMWi-Projekt, kostenlose Workshops, Leitfäden, Veranstaltungen	transferstelle-cybersicherheit.de
BSI CyberRisikoCheck (DIN SPEC 27076)	Standardisierter Sicherheitscheck für KMU, 1 Beratertag, staatlich förderfähig	BSI CyberRisikoCheck
Allianz für Cyber-Sicherheit (ACS)	BSI-Initiative, ~9.000 Mitglieder, kostenlose Mitgliedschaft, Informationsaustausch	allianz-fuer-cybersicherheit.de

Angebot	Beschreibung	URL
FINSOZ Orientierungshilfe	"NIS-2 für Sozialwirtschaft und kirchliche Organisationen" — kostenloser Download	finsoz-akademie.de
IHK CyberSicherheitsCheck	Kostenloser 60-Minuten-Check durch digiZ-Berater	Über lokale IHK

12.10.4 Branchenspezifischer Sicherheitsstandard: B3S Krankenhaus

Für Caritas-Krankenhäuser ist der **B3S "Medizinische Versorgung"** der Deutschen Krankenhausgesellschaft (DKG) besonders relevant:

- **Aktuelle Version:** 1.3 (vom BSI auf Eignung geprüft, gültig bis November 2028)
- **Umfang:** 168 Maßnahmen zur Sicherstellung resilienter IT
- **Schutzziele:** Neben IT-Schutz auch **Patientensicherheit und Behandlungseffektivität**
- **Kostenlos** auf der DKG-Website herunterladbar
- **Geltungsbereich:** Primär KRITIS-Krankenhäuser (≥30.000 vollstationäre Fälle/Jahr), aber auch für kleinere Häuser als Orientierung empfohlen

Download: DKG B3S Informationssicherheit im Krankenhaus

12.11 Pflichtdokumentation: Was Sie bereithalten müssen

NIS-2 ist eine **Nachweisaufgabe** — im Prüffall müssen Sie belegen können, dass Sie die Anforderungen umsetzen. Hier die vollständige Liste der Pflichtdokumente:

Nr.	Dokument	Beschreibung	Verantwortlich
1	**Informationssicherheitslinie**	Von GL verabschiedetes Grundsatzdokument (1-3 Seiten)	ISB + GL
2	**Risikoanalyse**	Systematische Bewertung aller IT-Risiken	ISB
3	**Risikobehandlungsplan**	Maßnahmen zu jedem identifizierten Risiko	ISB
4	**Statement of Applicability (SoA)**	Erklärung zur Anwendbarkeit aller Maßnahmen	ISB
5	**IT-Asset-Inventar**	Alle Systeme mit Klassifikation und Schutzbedarf	IT + ISB
6	**Incident-Response-Plan**	Eskalationsstufen, Rollen, Kommunikationswege, Meldefristen	ISB
7	**Business Continuity Plan**	Notfallplan für kritische Dienste	ISB + Fachbereiche

Nr.	Dokument	Beschreibung	Verantwortlich
8	**Disaster Recovery Plan**	Technischer Wiederherstellungsplan	IT
9	**Backup-Konzept**	3-2-1-Regel, Restore-Test-Protokolle	IT
10	**Lieferantenverzeichnis**	Alle IT-Dienstleister mit Kritikalitätsbewertung	IT + Einkauf
11	**Lieferantenverträge**	Mit Cybersicherheitsklauseln, Meldepflichten, Audit-Rechten	Recht + ISB
12	**Zugriffsrechte-Dokumentation**	Wer hat Zugriff auf was, wann zuletzt überprüft	IT
13	**Schulungsnachweise**	Alle Mitarbeiter + Geschäftsleitung, Datum, Inhalte	HR + ISB
14	**Audit-Berichte**	Interne/externe Audit-Ergebnisse und Korrekturmaßnahmen	ISB
15	**Maßnahmenplan**	Priorisierter Plan mit Verantwortlichkeiten und Terminen	ISB
16	**Kryptographie-Konzept**	Verwendete Verfahren, Schlüsselmanagement	IT + ISB
17	**Netzwerkplan**	Mit Sicherheitszonen und Segmentierung	IT
18	**Meldeprozess-Dokument**	Wer meldet was wann an wen (inkl. BSI, DSGVO)	ISB

12.12 Nachweispflichten und Audits

Wer wird geprüft?

Einrichtungstyp	Nachweispflicht	Häufigkeit
Betreiber kritischer Anlagen (KRITIS)	Pflichtnachweis durch Audits, Prüfungen oder Zertifizierungen (§39 BSIG)	Alle 3 Jahre
Besonders wichtige Einrichtungen (bwE)	Nachweis auf Anordnung des BSI (§61 BSIG)	Bei Anordnung
Wichtige Einrichtungen (wE)	Prüfung bei begründetem Verdacht (§62 BSIG)	Bei Verdacht

Anerkannte Nachweismethoden

- ISO 27001-Zertifizierung
- BSI IT-Grundschutz-Zertifizierung
- Externe Gutachten / Prüfberichte
- Interne Auditberichte

> ***Wichtig:*** *Es gibt* ***keine offizielle "NIS-2-Zertifizierung"****. Angebote, die mit diesem Begriff werben, sind nicht durch das BSI anerkannt. NIS-2-Konformität wird über bestehende Standards (ISO 27001, BSI IT-Grundschutz) nachgewiesen.*

12.13 Zusammenfassung: Die wichtigsten Sofortmaßnahmen

Wenn Sie als Caritas-Träger unter NIS-2 fallen, sind dies die **absoluten Prioritäten**:

Priorität	Maßnahme	Frist/Empfehlung
🔴 **KRITISCH**	BSI-Registrierung über MUK + BSI-Portal abschließen	Bis 06.03.2026
🔴 **KRITISCH**	Meldeprozess für Sicherheitsvorfälle etablieren (24h/72h/1 Monat)	Sofort
🔴 **KRITISCH**	Geschäftsleitungsschulung planen und terminieren	Innerhalb 30 Tagen
🟠 **HOCH**	IT-Sicherheitsbeauftragte/n benennen	Innerhalb 30 Tagen
🟠 **HOCH**	MFA für administrative Konten und VPN aktivieren	Innerhalb 30 Tagen
🟠 **HOCH**	IT-Asset-Inventar erstellen	Innerhalb 60 Tagen
🟡 **MITTEL**	Gap-Analyse gegen §30 BSIG durchführen	Innerhalb 60 Tagen
🟡 **MITTEL**	ISMS-Framework entscheiden und Projekt starten	Innerhalb 90 Tagen
🟡 **MITTEL**	Backup-Konzept prüfen und härten (3-2-1-Regel, Restore-Tests)	Innerhalb 90 Tagen
🔵 **PLANUNG**	ISMS-Aufbau und Zertifizierung	9-18 Monate

> ***Der wichtigste Rat:*** *Fangen Sie* ***jetzt*** *an. Es gibt keine Übergangsfrist. Die Pflichten gelten seit dem 06.12.2025. Jeder Tag ohne Maßnahmen erhöht das Haftungsrisiko der Geschäftsführung — und das Risiko, Opfer eines Cyberangriffs zu werden, der ohne grundlegende Schutzmaßnahmen weitaus verheerender ausfällt.*

Alle URLs und Informationen wurden im Februar 2026 recherchiert und geprüft. Da sich Webseiten und Angebote ändern können, empfehlen wir die regelmäßige Prüfung der BSI-Informationsseiten unter bsi.bund.de.

13. IT- und Digitalisierungsrefinanzierung: Politischer Druck notwendig

Das hier ist die Meinung des Autors und nicht Teil der Analyse zu NIS-2 – trotzdem ist dieses Thema für die effektive Sicherheit in der Caritas entscheidend, wenn wir langfristig Cybersicherheit ernsthaft und angemessen im Interesse der Hilfebedürftigen & Mitarbeitenden erreichen wollen. Heute und in Zukunft. Das darf als Appell verstanden werden, dass wir uns alle mehr politisch für unsere Interessen gemeinsam einsetzen MÜSSEN.

13.1 Das Grundproblem: Viele Gesetze fordern IT-Sicherheit — keines refinanziert sie

Die Sozialwirtschaft steht vor einem strukturellen Paradoxon: Der Gesetzgeber erlässt immer mehr Vorschriften, die IT-Sicherheit, Datenschutz und Digitalisierung von sozialen Einrichtungen verlangen — aber **kein einziges Gesetz** stellt eine systematische Refinanzierung dieser Anforderungen sicher. Und eine stabile IT-Sicherheit ist **Voraussetzung** für alle Digitalisierungsvorhaben inklusive Innovation & KI-Einsatz.

13.1.1 Die Gesetzeswand: 15+ unfinanzierte IT-Mandate

Ein typischer Caritas-Krankenhausträger (400 Betten, 1.500 Mitarbeiter) unterliegt **gleichzeitig** folgenden IT-Sicherheits- und Datenschutzverpflichtungen:

Nr.	Gesetz / Verordnung	IT-Sicherheitsanforderung	Systematische Refinanzierung?
1	**KDG §26** (Kirchliches Datenschutzgesetz)	Technische und organisatorische Maßnahmen, Überprüfung alle 2 Jahre	**NEIN**
2	**KDG-DVO** (KDG-Durchführungsverordnung)	Drei Datenschutzklassen mit gestaffelten Mindeststandards, MFA-Pflicht	**NEIN**
3	**DSGVO Art. 32**	TOM für staatlich-rechtliche Verarbeitungen	**NEIN**
4	**NIS2-RLUG / BSIG**	Vollumfängliche NIS-2-Compliance	**NEIN**
5	**§391 SGB V**	IT-Sicherheit nach Stand der Technik für **alle** Krankenhäuser, B3S-Ausrichtung	**NEIN** (theoretisch über DRG, praktisch nicht separiert)
6	**§393 SGB V**	C5-Typ-2-zertifizierte Cloud-Dienste für Gesundheitsdaten	**NEIN**
7	**KHZG**	Digitalisierungspflichten (bei Nichterfüllung: 2% Abschlag ab 2026!)	**EINMALIG** (Fonds ausgelaufen), Strafabschlag aber dauerhaft
8	**TI-Anbindung**	Konnektor, eHBA, TI-Gateway, ePA-Anbindung	**TEILWEISE** (TI-Pauschale: ca. 216 EUR/Monat — unzureichend)
9	**DigiG** (Digital-Gesetz)	ePA, E-Rezept, eArztbrief-Infrastruktur	**NEIN**
10	**PDSG** (Patientendaten-Schutz-Gesetz)	IT-Sicherheit für alle Krankenhäuser seit 01.01.2022	**NEIN**

Nr.	Gesetz / Verordnung	IT-Sicherheitsanforderung	Systematische Refinanzierung?
11	**BSI-KritisV** (bei KRITIS-Schwelle)	Zweijährliche Audits, Vorfallsmeldungen	**NEIN** (Auditkosten 50.000-150.000 EUR pro Zyklus)
12	**KRITIS-Dachgesetz** (ab Mitte 2026)	Physische Resilienz, Allgefahren-Risikoanalysen, BCM	**NEIN**
13	**Cyber Resilience Act**	Indirekt: höhere Beschaffungskosten für IT-Produkte	**NEIN** (Kosten werden von Herstellern durchgereicht)
14	**Landeskrankenhausgesetz**	Landesspezifische Datenschutzanforderungen	**NEIN**
15	**KHG-Dualfinanzierung**	IT-Investitionen theoretisch über Länder	**JA, aber strukturell kaputt**: Investitionslücke von **2,64 Mrd. EUR/Jahr**

Ergebnis: Von 15 regulatorischen IT-Mandaten hat genau eines (TI-Pauschale) eine dedizierte, aber völlig unzureichende Refinanzierung. Eines (KHG-Dualfinanzierung) hat einen theoretischen, aber chronisch unterfinanzierten Mechanismus. Die übrigen 13 haben keinerlei eigene Finanzierung.

Für ein **Caritas-Pflegeheim** sieht es nicht besser aus:

Nr.	Gesetz	Refinanzierung?
1	KDG §26 + KDG-DVO	**NEIN**
2	DSGVO Art. 32	**NEIN**
3	TI-Anbindungspflicht (seit 01.07.2025)	Teilweise (TI-Pauschale ca. 223 EUR/Monat)
4	DigiG (ePA-Readiness)	**NEIN**
5	§8 Abs. 8 SGB XI Digitalisierungsförderung	**EINMALIG** 12.000 EUR (bei 50% Eigenanteil)
6	Landesdatenschutzgesetz	**NEIN**
7	CRA (indirekt über höhere Beschaffungskosten)	**NEIN**

> ***Das KDG verdient besondere Beachtung:*** *Als kirchliches Datenschutzgesetz (Rechtsgrundlage: Art. 91 DSGVO) gilt es für **alle** Caritas-Einrichtungen und -Dienste. §26 KDG fordert technische und organisatorische Maßnahmen, die mit Art. 32 DSGVO praktisch identisch sind — mit einem entscheidenden Unterschied: Das KDG verlangt **explizit** eine Wirksamkeitsprüfung **mindestens alle zwei Jahre** (die DSGVO spricht nur von "regelmäßig"). Die neue KDG-DVO (2025) verschärft die Anforderungen weiter: MFA wird explizit gefordert, drei Datenschutzklassen mit gestaffelten Mindeststandards eingeführt, der BSI IT-Grundschutz-Katalog und ISO 27001 als Orientierung referenziert.* ***Für die Erfüllung dieser Pflichten existiert kein einziger Refinanzierungsmechanismus.***

13.1.2 Die Investitionslücke in Zahlen

Die systematische Unterfinanzierung der IT in der Sozialwirtschaft lässt sich beziffern:

Kennzahl	Wert	Quelle
Krankenhaus-Investitionslücke (gesamt)	2,64 Mrd. EUR/Jahr	DKG / Verbandsbuero 2023
IT-Anteil am Krankenhausbudget (Deutschland)	3,0%	DKG / Hochschule Osnabrück (2025)
IT-Anteil am Krankenhausbudget (Niederlande)	5,2%	DKG / Hochschule Osnabrück (2025)
IT-Anteil am Krankenhausbudget (Dänemark)	3,9%	DKG / Hochschule Osnabrück (2025)
Zusätzlicher IT-Investitionsbedarf (nächste 5 Jahre)	ca. 7 Mrd. EUR/Jahr	PwC-Studie
KHZG-Digitalisierungsförderung (einmalig)	4,3 Mrd. EUR (aufgebraucht)	BMG
Digitalisierungsförderung pro Pflegeeinrichtung	max. 12.000 EUR (einmalig!)	§8 Abs. 8 SGB XI
TI-Pauschale für Pflegeeinrichtungen	ca. 223 EUR/Monat	§106b SGB XI / §380 SGB V
Wertverlust der KHG-Investitionsförderung seit 1991	39,5% (inflationsbereinigt)	DKG

> ***Zum Vergleich:*** *Ein einziger Ransomware-Angriff auf eine Caritas-Einrichtung verursacht Schäden im zweistelligen Millionenbereich — der Angriff auf die Caritas München-Freising im September 2022 kostete geschätzt* ***23 Mio. EUR*** *und betraf über 350 Dienste und Einrichtungen. Die Investition in IT-Sicherheit, die diesen Schaden hätte verhindern können, wäre ein Bruchteil davon gewesen — aber sie wurde nie systematisch refinanziert.*

13.2 Das Digitalisierungsparadoxon: Warum das System Innovation bestraft

13.2.1 Eingabeorientierte Refinanzierung als Innovationsbremse

Das fundamentale Problem der Sozialwirtschaft liegt in ihrer **eingabeorientierten Refinanzierungslogik**: Bezahlt wird nicht das Ergebnis der Arbeit, sondern der Einsatz menschlicher Arbeitskraft.

So funktioniert das aktuelle System:

1. **Pflegesatzverhandlungen (§85 SGB XI):** Einrichtungen verhandeln Pflegesätze mit den Pflegekassen auf Basis eines **Stellenplans** — also der Zahl und Qualifikation des eingesetzten Personals
2. **Personalschlüssel / Betreuungsschlüssel:** Feste Verhältnisse wie “1 Pflegefachkraft pro 2,5 Bewohner” bestimmen das Personalbudget
3. **Fachkraftstunden:** Die refinanzierten Mittel sind direkt an die Zahl der geleisteten Fachkraftstunden gekoppelt

4. **Personaluntergrenzen (PpUGV, PPR 2.0):** Seit 2019 gelten in Krankenhäusern Mindest-Pflegepersonalvorgaben

Die zentrale Erkenntnis: In diesem System ist das Budget einer Einrichtung im Wesentlichen **Personalkosten × genehmigte Stellen + Sachkosten + Investitionskosten**. Es gibt keine Budgetlinie für Digitalisierung, keine Pauschale für IT-Sicherheit, keinen Personalschlüssel für IT-Fachkräfte.

13.2.2 Das Innovationsparadoxon in fünf Schritten

Am Beispiel einer KI-gestützten Sprachdokumentation (Voice) lässt sich das Paradoxon präzise zeigen:

Schritt 1 — Ausgangslage: Ein Caritas-Pflegeheim hat 50 VZÄ (Vollzeitäquivalente) Pflegefachkräfte. Der ausgehandelte Pflegesatz basiert auf diesem Stellenplan.

Schritt 2 — KI-Einführung: Die Einrichtung führt einen KI-Sprachassistenten ein (z.B. Voize). Jede Pflegekraft spart 20-30 Minuten pro Schicht bei der Dokumentation. Über die gesamte Einrichtung summiert sich das auf das Äquivalent von ca. 5 VZÄ.

Schritt 3 — Das Paradoxon schlägt zu: - **Option A:** Die Einrichtung behält alle 50 VZÄ. Die Pflegekräfte haben mehr Zeit für direkte Pflege, die Qualität steigt, Burnout sinkt. **ABER:** In der nächsten Pflegesatzverhandlung argumentieren die Pflegekassen, dass die dokumentierten Pflegebedarfe mit weniger Fachkraftstunden gedeckt werden können. Der Stellenplan wird auf 45 VZÄ **gekürzt** — der Pflegesatz entsprechend. - **Option B:** Die Einrichtung reduziert proaktiv auf 45 VZÄ. Die Effizienzgewinne fließen an die Pflegekassen, nicht an die Einrichtung. - **Option C:** Die Einrichtung führt die KI **nicht** ein. Das ist unter den aktuellen Anreizstrukturen das **rationale Verhalten**.

Schritt 4 — Der Sanktionsmechanismus: Nach §115 Abs. 3a SGB XI kann die Pflegevergütung **gekürzt** werden, wenn eine Einrichtung den vereinbarten Personalschlüssel unterschreitet. Im Extremfall droht die Kündigung des Versorgungsvertrags. Das System ist darauf ausgelegt, Personalstärken zu erzwingen — nicht Ergebnisqualität.

Schritt 5 — Die Investitionsfalle: Die KI-Technologie selbst kann ebenfalls nicht refinanziert werden. Es gibt keine "Digitalisierungspauschale" in der Pflegesatzstruktur. Die 12.000 EUR Einmalzuschuss nach §8 Abs. 8 SGB XI decken weder die Lizenzkosten noch den Betrieb.

> ***Das Ergebnis ist ein negativer Rückkopplungskreislauf:*** *Innovation → Effizienz → geringerer Stellenplan → weniger Refinanzierung → Investition kann nicht amortisiert werden → kein Anreiz zur Innovation*

Der Deutsche Pflegerat bringt es auf den Punkt: *"Die Regelungen zur Refinanzierung der Pflegedigitalisierung müssen grundlegend reformiert werden: Investitionen, Betriebskosten, IT-Ressourcen und personelle Aufwendungen müssen verlässlich abgebildet werden."*

13.3 Demografischer Wandel: Warum IT/KI keine Option, sondern Notwendigkeit ist

13.3.1 Der Fachkräftemangel in Zahlen

Der demografische Wandel macht die bisherige Logik "mehr Pflegebedarf = mehr Personal einstellen" schlicht unmöglich:

Kennzahl	Aktuell	2034 (Prognose)	2049 (Prognose)
Unbesetzte Pflegestellen	ca. 30.000	90.000 - 350.000	280.000 - 690.000

Kennzahl	Aktuell	2034 (Prognose)	2049 (Prognose)
Vakanzzeit Altenpflege-Fachkraft	246-286 Tage	steigend	—
Pflegebedürftige	5,7 Mio.	steigend	steigend
Erwerbspersonenpotenzial	sinkend um 400.000/Jahr	—	—

Quellen: Statistisches Bundesamt Pflegekräftevorausberechnung 2024, Bundesagentur für Arbeit Engpassanalyse 2024, Bertelsmann Stiftung Pflegereport 2030

Caritas-spezifisch: - **Jede fünfte Stelle (20%)** bei der Caritas ist unbesetzt — in der Eingliederungshilfe sogar **jede vierte (25%)** - In den kommenden Jahren werden ca. **200.000 Caritas-Mitarbeiter** in den Ruhestand gehen - Das Beschäftigungswachstum in der Pflege wird seit 2022 **ausschließlich durch ausländische Fachkräfte** getragen.

13.3.2 KI und Voice: Die Lösung, die das System nicht refinanziert

Moderne KI-Technologie kann einen substantiellen Teil des Fachkräftemangels kompensieren — wenn man sie lässt.

Das Beispiel Voice-Dokumentation:

Pflegekräfte verbringen **13-36% ihrer Arbeitszeit** mit Dokumentation — je nach Kontext mehr als eine volle Stunde pro Schicht. Bei Ärzten sind es sogar **44%**. Die jährlichen Dokumentationskosten allein in der Pflege belaufen sich auf ca. **2,7 Mrd. EUR**.

KI-Sprachassistenten wie **Voize** (bereits in über 1.100 Einrichtungen mit 75.000 Pflegekräften im Einsatz) ermöglichen es, Pflegedokumentation per Sprache direkt am Bewohner zu diktieren. Die KI wandelt natürliche Sprache in strukturierte, kodierte Dokumentationseinträge um — ohne manuelle Nacharbeit.

Die Evidenz ist eindeutig:

Die **Charité-Voize-Pilotstudie** (14 Pflegeeinrichtungen, 52 Pflegefachkräfte, ca. 770 beobachtete Stunden) — die erste bundesweite deutsche Studie unter Realbedingungen — ergab:

- Durchschnittliche Dokumentationszeit pro Schicht: **von 64 auf 24,81 Minuten** (Reduktion um **61,2%**)
- Konservativere Messung über verschiedene Studienphasen: **27% Reduktion** des Dokumentationsaufwands
- Praktische Zeitersparnis: **20-30 Minuten pro Schicht**

Was bedeutet "10% der Arbeitszeit besser nutzbar"?

Wenn Dokumentation 13-30% der Arbeitszeit ausmacht und KI diese um 27-61% reduziert, ergibt sich eine Netto-Zeitersparnis von **3,5% bis 18,3%** der Gesamtarbeitszeit. Die Aussage, dass **10% der Arbeitszeit** durch Voice-Technologie besser nutzbar werden, liegt damit solide im Mittelfeld der wissenschaftlichen Evidenz.

Konkret: Bei einer 8-Stunden-Schicht sind das **48 Minuten mehr** für direkte Pflege, Zuwendung und fachliche Betreuung — pro Pflegekraft, pro Schicht, jeden Tag.

Auf eine Einrichtung mit 50 Pflegekräften hochgerechnet, entspricht das dem Äquivalent von **ca. 5 Vollzeitstellen** — Stellen, die am Arbeitsmarkt nicht mehr zu besetzen sind.

13.3.3 Caritas-Praxisbeispiele

Die Technologie ist keine Zukunftsmusik — sie wird bereits in Caritas-Einrichtungen erfolgreich eingesetzt:

Caritasverband Stuttgart e. V.: - Pilotstart Februar 2020 mit Voize in der Altenhilfe - Seit Anfang 2023 in **allen fünf Altenhilfeeinrichtungen** im Einsatz - Ergebnisse: schnellere Dokumentation, verbesserte Dokumentationsqualität, gesteigerte Attraktivität des Pflegeberufs

Weitere Einsatzbeispiele in der Wohlfahrt: - **Diakoneo** (Evangelische Diakonie, Bayern): Voize erfüllt sowohl KDG- als auch DSG-EKD-Anforderungen; Mitarbeiter berichten von der Eliminierung von Überstunden für Dokumentation am Schichtende - **Diakonie Hochfranken**: KI-Dokumentationstool als "neue Wege in der Pflege"

13.3.4 Von der Eingabeorientierung zur Wirkungsorientierung

Die Lösung liegt in einem **Paradigmenwechsel der Refinanzierung**: Weg von der Bezahlung für eingesetzte Arbeitsstunden, hin zur Bezahlung für erzielte Wirkung.

Was Wirkungsorientierung bedeutet:

Statt zu fragen *"Wie viele Fachkraftstunden wurden erbracht?"* fragt ein wirkungsorientiertes System: - Wie hat sich die Lebensqualität der Bewohner entwickelt? - Wie hoch ist die Inzidenz von Stürzen, Dekubitus, Mangelernährung? - Wie zufrieden sind Bewohner und Angehörige? - Wie gut ist die kognitive Aktivierung?

In einem solchen System könnte eine Einrichtung, die mit 45 Pflegekräften + KI **dieselbe oder bessere Wirkung** erzielt wie eine andere mit 50 Pflegekräften ohne KI, **die Effizienzgewinne behalten** — und in weitere Innovation investieren.

Wer fordert diesen Wandel?

- Die **BAGFW** hat bereits 2015 in ihrer "Standortbestimmung zur Wirkungsorientierung" Wirkungsorientierung als Kernelement der Freien Wohlfahrtspflege definiert
- Der **Deutsche Pflegerat** fordert eine grundlegende Reform der Refinanzierungsregeln
- Das **Bündnis Digitalisierung in der Pflege** (8 Verbände, darunter VKAD und VdDD) fordert eine Digitalisierungspauschale und Personalschlüssel für IT-Personal
- **PHINEO** und die **Bertelsmann Stiftung** arbeiten an Modellen wirkungsorientierter Steuerung im Dritten Sektor

Das Mindeste, was sofort möglich wäre:

Auch ohne vollständigen Systemumbau müsste gelten: **Wenn der demografische Wandel dazu führt, dass Stellen nicht mehr besetzt werden können**, muss es erlaubt sein, die Wirkung dieser fehlenden Stellen durch IT/KI-Einsatz zu ersetzen — **ohne dass die Refinanzierung gekürzt wird**. Die eingesparten Personalkosten für nicht-besetzbare Stellen müssen in Technologie investiert werden dürfen.

13.4 Investitions- und Betriebskosten: Beide Seiten der Medaille

Eine nachhaltige IT-Strategie erfordert die Refinanzierung **beider** Kostenarten — sowohl der einmaligen Investitionen als auch des laufenden Betriebs. Das aktuelle System versagt bei beiden.

13.4.1 Investitionskosten (CAPEX)

Investition	Einmalige Kosten	Refinanzierung?
ISMS-Aufbau und -Zertifizierung (ISO 27001)	25.000 - 250.000 EUR	Nein
Netzwerksegmentierung und Firewall-Infrastruktur	50.000 - 200.000 EUR	Theoretisch KHG, praktisch Investitionsstau
MFA-Einführung (Hardware-Token, Infrastruktur)	10.000 - 50.000 EUR	Nein
SIEM/SOC (Security Monitoring)	30.000 - 150.000 EUR	Nein
Backup-Infrastruktur (immutable, offsite)	20.000 - 100.000 EUR	Nein
KI-Sprachdokumentation (Lizenz, Einführung)	20.000 - 80.000 EUR	Max. 12.000 EUR einmalig (§8 Abs. 8 SGB XI)
TI-Anbindung (Konnektor, Karten, Software)	5.000 - 20.000 EUR	Teilweise (TI-Pauschale)
Schulungen (Security Awareness, GL-Schulung)	10.000 - 40.000 EUR	Nein

13.4.2 Betriebskosten (OPEX) — oft vergessen, immer unterschätzt

Laufende Kosten	Jährlich	Refinanzierung?
IT-Sicherheitsbeauftragte/r (0,5-1,0 VZÄ)	30.000 - 90.000 EUR	Nein (kein Personalschlüssel für IT)
ISMS-Betrieb (Audits, Tools, Aktualisierung)	20.000 - 80.000 EUR	Nein
Software-Lizenzen (Antivirus, EDR, SIEM)	10.000 - 60.000 EUR	Nein
Penetrationstests (jährlich)	5.000 - 30.000 EUR	Nein
Security-Awareness-Schulungen	5.000 - 20.000 EUR	Nein
KI-Sprachdokumentation (laufende Lizenz)	15.000 - 50.000 EUR	Nein
Managed Security Services	20.000 - 80.000 EUR	Nein
TI-Betrieb, Updates, Support	5.000 - 15.000 EUR	Teilweise (TI-Pauschale)
KRITIS-Nachweisprüfung (alle 2 Jahre)	25.000 - 75.000 EUR (umgelegt)	Nein

Typische Gesamtkosten pro Jahr für ein Caritas-Krankenhaus: - **Investitionskosten (Erstjahr):** 200.000 - 800.000 EUR - **Laufende Betriebskosten:** 150.000 - 500.000 EUR/Jahr - **Davon refinanziert:** Praktisch nichts

Typische Gesamtkosten pro Jahr für ein Caritas-Pflegeheim: - **Investitionskosten (Erstjahr):** 30.000 - 150.000 EUR - **Laufende Betriebskosten:** 30.000 - 100.000 EUR/Jahr - **Davon refinanziert:** Max. 12.000 EUR einmalig + ca. 2.600 EUR/Jahr TI-Pauschale

13.5 Der politische Handlungsrahmen: Wer muss was tun?

13.5.1 Die BAGFW als Dach der politischen Interessenvertretung

Die **Bundesarbeitsgemeinschaft der Freien Wohlfahrtspflege (BAGFW)** vereint die sechs Spitzenverbände der Freien Wohlfahrtspflege:

Verband	Hauptamtliche Mitarbeiter	Einrichtungen
Deutscher Caritasverband (DCV)	740.000	25.400
Diakonie Deutschland	627.000	33.000
Arbeiterwohlfahrt (AWO)	270.000	18.000
Deutsches Rotes Kreuz (DRK)	210.000	4.000
Der Paritätische Gesamtverband	500.000	39.250
Zentralwohlfahrtsstelle der Juden (ZWST)	—	—
Gesamt	**ca. 2 Mio.**	—

Diese Verbände beschäftigen zusammen rund **2 Millionen Menschen** und engagieren **3 Millionen Ehrenamtliche**. Die BAGFW ist damit rein rechnerisch einer der größten Arbeitgeber Deutschlands (der größte nach dem Staat) — und einer der politisch einflussreichsten Akteure im Sozialbereich.

Was die BAGFW bereits tut:

- **"Wohlfahrt Digital"**: Gemeinsames Programm mit dem BMFSFJ zur digitalen Transformation der Wohlfahrtspflege (diewohlfahrt.digital)
- **Koordinierungsstelle Digitalisierung**: Bündelt digitale Aktivitäten aller sechs Verbände
- **Forderung nach Sondervermögens-Mitteln** (Mai 2025): Brief an Bundesfinanzminister und Kanzleramtsminister mit der Forderung nach **3 Mrd. EUR für "digitale Erreichbarkeit"** sozialer Dienste und **10 Mrd. EUR für Klimaanpassung** gemeinnütziger Einrichtungen
- **TI-Infrastruktur-Stellungnahme** (Juli 2025): Befragung von 1.460 Einrichtungen; 90% haben TI-Anbindung begonnen, aber nur ein kleiner Teil zum Stichtag 01.07.2025 tatsächlich angebunden — u.a. wegen monatelanger Wartezeiten und Kosten, die die Refinanzierungsmöglichkeiten übersteigen
- **Umfrage zur finanziellen Stabilität** (2026): Über 80 Prozent der Befragten rechnen perspektivisch mit der Kürzung oder Einstellung von sozialen Angeboten, 20 Prozent der befragten Träger haben in den vergangenen zwei Jahren Angebote vollständig eingestellt, mehr als 60 Prozent der Einrichtungen und Organisationen gaben an, dass das soziale Angebot in ihrer Region nicht oder nur in Teilen ausreichend ist

Was die BAGFW zusätzlich tun muss:

Die bisherigen BAGFW-Aktivitäten zur Digitalisierung fokussieren stark auf **digitale Teilhabe** und **Organisationsentwicklung**. Was fehlt, ist eine **koordinierte, verbändeübergreifende Kampagne** zur systematischen Refinanzierung von IT-Sicherheit und Digitalisierung. Bisher existiert kein eigenes BAGFW-Positionspapier zu NIS-2, zur IT-Sicherheitsrefinanzierung oder zur Wirkungsorientierung in der Vergütung. Diese Lücke muss dringend geschlossen werden, mit Unterstützung aller Wohlfahrtsverbände.

13.5.2 Die besondere Verantwortung des Deutschen Caritasverbandes

Der **Deutsche Caritasverband (DCV)** ist als größter Wohlfahrtsverband Deutschlands in einer besonderen Position:

Was der DCV bereits tut:

- **Positionspapier "Digitale Zukunft gestalten"** (Januar 2024): Fünf Kernforderungen zur digitalen Teilhabe
- **Pressemitteilung Sondervermögen** (Juni 2025): Vorstandsmitglied Susanne Pauser: *"Die soziale Infrastruktur darf beim digitalen Wandel nicht zurückgelassen werden"* — Forderung nach IT-Sicherheitsmitteln für Gesundheitswesen, Kitas, Krankenhäuser und Beratungsstellen
- **Krisenresilienz-Forderung** (März 2025): Caritas-Präsidentin Eva Welskop-Deffaa: *"Krisenresilienz ist ohne eine konzertierte Digitalisierungsanstrengung nicht zu gewährleisten"*
- **caritas|digital-Plattform**: Laufende Analyse und Advocacy zu Digitalisierungsthemen, u.a. der wegweisende Artikel "Refinanzierung der Digitalisierung — zwischen Systemlogik, Dilemma und Chancen"
- **Cybersecurity-Fachkongress** (gemeinsam mit Diakonie, Juni 2025): Johannes Landstorfer (DCV): *"Aktuelle Finanzierungsmodelle berücksichtigen keine angemessene IT-Sicherheit"*
- **Lobbyregistereintrag** im Bundestag (R000896): Systematische Interessenvertretung auf Bundesebene

Was der DCV mit der BAGFW zusätzlich leisten muss:

5. **Federführung** bei der Erarbeitung eines BAGFW-Positionspapiers zur IT-Sicherheitsrefinanzierung übernehmen
6. **Koordination** mit Diakonie, AWO, DRK und Paritätischem für eine gemeinsame Kampagne
7. **Quantifizierung** des Refinanzierungsbedarfs: Wie viel kostet NIS-2-Compliance für die gesamte Caritas? Wie hoch ist der IT-Investitionsstau?
8. **Modellprojekte** zur wirkungsorientierten Vergütung initiieren und evaluieren
9. **Politische Gespräche** mit den zuständigen Bundesministerien (BMG, BMFSFJ, BMAS, BMDV) führen
10. **Gesetzesänderungen** konkret einfordern: Digitalisierungspauschale in SGB XI, IT-Personalschlüssel in Landesrahmenverträgen, KHZG-Äquivalent für Sozialwirtschaft

13.5.3 Das Caritas-Netzwerk IT e. V.: Fachliche Unterstützung und "Cyber-Feuerwehr"

Das **Caritas-Netzwerk IT e. V.** (Sitz: Frankfurt am Main, Geschäftsführer: Gerhard Müller) bündelt die IT-Interessen von Caritas-Trägern und bietet konkrete Unterstützung:

Leistungen:

- **Incident & Response Service ("Cyber-Feuerwehr")** — seit 01.11.2024 für alle Mitglieder des Deutschen Caritasverbands:
    - 24/7-Notfall-Hotline
    - Bis zu 100 Expertenstunden pro erfolgreichem Angriff und Mitglied
    - Remote-Unterstützung innerhalb von max. 4 Stunden
    - Vor-Ort-Unterstützung innerhalb von max. 24 Stunden
    - Zugang zu Playbooks, Konfigurationshilfen und Checklisten über CariNet
    - 2-3 Workshops pro Jahr zu IT-Sicherheitsthemen
- **Strategische IT-Beratung:** Entwicklung von IT-Strategien, Bedarfserhebung, Erfahrungsaustausch und Bündelung von IT-Anforderungen

- **Politische Mitwirkung:** z.B. Co-Organisation des Cybersecurity-Fachkongresses gemeinsam mit DCV und Diakonie

Das Angebot des Caritas-Netzwerk IT an die Verbände:

Das Caritas-Netzwerk IT e. V. bietet seine Expertise und Unterstützung ausdrücklich für die politische Advocacy-Arbeit an. Konkret kann es helfen bei:

- **Fachlicher Unterstützung** der BAGFW-Positionierung zu IT-Sicherheit und Digitalisierung
- **Quantifizierung** der IT-Investitions- und Betriebskosten über verschiedene Trägertypen
- **Entwicklung** von Musterargumentationen für Pflegesatzverhandlungen und politische Gespräche
- **Vernetzung** von Caritas-IT-Verantwortlichen für koordiniertes Vorgehen
- **Best-Practice-Dokumentation** erfolgreicher Digitalisierungsprojekte (z.B. Caritas Stuttgart/Voize)
- **Technische Bewertung** von Gesetzesvorschlägen und Verordnungsentwürfen

Website: https://www.caritas-netzwerk-it.de/ Kontakt: info@caritas-netzwerk-it.de

13.6 Konkrete politische Forderungen

Auf Basis der Analyse ergibt sich ein **Forderungskatalog**, den die Wohlfahrtsverbände gemeinsam — unter dem Dach der BAGFW und mit fachlicher Unterstützung durch Organisationen wie dem Caritas-Netzwerk IT — gegenüber Politik und Kostenträgern vertreten müssen:

Sofortmaßnahmen (2026-2027)

Nr.	Forderung	Adressat	Mechanismus
1	**Mittel aus dem Sondervermögen Infrastruktur** für IT-Sicherheit und Digitalisierung der Sozialwirtschaft bereitstellen	Bundesregierung, Bundestag	Mindestens **3 Mrd. EUR** für “digitale Erreichbarkeit” sozialer Dienste (BAGFW-Forderung)
2	**Digitalisierungspauschale in SGB XI** einführen: verlässliche, dauerhafte Refinanzierung von IT-Investitions- und Betriebskosten in Pflegesätzen	BMG, Bundestag	Gesetzesänderung §84/§85 SGB XI
3	**IT-Personalschlüssel** in Landesrahmenverträgen verankern: Anerkennung von IT-Sicherheits- und Digitalisierungspersonal	Länder, Kostenträger	Änderung der Landesrahmenverträge nach SGB XI
4	**§8 Abs. 8 SGB XI** deutlich aufstocken und verstetigen: statt 12.000 EUR einmalig mindestens **50.000 EUR** und laufende Fördermöglichkeit	BMG, Bundestag	Gesetzesänderung

Strukturelle Reformen (2027-2030)

Nr.	Forderung	Adressat	Mechanismus
5	**KHZG-Äquivalent für die Sozialwirtschaft** schaffen: Investitionsfonds für IT-Sicherheit und Digitalisierung in Pflege, Eingliederungshilfe und Jugendhilfe	Bundesregierung	Neues Gesetz nach Vorbild KHZG
6	**Wirkungsorientierte Vergütungselemente** pilotieren: Modellprojekte, bei denen	BMG, BMFSFJ, Innovationsfonds	Modellvorhaben nach §8 Abs. 3 SGB XI

Nr.	Forderung	Adressat	Mechanismus
	Ergebnisqualität statt Fachkraftstunden vergütet wird		
7	**Effizienzgewinne durch Digitalisierung** dürfen nicht zu Kürzungen führen: Gesetzliche Klarstellung, dass technologiebedingte Einsparungen reinvestiert werden dürfen	BMG, Bundestag	Klarstellung in SGB XI und SGB V
8	**Gemeinnützige Träger** in Digitalisierungsförderprogramme einbeziehen: Sozialwirtschaft wird bisher von KMU-Förderprogrammen (go-digital, BAFA etc.) systematisch ausgeschlossen	BMWi/BMDV	Erweiterung der Förderrichtlinien

Ordnungspolitische Forderungen

Nr.	Forderung	Adressat	Begründung
9	**"Kein Gesetz ohne Finanzierung"**: Jedes neue Gesetz mit IT-Sicherheitsanforderungen muss eine Refinanzierungsregelung enthalten	Bundestag, Bundesrat	Analog zum Konnexitätsprinzip bei Kommunen
10	**KDG und DSGVO harmonisieren**: Doppelte Compliance-Kosten durch parallele Datenschutzregime reduzieren	Bischofskonferenz, EU-Kommission	Abstimmung der Anforderungen
11	**Regulatorische Konsolidierung**: Die 15+ IT-Sicherheitsgesetze zu einem kohärenten Rahmen bündeln	BMI, BMG, BMDV	Entlastung der Einrichtungen

13.7 Der Appell: Gemeinsam handeln — jetzt

Die Sozialwirtschaft steht an einem Scheideweg. Zwei Megatrends — **demografischer Wandel** und **Digitalisierung/KI** — treffen auf ein **Refinanzierungssystem aus dem 20. Jahrhundert**, das weder IT-Sicherheit noch digitale Innovation systematisch finanziert.

Die Lage ist paradox: - Der Gesetzgeber **verlangt** IT-Sicherheit durch immer mehr Gesetze (NIS-2, BSIG, KDG, DSGVO, DigiG, PDSG, CRA, KRITIS-Dachgesetz…) - Die Kostenträger **finanzieren** sie nicht - KI-Technologie **könnte** den Fachkräftemangel teilweise kompensieren - Das Refinanzierungssystem **bestraft** Einrichtungen, die KI einsetzen

Was passiert, wenn nichts geschieht? - Steigende Cyberangriffe auf ungeschützte Sozialeinrichtungen (s. Caritas München 2022: 23 Mio. EUR Schaden) - Wachsender Fachkräftemangel ohne technologische Kompensation - Zunehmende Versorgungslücken in Pflege, Eingliederungshilfe und Jugendhilfe - Persönliche Geschäftsleiterhaftung bei NIS-2-Verstößen ohne Möglichkeit zur Refinanzierung der Schutzmaßnahmen - Bußgelder bis 10 Mio. EUR für Einrichtungen, die die Gesetze nicht erfüllen können, weil die Mittel fehlen

Was nötig ist:

Die Freie Wohlfahrtspflege muss **gemeinsam, koordiniert und mit Nachdruck** politischen Druck ausüben. Das bedeutet:

1. **Die BAGFW** muss IT-Sicherheitsrefinanzierung als strategisches Schwerpunktthema aufgreifen und ein verbändeübergreifendes Positionspapier vorlegen

2. **Der Deutsche Caritasverband** muss als größter Wohlfahrtsverband eine Führungsrolle übernehmen und die Koordination mit den anderen fünf Verbänden vorantreiben
3. **Das Bündnis Digitalisierung in der Pflege** (VKAD, VdDD, FINSOZ, vediso, bvitg, DPR u.a.) liefert die fachliche Grundlage und die konkreten Forderungen
4. **Das Caritas-Netzwerk IT e. V.** steht als fachlicher Partner bereit, um die politische Arbeit mit technischer Expertise und Praxiserfahrung zu unterstützen
5. **Jeder einzelne Caritas-Träger** muss das Thema in seinen Gremien, in den Pflegesatzverhandlungen und im Dialog mit der Kommunalpolitik adressieren

> ***Die soziale Infrastruktur Deutschlands darf beim digitalen Wandel nicht zurückgelassen werden.*** *Wer IT-Sicherheit gesetzlich vorschreibt, muss sie auch refinanzieren. Wer den Fachkräftemangel beklagt, muss technologische Lösungen zulassen und finanzieren. Wer Ergebnisqualität will, muss aufhören, nur Personalstunden zu bezahlen.*
>
> *Das ist keine technische Frage. Das ist eine* ***politische Aufgabe****.*

13.8 Quellen zu Kapitel 13

Gesetze und Verordnungen: - KDG §26 — Technische und organisatorische Maßnahmen - KDG-DVO (neue Fassung 2025) - §391 SGB V — IT-Sicherheit im Krankenhaus - §393 SGB V — Cloud-Computing im Gesundheitswesen - §8 Abs. 8 SGB XI — Digitalisierungsförderung - §85 SGB XI — Pflegesatzverfahren - §115 Abs. 3a SGB XI — Vergütungskürzung - KRITIS-Dachgesetz - Cyber Resilience Act

Investitions- und Finanzierungslücken: - DKG — Krankenhaus-Investitionslücke 2,64 Mrd. EUR - PwC — Finanzierungslücken bremsen Krankenhaus-Digitalisierung - DKG — IT-Ausgaben im internationalen Vergleich - Roland Berger Hospital IT Monitor 2024

Fachkräftemangel: - Statistisches Bundesamt — Pflegekräftevorausberechnung 2024 - Bundesagentur für Arbeit — Engpassanalyse 2024 - Caritas — “20 Prozent der Stellen sind unbesetzt” - Bertelsmann Stiftung — Pflegereport 2030 - IAB — Fach- und Arbeitskräftemangel

KI und Voice-Technologie: - Charité-Voize-Pilotstudie - Charité-Studie — 27% weniger Dokumentationsaufwand - Caritasverband Stuttgart — Voize-Erfahrungsbericht - Voize

Politische Positionen und Forderungen: - BAGFW — Wohlfahrt Digital - BAGFW — Sondervermögen-Forderung - BAGFW — Telematik-Infrastruktur-Stellungnahme - DCV — Sondervermögen-Forderung (Juni 2025) - DCV — Krisenresilienz (März 2025) - DCV — Digitale Zukunft gestalten (Januar 2024) - caritas|digital — Refinanzierung der Digitalisierung - neue caritas — Der Knackpunkt (2024) - Bündnis Digitalisierung in der Pflege - DEVAP — Pflege: Ohne Refinanzierung keine nachhaltige Digitalisierung - Deutscher Pflegerat — Refinanzierung Digitalisierungskosten - FINSOZ — Pflegereform muss auf Digitalisierung setzen - Paritätischer — Positionspapier Digitalisierung - vediso — Lobbyregister - Caritas-Netzwerk IT e. V. - Koalitionsvertrag 2025 (CDU/CSU-SPD)

Praxisbeispiel Cyberangriff: - Ransomware-Angriff Caritas München 2022 — 23 Mio. EUR Schaden

Anhang A: Generelle Quellen

Gesetzliche Grundlagen

- NIS2-RLUG — Bundesgesetzblatt 2025 I Nr. 301
- BSI — NIS-2-regulierte Unternehmen
- BSI — NIS-2 FAQ allgemein
- BSI — NIS-2 Sektorspezifische FAQ
- BSI — Betroffenheitsprüfung (Online-Tool)
- §30 BSIG — Risikomanagementmaßnahmen
- §32 BSIG — Meldepflichten
- §38 BSIG — Geschäftsleiterpflichten

Caritas-spezifisch

- Caritas Statistik — Die Caritas in Zahlen
- KKVD — Katholischer Krankenhausverband
- SoCura — Über uns
- Caritas-Netzwerk IT — Leistungen
- DCV/Diakonie — Sozialwirtschaft und Cybersicherheit

Krankenhausfinanzierung

- BMG — Krankenhausfinanzierung
- BMG — KHZG
- DKG — Krankenhauszukunftsfonds
- DKG — Investitionsstau
- Planfox — Krankenhaustransformationsfonds
- PwC — KHZG und NIS-2 Synergien
- InEK — Kalkulationshandbuch

DKG-Stellungnahmen zu NIS-2

- DKG — Stellungnahme Oktober 2023 (PDF)
- DKG — Stellungnahme Juli 2024 (PDF)
- DKG — Stellungnahme September 2024 (PDF)

Pflege und Refinanzierung

- §84 SGB XI — Bemessungsgrundsätze
- §85 SGB XI — Pflegesatzverfahren
- GKV-Spitzenverband — Digitalisierungsförderung §8 Abs. 8 SGB XI
- §125 SGB IX — Leistungsvereinbarung
- §78c SGB VIII — Entgeltvereinbarung

Verbände und Stellungnahmen

- V3D — Fachkongress Cybersecurity 2025
- Der Paritätische — NIS2 und Wohlfahrt

- BAGFW — Wohlfahrt digital
- FINSOZ — NIS-2 Orientierungshilfe

Förderprogramme

- ESF Plus — rückenwind3
- KfW — ERP-Förderkredit Digitalisierung
- Transferstelle Cybersicherheit

Fachquellen

- OpenKRITIS — NIS2 Sektoren
- OpenKRITIS — Geltungsbereich
- Solidaris — NIS-2-Umsetzungsgesetz
- Solidaris — Pflege-Einrichtungen und NIS-2
- GvW — NIS-2 und die Vernachlässigbarkeit
- Heuking — Scope for Corporate Groups

Praxisbeispiel

- Ransomware-Angriff Caritas München 2022 — 23 Mio. EUR Schaden

Anhang B: Der Caritas-Netzwerk IT e. V. im Überblick

Der Caritas-Netzwerk IT e. V. ist ein eingetragener Verein mit Sitz in Frankfurt am Main (Amtsgericht Frankfurt am Main, Vereinsregister VR 16954). Er wurde im Januar 2022 gegründet und versteht sich als strategische Interessenvertretung und Kooperationsplattform für IT-Themen in der Caritas-Welt.

Der Verein bündelt die Bedarfe, das Fachwissen und die Zusammenarbeit seiner Mitglieder, um professionelle IT-Strategien und IT-Strukturen nachhaltig und finanzierbar aufzubauen. Dabei werden IT-Fragen der Träger als Geschäftskooperation behandelt – der Verein dient seinen Mitgliedern als strategischer Partner für innovative, bedarfsgerechte, sichere und digitale Lösungen.

Durch gemeinsame Sprache und gebündelte Positionen kann der Verein gegenüber Politik, Software- und Hardwareherstellern sowie Infrastrukturbetreibern für geeignete Rahmenbedingungen eintreten, die eine gute Unterstützung der Sorgearbeit ermöglichen.

Mitglieder und Reichweite

Mitglied im Caritas-Netzwerk IT e. V. können ausschließlich Rechtsträger der Caritas werden. Der Verein ist darüber hinaus offen für die Zusammenarbeit mit allen Organisationen der Sozialwirtschaft.

Seit der Gründung im Januar 2022 ist der Verein stark gewachsen: Von rund 100 Gründungsmitgliedern auf mittlerweile ca. 150 Caritas-Rechtsträger (Stand Februar 2026). Die Mitgliedsorganisationen repräsentieren zusammen ca. 80.000 Mitarbeitende in ganz Deutschland.

Organisation und Struktur

Ehrenamtlicher Vorstand

Der Verein wird von einem ehrenamtlichen Vorstand geleitet, der im Caritas-Verbandswesen breit vernetzt ist und die operative sowie strategische Ausrichtung verantwortet:

Name	Funktion
Dr. Rainer Brockhoff	Vorstandsmitglied (ehem. Caritasdirektor der Diözese Rottenburg-Stuttgart)
Markus Nikolaus	Vorstandsmitglied (Finanzdirektor Caritasverband für die Stadt Köln)
Alexander Rees	Vorstandsmitglied (Abteilungsleiter Digitales, Deutscher Caritasverband e. V.)

Geschäftsstelle

Die operative Arbeit wird von der Geschäftsstelle geleistet:

Gerhard Müller – Geschäftsführer

Mirco Beyer – Referent für Kooperationsentwicklung

Gabriella Bamberger – Vorstandsassistenz & Mitgliederverwaltung

Interesse an einer Mitgliedschaft? Gabriella Bamberger ist die erste Ansprechpartnerin für alle Fragen rund um den Beitritt zum Verein. Kontakt zum Verein unter https://caritas-netzwerk-it.de/kontakt.

Angebote und Leistungen

Erfahrungsaustauschgruppen

Die Erfahrungsaustauschgruppen sind ein Herzstück des Vereins. In ihnen kommen Fachleute aus der Caritas-Welt als „Teilgeber:innen" zusammen, um sich zu konkreten IT-Themen auszutauschen. Der Grundgedanke: Voneinander lernen, miteinander wachsen. Die Treffen finden ca. alle vier Wochen virtuell über Microsoft Teams statt (45–60 Minuten) und werden unter der Chatham House Rule geführt.

Aktuelle Erfahrungsaustauschgruppen:

- **Notfallmanagement** – Backup-Strategien, Notfallkonzepte, Incident & Response, IT-Notfallvorsorge
- **Einführung und Nutzung von Microsoft 365** – Migration, produktiver Einsatz, Change-Management, rechtliche Rahmenbedingungen
- **Einführung und Nutzung von KI** – Einsatzszenarien, rechtliche Grundlagen, Tools, Chancen und Herausforderungen
- **Kunden und potenzielle Kunden von SoCura** – Austausch für Einrichtungen, die SoCura als IT-Dienstleister nutzen oder dies erwägen
- **Connext Vivendi** – Einführung, Konfiguration, Updates und Best Practices der Fachsoftware

Alle Treffen werden aufgezeichnet und KI-gestützt zusammengefasst (mit redaktioneller Prüfung). Die Zusammenfassungen werden im CariNet/per Mail veröffentlicht und bilden eine wachsende Wissensbasis.

Cyber-Feuerwehr: Incident & Response

Seit November 2024 bietet der Verein allen Mitgliedern des Deutschen Caritasverbandes den IT-Sicherheitsservice „Incident & Response" an – eine Cyber-Feuerwehr für den Ernstfall. Der Dienst existiert seit Oktober 2023 und hat bereits zahlreiche Mitglieder erfolgreich durch IT-Krisen begleitet.

Kernleistungen der Cyber-Feuerwehr:

- 24/7-Hotline: Rund-um-die-Uhr-Erreichbarkeit, sieben Tage die Woche
- Bis zu 100 Stunden Expertenhilfe pro Vorfall (durch den IT-Dienstleister SVA)
- Professionelles Onboarding zur Vorbereitung auf IT-Notfälle, Playbooks, Workshops
- Kosten: 1,00 € brutto pro Vollzeitäquivalent/Monat (Mitglieder); 1,50 € (Nichtmitglieder)

CariNet – Die Community-Plattform

CariNet (https://carinet.de) ist die zentrale Intranet- und Community-Plattform des Vereins. Sie bietet Zusammenfassungen der Treffen, Wissensbeiträge und Best Practices, Ankündigungen, ein Mitgliederverzeichnis sowie weiterführende Materialien wie Präsentationen und Leitfäden. Mitglieder haben Schreibrechte und können sich aktiv einbringen.

Newsletter

Der Verein gibt ca. alle vier bis sechs Wochen einen **Newsletter** heraus, der über Neuigkeiten, Veranstaltungen, Impulse aus den Erfahrungsaustauschgruppen und relevante IT-Trends in der freien Wohlfahrt informiert. Der Newsletter kann auch von Nicht-Mitgliedern kostenfrei abonniert werden.

Veranstaltungen, Arbeitsgruppen und Netzwerk

Neben den Erfahrungsaustauschgruppen organisiert der Verein – normalerweise in Kooperation mit anderen Organisationen, wie z.B. dem Deutschen Caritasverband (DCV) oder der Diakonie – Fachtagungen, Arbeitsgruppen und Projekte zu übergreifenden IT-Themen. Mitglieder erhalten Zugang zu einem breiten Netzwerk von IT-Fachleuten aus der gesamten Caritas-Landschaft.

Beispiele für Veranstaltungen 2026:

- **Fachkongress Cybersecurity** – 11./12. Juni 2026 in Berlin (gemeinsam mit der Diakonie)
- **IT-Leiter-Tagung** – 29. September – 2. Oktober 2026 (gemeinsam mit dem DCV)

Mitgliedschaftsbeiträge

Die Mitgliedschaft im Caritas-Netzwerk IT e. V. ist bewusst niedrigschwellig und solidarisch gestaltet. Die Beiträge bemessen sich nach der Anzahl der Vollzeitäquivalente (VZÄ) der Mitgliedsorganisation:

- Einmalige Aufnahmegebühr: 1,00 € pro Vollzeitäquivalent
- Jährlicher Mitgliedsbeitrag: 2,00 € pro Vollzeitäquivalent

Der Mehrwert einer Mitgliedschaft

- Strategische Interessenvertretung gegenüber Politik, Herstellern und Infrastrukturbetreibern
- Strukturierter Erfahrungsaustausch mit IT- bzw. Digitalisierungs-Fachleuten aus der gesamten Caritas
- Gemeinsame Bedarfsermittlung und Definition von Standards
- Zugang zur Cyber-Feuerwehr mit 24/7-Hotline zu vergünstigten Konditionen
- Nutzung der Community-Plattform CariNet als Wissensbasis und Austauschforum
- Teilnahme an Fachtagungen, Arbeitsgruppen und Projekten
- Regelmäßiger Newsletter mit relevanten IT-Trends der Sozialwirtschaft

Kontakt

Caritas-Netzwerk IT e. V.

Sitz: 60311 Frankfurt am Main

Vereinsregister: VR 16954, Amtsgericht Frankfurt am Main

Webseite: https://www.caritas-netzwerk-it.de

Kontaktinformationen: https://www.caritas-netzwerk-it.de/kontakt

Satzung, Mitgliederliste, Vereinspräsentation, Template-Angebot für das Cyber-Feuerwehr: In der für alle offenen Carinet-Gruppe ‚Allgemeine Informationen zum Caritas-Netzwerk IT e. V.' einsehbar

Geschäftsstelle:

Gerhard Müller (Geschäftsführer) – Gerhard.Mueller@caritas-netzwerk-it.de

Mirco Beyer (Referent für Kooperationsentwicklung) – Mirco.Beyer@caritas-netzwerk-it.de

Gabriella Bamberger (Vorstandsassistenz & Mitgliederverwaltung) – Gabriella.Bamberger@caritas-netzwerk-it.de

Stand: Ende Februar 2026