Warum NIS2 die Schweiz direkt betrifft / nis2-audit.ch

Die EU-Richtlinie NIS2 entfaltet durch globale Lieferketten eine massive extraterritoriale Wirkung. Kombiniert mit den verschärften Schweizer Gesetzen (revDSG, ISG) entsteht für Stiftungen und KMU ein sofortiger Handlungsbedarf auf Management-Ebene.

⚠ **Management-Haftung im Fokus:**
Persönliche Haftungsrisiken für Geschäftsleitung und Stiftungsräte sind real. Privatvermögen inklusive.

Stand: April 2026

Für KMU, Stiftungen und NPO

Inhaltsverzeichnis

Revidiertes Datenschutzgesetz (DSG)

Das revidierte Datenschutzgesetz (DSG) seit Sept 2023 verlangt adäquate Datensicherheit nach EU Standards. Zudem trat Jan 2024 das **Bundes-Informationssicherheitsgesetz (ISG)** in Kraft, das für Bundesbehörden und Betreiber kritischer Infrastrukturen (u.a. Banken, Versicherer, Gesundheitswesen, Energie, Verkehr) ein **ISMS nach ISO 27001** verlangt.

Damit steigt der Compliance-Druck auch auf grössere Organisationen in der Schweiz, sich nach NIS2-ähnlichen Vorgaben zertifizieren zu lassen.

NIS2, ISG & revDSG: Was gilt wo?

Schweiz (CH)

Eigenständiges Recht (revDSG, ISG, KRITIS-Meldepflicht).

24h KRITIS-Meldung ans BACS und **14 Tage** für den Ergänzungsbericht.

Liechtenstein (LI)

NIS2 vollständig umgesetzt via CSG (seit 1.2.2025).

3-Stufen-Meldung: **24h** Frühwarnung

72h Vorfallmeldung,

1 Monat Bericht ans CSIRT.LI.

Deutschland (DE)

NIS2-pflichtig (NIS2UmsuCG seit 1.3.2025). Gleiches 3-Stufen-Meldesystem wie LI an das BSI.

Management-Schulungen sind in LI und DE gesetzliche Pflicht (Art. 20 Abs. 2).

Warum jetzt handeln: Persönliche Haftung der Geschäftsleitung ist in beiden Ländern real. Sanktionen gegen Privatvermögen. Kein Versicherungsschutz für fahrlässige Untätigkeit.

Cybersicherheit & Compliance: Die Treiber

Warum Handlungsbedarf besteht

Marktforderungen übersteigen zunehmend die reine Inlandsgesetzgebung.

Die Treiber für Cybersicherheit im Schweizer Mittelstand setzen sich wie folgt zusammen:

Externe Marktanforderungen

EU-Kundenforderungen (NIS2/Verträge) und Cyber-Versicherungsvorgaben drängen auch **Schweizer Unternehmen** zur Compliance. Unabhängig von der direkten Gesetzespflicht.

Schweizer Gesetzgebung & Risikomanagement

Das revDSG und das Informationssicherheitsgesetz (ISG) schaffen klare inländische Pflichten.

Ergänzt durch das eigene Risikomanagement ergibt sich ein umfassender Handlungsrahmen.

Der Domino-Effekt

Auch wenn die EU-Richtlinie NIS2 in der Schweiz rechtlich nicht direkt gilt, werden Schweizer Unternehmen durch globale Lieferketten faktisch in die Pflicht genommen.

Vertragliche Weitergabe

EU-Unternehmen (KRITIS) müssen gemäss Artikel 21 (NIS2) die Sicherheit ihrer Lieferkette garantieren.

Faktische Pflicht für Schweizer KMU

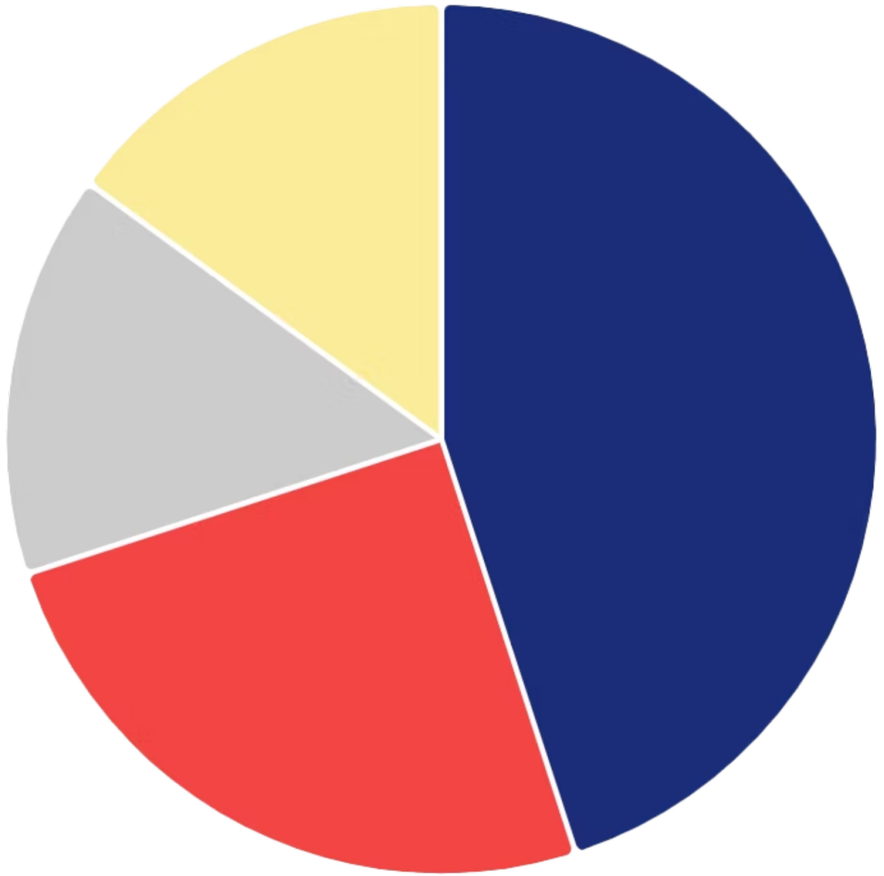
Diese Anforderungen werden vertraglich an Schweizer Zulieferer und Dienstleister weitergegeben.

Die Konsequenz

Wer nicht "NIS2-ready" ist, verliert EU-Aufträge. Kombiniert mit den verschärften Schweizer Gesetzen entsteht ein sofortiger Handlungsbedarf auf Management-Ebene.

Treiber für Cybersicherheit

im Schweizer Mittelstand



Treiber (Schätzung)

45%

EU-Kundenforderungen

NIS2/Verträge

25%

Schweizer Gesetzgebung

revDSG/ISG

15%

Eigenes Risikomanagement

15%

Cyber-Versicherungsvorgaben

Marktforderungen übersteigen zunehmend die reine Inlandsgesetzgebung.

Schweizer Regelwerk vs. NIS2

Eine ISO 27001 Zertifizierung schliesst die Lücke zwischen Schweizer Recht und EU-Anforderungen und minimiert das persönliche Haftungsrisiko drastisch.

Gesetzlich verpflichtend

Neues Datenschutzgesetz (revDSG)

Meldepflicht bei Datenschutzverletzungen. Persönliche Bussen für Geschäftsleitung & Stiftungsräte bis zu **CHF 250'000**.

Meldepflicht für Cyberangriffe (ab 2025)

Obligatorische Meldung an BACS innerhalb von **24h** für KRITIS-Betreiber.

Informationssicherheitsgesetz (ISG)

Grundstein für Sicherheit von Bundesdaten und KRITIS.

Zwingende B2B-Verträge

Vertragliche Verpflichtung zur Umsetzung von NIS2-Massnahmen durch EU-Kunden.

Stark empfohlen

ISO/IEC 27001:2022

Deckt ~70–80% der NIS2-Anforderungen ab. Stärkster Einzelnachweis der Sorgfaltspflicht.

IKT-Minimalstandard (BACS)

108 Massnahmen basierend auf NIST CSF. Freiwillig, gilt aber vor CH-Gerichten als Sorgfaltsmassstab.

Governance & Schulung

Regelmässige Sensibilisierung der Geschäftsleitung und des Stiftungsrates.

Incident Response Plan

Etablierte, getestete Prozesse zur Erfüllung der 24h-Meldepflichten.

Konvergenz der Standards:

Abdeckung der NIS2-Ziele

Die Lücke schliessen

Wer sich ausschliesslich auf das Schweizer Recht (revDSG, ISG) beschränkt, weist erhebliche Lücken in der **Lieferkettensicherheit** und im **Risikomanagement** auf.

Die Umsetzung des **IKT-Minimalstandards** oder einer **ISO 27001 Zertifizierung** schliesst diese Lücken pragmatisch. Die Vorbereitung auf NIS2 deckt gleichzeitig alle Schweizer Regularien ab und minimiert das persönliche Haftungsrisiko der Organe drastisch.

⚠ Die Schweizer Rechtslage **allein** genügt oft nicht für EU-Kunden. ISO 27001 schliesst die Lücke massgeblich.

Wer ist betroffen?

Fokus-Sektoren

Folgende Sektoren stehen im Fokus der neuen Regulierungen:

Kritische Infrastrukturen

- **Energie & Wasser**
  Strom, Gas, Fernwärme, Trink & Abwasser
- **Gesundheitswesen**
  Krankenhäuser, Pharma, Labore, Medtech
- **Transport**
  Luftfahrt, Schiene, Schifffahr, ÖPNV
- **Bank- & Finanzwesen**
  Kreditinstitute, Handelsplätze

Digitale Dienste & Infrastruktur

- **Digitale Ifrastruktur**
  Cloud, Rechencenter, Vertrauensdienste, DNS
- **Digitale Dienste**
  Marktplätze, Suchmaschinen, Soziale Netzwerke

Weitere Wirtschaftszweige

- **Verarbeitendes Gewerbe**
  Maschinenbau, Kfz, Elektronik
- **Lebensmittel**
  Produktion, Verarbeitung& Grosshandel
- **Entsorgung**
  Abfallbewirtschaftung
- **Chemikalien**
  Herstellung und Vertrieb
- **Post- & Kurierdienste**

Auch indirekt betroffene Unternehmen, insbesondere Zulieferer und Dienstleister für KRITIS-Betreiber, müssen mit vertraglichen Weitergabepflichten rechnen.

Wer ist betroffen?

Stiftungen & NPO

Eine Stiftung ist dann betroffen, wenn sie eine wirtschaftliche Tätigkeit ausübt und in einen der genannten Sektoren fällt:

Tätigkeiten

- **Stiftungen im Gesundheitswesen:**
  Krankenhäuser/Pflege (ab 50 MA NIS2-pflichtig)
- **Forschungsstiftungen:**
  Sofern keine reine akademische Grundlagenforschung
- **Bildungsstiftungen:**
  Meist ausgenommen, ausser bei digitaler Infrastruktur
- **Abgrenzung:**
  Gemeinnützigkeit schützt nicht vor Audit-Pflichten bei Erreichen der Schwellenwerte

Betroffen sind Stiftungen…

- mit EU-Niederlassungen, Projektträgern oder Tochterorganisationen
- die IT- oder Cloud-Services nutzen
- die kritische, relevante oder gesellschaftliche Leistungen bieten
- die personenbezogene oder medizinische Daten verwalten
- mit indirekter Betroffenheit als Lieferanten oder Partner

Die 10 Mindestmassnahmen (Art. 21 NIS2)

Verbindlich in der EU/LI und als Best Practice in der Schweiz massgeblich:

1

Risikoanalyse & Sicherheitsrichtlinien

ISMS, Risikoregister

2

Incident Management

IRP mit 24h-Meldefähigkeit, Tests

3

Business Continuity

Backup-Konzepte, Restore-Tests

4

Supply Chain Security

Lieferantenregister, Audit-Rechte

5

IT-Erwerb, Entwicklung, Wartung

Patch Management, Asset-Inventar

6

Wirksamkeitsbewertung

Interne Audits, Penetrationstests

7

Cyberhygiene & Schulungen

Awareness, dokumentierte Management-Schulung

8

Kryptographie & Verschlüsselung

AES-256, TLS 1.2+

9

Personalsicherheit & Zugangskontrolle

Least Privilege, schnelle Sperrungen

10

MFA & sichere Kommunikation

Phishing-resistente MFA für Remote & Cloud

⚠

Dunkelblau markierte Massnahmen werden in Audits am häufigsten als unzureichend bewertet.

Sanktionen und Management-Haftung

Das persönliche Risiko für Geschäftsleitungen und Stiftungsräte ist real. Es gibt keinen Versicherungsschutz für fahrlässige Untätigkeit.

EU / Liechtenstein (NIS2)

Wesentliche Einrichtung:
Bis zu CHF 10 Mio. oder 2% des weltweiten Jahresumsatzes.

+ Zwangsgelder (CHF 100'000/Tag)
+ bis zu 3 Jahre Funktionssperre für das Management.

EU / Liechtenstein (NIS2)

Wichtige Einrichtung:
Bis zu CHF 7 Mio. oder 1,4% des weltweiten Jahresumsatzes.
Persönliche Haftung Stiftungsrat/GF
Keine D&O-Abdeckung für Vorsatz

Schweiz (CH)

Bis zu **CHF 250'000** (revDSG) direkt gegen natürliche Personen

Art. 754 OR: unlimitierte PrivathaftungCHF 100'000 bei KRITIS-Nichtmeldung Strukturell schärfer als EU-Obergrenzen, da das Privatvermögen direkt haftet.

> **Das persönliche Haftungsrisiko in der Schweiz ist strukturell schärfer als in der EU. Das Privatvermögen der Entscheidungsträger haftet direkt.**

Stiftungen: Besonders exponiert

Stiftungsräte sind besonders exponiert. Das revidierte DSG verlangt adäquate Datensicherheit nach EU-Standards.

Strukturelle Risiken

- Keine Aktionäre / Gesellschafter als Kontrollkorrektiv
- IT vollständig ausgelagert = Supply-Chain-Risiko nach NIS2
- Sensible Daten: Begünstigte, Spender, Gesundheitsbezug
- Ressourcenknappheit: keine dedizierte IT-Security
- Oft in regulierten Sektoren tätig (Gesundheit, Finanzen

Wer fällt unter NIS2?

- Finanzstiftungen mit Bank-/Anlageaktivitäten >50 MA
- Stiftungen im Gesundheitswesen >10 Mio. EUR
- Treuhandgesellschaften als ICT-Dienstleister B2B
- Familienstiftungen: Prüfung nach Sektor & Grösse
- Kleine gemeinnützige Stiftungen: meist nicht direkt betroffen

Haftung Stiftungsrat

- **LI:** BJR (Art. 182 PGR) schützt nur bei nachweislicher Information
- **LI:** 3-jährige Funktionssperre bei wiederholten Verstössen
- **CH:** **Art. 84 ZGB**, objektiver Sorgfaltsmassstab
- **CH:** Art. 754 OR, unlimitierte Privathaftung, Beweislastumkehr
- Delegation an IT reicht nicht ➔ GF-Ebene bleibt verantwortlich

Sofortmassnahmen

1. Scoping-Check (Betroffenheit prüfen)
2. Stiftungsratsprotokoll mit Cybersecurity-Beschluss
3. Management-Schulung inkl. Dokumentation
4. IT-Dienstleister-Audit (Vertragscheck)
5. Incident Response Plan (24h-Meldefähigkeit testen)

Handlungsplan: In 4 Phasen zur Compliance

Phase 1 (0–30 Tage)

- MFA für alle Cloud-Dienste & VPN aktivieren
- Backup-Restore tatsächlich testen (offline Kopie!)
- Verantwortlichkeit in Geschäftsleitung benennen
- Notfallkontaktliste (CSIRT.LI / BACS / Anwalt)
- Öffentliche Ports / Shadow IT scannen

Phase 2 (1–3 Monate)

- Gap-Analyse gegen Art. 21 NIS2 / IKT-Minimalstandard
- Incident Response Plan + Tabletop-Übung
- IT-Lieferanten-Inventar & Vertragscheck
- Management-Schulung (dokumentiert)
- ISMS-Basisdokumentation: Richtlinien, Risikoregister

Phase 3 (3–12 Monate)

- ISO 27001 Implementierung starten
- Externer Penetrationstest
- Supply Chain: ISO 27001 / SOC 2 bei Lieferanten einfordern
- Monitoring / Managed SOC einführen
- Registrierung BSI / Stabsstelle abschliessen

Phase 4 (12–24 Monate)

- ISO 27001 Zertifizierung abschliessen
- Quartalsweise KPI-Berichterstattung an Leitungsorgane
- Externe Audits alle 2–3 Jahre etablieren
- Regulatorisches Monitoring: KRITIS-G Schweiz, NIS2-Anpassungen
- Cyber-Versicherung prüfen & optimieren

Frameworks & Standards zur Umsetzung

ISO/IEC 27001:2022

- Deckt ~70–80% der NIS2-Anforderungen ab
- Stärkster Einzelnachweis in CH, LI und DE
- Anerkannt als Sorgfaltspflichtmassstab vor Gericht
- Pflichthafte Management-Review-Zyklen (Kap. 9.3)
- Zertifizierung durch akkreditierte Stelle empfohlen

IKT-Minimalstandard BACS (CH)

- 108 Massnahmen auf Basis NIST CSF – freiwillig aber massgeblich
- Schwellen: Identify, Protect, Detect, Respond, Recover
- Obligatorisch für Strom- und Gasbranche
- Geplante KRITIS-G Schweiz orientiert sich an NIS2 + IKT-Minimalstandard
- Best Practice für CH-Gerichte als Sorgfaltsmassstab

NIST CSF 2.0

- Neu: Governanz-Funktion (GV) als 6. Säule
- International anerkannt, kein Zertifikat, aber Strukturgeber
- NIS2 Mapping: GV.RM = Art. 21(a), RS.MA = Art. 21(b)
- BSI IT-Grundschutz deckt NIS2 ebenfalls vollständig ab
- Für KMU: **BSI Basis-Absicherung** als pragmatischer Einstieg

Weitere Informationen unter: **nis2-audit.ch**

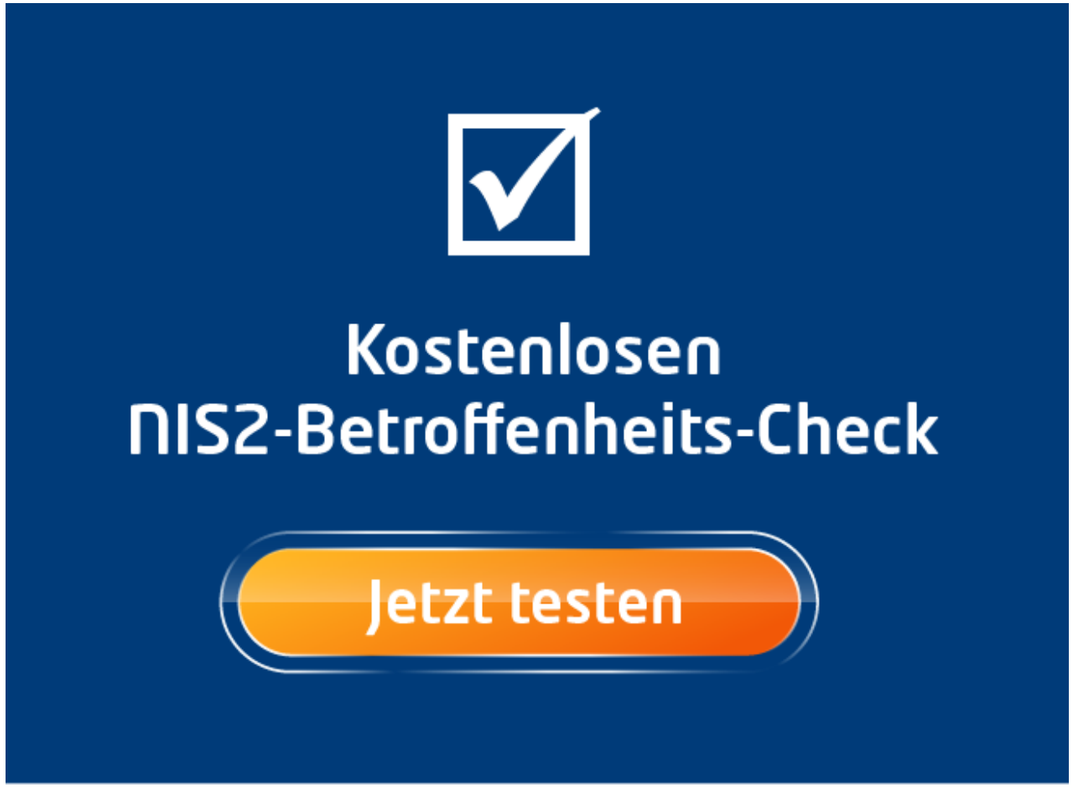
Kontakt

Crisanto Farese

NIS2-Audit für Stiftungen & KMU

+41 41 748 60 10 | crisanto.farese@profetas.ch

nis2-audit.ch **nis2-schweiz.ch**



Quellenverzeichnis

EU Legal Basis

NIS2 Directive (EU 2022/2555): https://eur-lex.europa.eu/eli/dir/2022/2555/oj

Implementing Regulation (EU 2024/2690) (Minimum Measures Art. 21): https://eur-lex.europa.eu/eli/reg_impl/2024/2690/oj

ENISA (EU Agency for Cybersecurity): https://www.enisa.europa.eu/

NIS2 Directive Portal (ENISA): https://www.enisa.europa.eu/topics/cybersecurity-policy/nis-directive-new

Swiss Legal Basis

Revised Data Protection Act (revDSG, SR 235.1): https://www.fedlex.admin.ch/eli/cc/2022/491/de

Information Security Act (ISG, SR 128): https://www.fedlex.admin.ch/eli/cc/2022/232/de

Ordinance to the ISG (ISV): https://www.fedlex.admin.ch/eli/cc/2023/735/de

Code of Obligations Art. 754 OR (Responsibility of Organs): https://www.fedlex.admin.ch/eli/cc/27/317_321_377/de#art_754

Civil Code Art. 84 ZGB (Foundation Oversight): https://www.fedlex.admin.ch/eli/cc/24/233_245_233/de#art_84

KRITIS Reporting Obligation / BACS: https://www.ncsc.admin.ch/ncsc/de/home/cyberbedrohungen/meldepflicht.html

Liechtenstein

Cybersecurity Act (CSG): https://www.gesetze.li/ (Search term "Cybersicherheit")

Persons and Company Law (PGR): https://www.gesetze.li/konso/1926007000

CSIRT.LI: https://www.csirt.li/

Office of IT / Cybersecurity LI: https://www.llv.li/

Germany

NIS2 Implementation and Cybersecurity Strengthening Act (NIS2UmsuCG): https://www.bmi.bund.de/ (Keyword NIS2UmsuCG)

Federal Office for Information Security (BSI): https://www.bsi.bund.de/

BSI IT-Grundschutz Compendium: https://www.bsi.bund.de/IT-Grundschutz

BSI NIS2 Impact Assessment: https://www.bsi.bund.de/DE/Themen/Regulierte-Wirtschaft/NIS-2-regulierte-Unternehmen/nis-2-regulierte-unternehmen_node.html

Quellenverzeichnis

Standards and Frameworks

ISO/IEC 27001:2022: https://www.iso.org/standard/27001

ISO/IEC 27002:2022 (Controls): https://www.iso.org/standard/75652.html

NIST Cybersecurity Framework 2.0: https://www.nist.gov/cyberframework

ICT Minimal Standard BACS: https://www.ncsc.admin.ch/ncsc/de/home/dokumentation/ikt-minimalstandard.html

SOC 2 (AICPA): https://www.aicpa-cima.com/topic/audit-assurance/audit-and-assurance-greater-than-soc-2

Authorities and Reporting Offices

BACS (Federal Office for Cybersecurity, Switzerland): https://www.ncsc.admin.ch/ / https://www.bacs.admin.ch/

BSI (Germany): https://www.bsi.bund.de/

CSIRT.LI (Liechtenstein): https://www.csirt.li/

Federal Data Protection and Information Commissioner (FDPIC): https://www.edoeb.admin.ch/

European Data Protection Board (EDPB): https://www.edpb.europa.eu/

Further Resources

Nis2-Audit.ch (Project Info): https://nis2-audit.ch/

swissICT (Association): https://www.swissict.ch/

SwissCyberSecurity.net (News): https://www.swisscybersecurity.net/

Digital Security Alliance Switzerland: https://www.digitale-sicherheit.ch/

Swiss Cyber Forum: https://swisscyberforum.com/

Citation Recommendation

Bitte beachten Sie die einzelnen Artikel mit der vollständigen Rechtsquelle (SR-Nummer CH, ELI-Link EU, LR-Nummer LI). Links gültig ab: April 2026. Die Gültigkeit der URLs sollte vor der Veröffentlichung überprüft werden.

Glossar, NIS2-Kernbegriffe

Wesentliche Einrichtung (Essential Entity, Art. 3 Abs. 1 NIS2): Grössere Unternehmen in kritischen Sektoren (ab 250 MA oder 50 Mio. EUR Umsatz) sowie qualifizierte Anbieter unabhängig von der Grösse (z. B. Vertrauensdienste, TLD-Registries, DNS-Dienste). Unterliegen Vorab-Aufsicht, Bussen bis 10 Mio. EUR oder 2 Prozent des globalen Konzernumsatzes.

Wichtige Einrichtung (Important Entity, Art. 3 Abs. 2 NIS2): Mittelgrosse Unternehmen (ab 50 MA oder 10 Mio. EUR Umsatz) in kritischen oder relevanten Sektoren. Nachgelagerte Aufsicht, Bussen bis 7 Mio. EUR oder 1,4 Prozent Konzernumsatz.

Artikel 21 NIS2 (Risk-Management Measures): Zehn verbindliche Mindestmassnahmen: Risikoanalyse, Incident Handling, Business Continuity, Supply Chain Security, Acquisition/Development/Maintenance, Wirksamkeitsbewertung, Cyberhygiene/Training, Kryptografie, HR-Sicherheit und Zugangskontrolle, MFA und sichere Kommunikation.

Artikel 23 NIS2 (Meldepflichten): Dreistufige Meldung bei "significant incidents": Frühwarnung innerhalb 24h, Vorfallmeldung innerhalb 72h, Abschlussbericht innerhalb 1 Monat. Zwischenmeldung bei langanhaltenden Vorfällen.

Artikel 20 Abs. 2 NIS2 (Management-Verantwortung): Leitungsorgane müssen Cybersicherheits-Schulungen nachweislich absolvieren. Keine Delegation auf IT möglich.

Significant Incident: NIS2-Schwellenwert für Meldepflicht: erhebliche Betriebsstörung, finanzieller Schaden, Beeinträchtigung Dritter durch materielle oder immaterielle Schäden. Konkretisiert durch Durchführungsverordnung (EU) 2024/2690.

Zwangsgelder (Periodic Penalty Payments, Art. 34 NIS2): Tägliche Strafzahlungen bei fortgesetzter Non-Compliance, in DE bis CHF/EUR 100'000 pro Tag.

Funktionssperre (Art. 32 Abs. 5 NIS2): Behördliche Befugnis zum vorübergehenden Berufsverbot für CEO oder Legal Representative. EU bis unbegrenzte Dauer während Verstoss, LI bis 3 Jahre bei Wiederholung.

NIS2-Kooperationsgruppe: EU-Gremium (Kommission, ENISA, Mitgliedstaaten) für Abstimmung von Durchsetzung, Supply-Chain-Risikobewertungen und Peer Reviews.

Glossar, CH & Liechtensteinische Rechtsbegriffe

Adäquate Datensicherheit (Art. 8 revDSG): Unbestimmter Rechtsbegriff. Mindestmassstab sind technische und organisatorische Massnahmen (TOM) gemäss Art. 1-6 DSV. Gerichtspraxis zieht ISO 27001 und IKT-Minimalstandard als Konkretisierung heran.

Beweislastumkehr (Art. 754 OR i. V. m. Haftungspraxis): Nach eingetretenem Schaden muss der beklagte Verwaltungsrat / Stiftungsrat selbst beweisen, dass er sorgfältig gehandelt hat. Ohne dokumentierten ISMS- und Governance-Nachweis kaum zu führen.

Sorgfaltsmassstab objektiv (Art. 717 OR, Art. 84 ZGB): Gemessen wird nicht am individuellen Wissensstand, sondern an dem, was ein "ordentlicher und gewissenhafter" Organträger in vergleichbarer Lage gewusst hätte. Unwissenheit in IT-Fragen schützt nicht.

Business Judgment Rule (BJR, Art. 182 PGR Liechtenstein): Haftungsprivileg: kein Verschuldensvorwurf, wenn Organ auf Basis angemessener Information, ohne Interessenkonflikt und zum Wohl der Gesellschaft entschieden hat. In CH richterrechtlich anerkannt, aber nicht kodifiziert.

KRITIS-Meldepflicht (Art. 74a ff. revISG / ab 2024): Schweizer Betreiber kritischer Infrastrukturen melden Cyberangriffe innerhalb 24h ans BACS, schriftlicher Ergänzungsbericht innerhalb 14 Tagen. Verstoss: bis CHF 100'000 Busse.

Bussgeldrahmen revDSG: Bis CHF 250'000 direkt gegen natürliche Personen (Art. 60 ff. revDSG), nicht gegen die juristische Person. Keine D&O-Deckung bei Vorsatz.

Art. 754 OR: Verantwortlichkeitsklage gegen Verwaltungsrat. Unlimitierte Solidarhaftung mit Privatvermögen bei Pflichtverletzung, Schaden und Kausalität.

Art. 84 ZGB: Stiftungsaufsicht. Aufsichtsbehörde kann Stiftungsräte bei Pflichtverletzung abberufen und zu Schadenersatz verpflichten.

Glossar, Standards und Frameworks

ISO/IEC 27001:2022: Zertifizierbarer ISMS-Standard. 93 Controls in Annex A, gruppiert in vier Themen: Organisation, Personen, Physisch, Technisch. Deckt 70-80 Prozent von Art. 21 NIS2 ab. Pflichtkapitel 4-10 (Kontext, Leadership, Planung, Support, Betrieb, Bewertung, Verbesserung).

ISO/IEC 27002:2022: Begleitstandard mit Implementierungsleitfaden zu den 93 Controls. Nicht zertifizierbar, aber massgebend für Prüfer.

NIST CSF 2.0: Sechs Funktionen: Govern (neu), Identify, Protect, Detect, Respond, Recover. Strukturgeber ohne Zertifizierung. Mapping auf NIS2: Govern/RM-Kategorie deckt Art. 21(a), Respond/MA deckt Art. 21(b).

IKT-Minimalstandard (BACS): 108 Massnahmen basierend auf NIST CSF, in drei Reifegraden. Freiwillig ausser für Strom- und Gasbranche (StromVG, GasVG). Gilt vor Schweizer Gerichten als Konkretisierung der Sorgfaltspflicht.

BSI IT-Grundschutz: Methodik mit Bausteinen, Gefährdungen und Anforderungen in drei Stufen: Basis, Standard, Kern. Basis-Absicherung als pragmatischer KMU-Einstieg. Deckt NIS2-Anforderungen vollständig ab.

SOC 2 (AICPA Trust Services Criteria): Type I prüft Kontrolldesign zu einem Stichtag, Type II prüft Wirksamkeit über 6-12 Monate. Fünf Kriterien: Security (Pflicht), Availability, Processing Integrity, Confidentiality, Privacy. Wird in Supply-Chain-Audits häufig als Alternative zu ISO 27001 akzeptiert.

CIS Controls v8: 18 priorisierte Sicherheitsmassnahmen. Implementation Group 1 als Minimum für kleine Organisationen, IG2/IG3 für grössere. Oft als Mapping-Basis zwischen Frameworks genutzt.

Glossar, Meldewesen & Incident Response

ISMS (Information Security Management System): Dokumentiertes Gesamtsystem aus Policies, Prozessen, Rollen, Risikoregister und Wirksamkeitskontrollen. Kein Tool, sondern Managementsystem mit PDCA-Zyklus.

IRP (Incident Response Plan): Dokumentiertes Playbook mit Rollen (Incident Commander, Kommunikation, Forensik), Eskalationsmatrix, Meldewegen (intern/extern/Behörden), Kommunikationsvorlagen. Muss die 24h-Meldefähigkeit technisch und organisatorisch sicherstellen.

CSIRT (Computer Security Incident Response Team): Behördliches oder internes Response-Team. In der EU koordinieren nationale CSIRTs die Meldungen unter NIS2.

Tabletop-Übung: Moderiertes Durchspielen eines Incident-Szenarios ohne technische Aktion. Testet Kommunikation, Entscheidungswege und Meldefähigkeit auf Management-Ebene. Ergebnis wird protokolliert (Nachweis Sorgfalt).

RTO / RPO (Recovery Time / Point Objective): Zielwerte für Business Continuity: RTO ist die zulässige Ausfallzeit, RPO der zulässige Datenverlust. Müssen pro kritischem Prozess definiert und regelmässig getestet sein.

Backup 3-2-1-Regel: Drei Kopien, zwei Medien, eine offsite/offline. Offline-Backup (Air Gap) ist nach aktueller Audit-Praxis faktisch Pflicht wegen Ransomware.

BCM / DRP (Business Continuity Management / Disaster Recovery Plan): BCM umfasst die gesamten geschäftlichen Fortführungsmassnahmen, DRP ist die IT-technische Wiederherstellung. Art. 21(c) NIS2 verlangt beides.

Glossar, Technische Sicherheitsmassnahmen

MFA phishing-resistent: Authentisierung gegen Phishing-Angriffe immun. Erfüllbar nur mit FIDO2/WebAuthn, Passkeys oder Smartcards. SMS-OTP, TOTP-Apps und Push-Bestätigungen gelten nicht als phishing-resistent.

Zero Trust: Architektur-Prinzip "never trust, always verify". Jeder Zugriff wird unabhängig vom Netzwerkstandort authentisiert, autorisiert und verschlüsselt. NIS2 verlangt zwar nicht explizit Zero Trust, faktisch aber dessen Kerninhalte (Segmentierung, MFA, Least Privilege).

Least Privilege / PoLP: Prinzip minimaler Rechte. Umfasst Just-in-Time Admin, tiered admin accounts, regelmässige Access Reviews. Schnelle Sperrung bei Austritt (Art. 21(i) NIS2).

PAM (Privileged Access Management): Kontrollierter Zugriff auf privilegierte Konten über Vault, Session Recording und Just-in-Time-Rechte. Audit-kritisch.

SIEM (Security Information and Event Management): Zentrale Sammlung, Korrelation und Alarmierung von Sicherheitsereignissen aus allen Quellen. Basis für Detect-Fähigkeit.

EDR / XDR (Endpoint / Extended Detection and Response): Verhaltensbasierte Erkennung auf Endpoints (EDR) oder plattformübergreifend (XDR). Ersetzen klassischen AV als Erkennungsschicht.

SOC (Security Operations Center): 24/7-Überwachung durch geschultes Personal. Managed SOC als Outsourcing-Variante für mittelständische Organisationen.

SBOM (Software Bill of Materials): Maschinenlesbare Stückliste aller in einer Software enthaltenen Komponenten (SPDX oder CycloneDX). Zunehmend gefordert für Supply-Chain-Transparenz, verpflichtend nach Cyber Resilience Act (CRA).

Asset-Inventar / CMDB: Vollständiges Register aller Hardware, Software, Daten und Services inkl. Owner und Kritikalität. Ohne Asset-Inventar kein Risikomanagement, kein Patch Management, keine Audit-Bestehensfähigkeit.

Patch Management: Dokumentierter Prozess: Inventarisierung, Schwachstellen-Scan, Priorisierung (CVSS), Test, Rollout, Verifikation, Ausnahmedokumentation. SLA pro Kritikalitätsstufe.

Vulnerability Management: Kontinuierlicher Zyklus aus Scanning, Bewertung, Remediation und Reporting. CVE- und CVSS-basiert.

Penetrationstest: Zielgerichteter Angriff durch autorisierte Tester (Black/Grey/White Box). Ergänzt, ersetzt aber keine Schwachstellenscans. Mindestens jährlich, nach wesentlichen Änderungen und auf Kundenwunsch.

Red Team / Purple Team: Red Team simuliert realen Angreifer inkl. Social Engineering und physischer Intrusion. Purple Team kombiniert Red und Blue Team zur unmittelbaren Detect-Verbesserung.

Cyberhygiene (Art. 21(g) NIS2): Grundlegende Praktiken: Awareness-Trainings, Passwort-Hygiene, Update-Disziplin, Berechtigungsreviews, Clean-Desk. Dokumentationspflicht.

AES-256 / TLS 1.2+ / TLS 1.3: Pflicht-Kryptografie nach Art. 21(h) NIS2. AES-256 für Data at Rest, TLS 1.3 für Data in Transit (1.2 noch akzeptiert, SSL/TLS 1.0/1.1 nicht mehr).

DNSSEC / DoH / DoT: Absicherung der DNS-Auflösung: DNSSEC gegen Manipulation, DoH/DoT gegen Abhören. DNS-Provider sind unter NIS2 als Vertrauensdienst reguliert.

Vertrauensdienst (eIDAS / Art. 3 eIDAS-VO): Qualifizierte elektronische Signatur, Siegel, Zeitstempel, Zustellung, Website-Authentisierung. Anbieter unterliegen NIS2 als wesentliche Einrichtung unabhängig von der Grösse.

Glossar, Supply Chain und Audit

Supply Chain Security (Art. 21(d) NIS2): Sicherheitsanforderungen werden vertraglich an Lieferanten weitergegeben. Umfasst Lieferantenregister, Risikobewertung pro Lieferant, Audit-Rechte, Exit-Klauseln, SBOM-Pflicht.

TPRM (Third Party Risk Management): Programm zur laufenden Bewertung aller Drittparteien nach Kritikalität. Tiering (Tier 1-3) nach Datenzugriff und Business-Abhängigkeit.

Gap-Analyse: Strukturierter Soll-Ist-Abgleich gegen einen Zielrahmen (ISO 27001 Annex A, Art. 21 NIS2 oder IKT-Minimalstandard). Ergebnis: priorisierte Remediation Roadmap.

Scoping-Check (Betroffenheitsprüfung): Strukturierte Prüfung, ob und in welcher Rolle (wesentlich/wichtig, direkt/indirekt) eine Organisation unter NIS2 oder Schweizer KRITIS-Regime fällt. Grundlage für die weitere Roadmap.

Shadow IT: Ohne IT-Freigabe genutzte Systeme, SaaS-Tools oder Geräte. Nicht inventarisiert, nicht gepatcht, nicht überwacht. Primäres Einfallstor in Audits.

Management-Review (ISO 27001 Kap. 9.3): Mindestens jährliche formale Bewertung der ISMS-Wirksamkeit durch die Geschäftsleitung. Protokolliert. Fehlende Reviews sind häufigster "Major Non-Conformity" in Audits.

D&O-Versicherung (Directors & Officers): Organhaftpflicht. Deckt fahrlässige Pflichtverletzungen, nicht aber Vorsatz, Bussen persönlichen Charakters oder bewusste Untätigkeit. Police-Lektüre pre-incident dringend empfohlen.