



Compliance ist kein Ordner

Von NIS2 und Governance zu echter Cyber-Resilienz

Crisanto Farese

Marc Lanz

DAS PROBLEM

Papier ist nicht Betrieb



Auf dem Papier

- Reglemente vorhanden
- Policies unterschrieben
- Zuständigkeiten definiert
- Auditor hat genickt



Montag, 09:17 Uhr

Wer weiss jetzt konkret, was das Reglement bedeutet? Wer entscheidet, wer sperrt, wer sieht die Logs?

CRISANTO · DER RAHMEN

Woher der Druck kommt



NIS2 / EU

Nachweispflicht, Lieferketten-Verantwortung, persönliche Haftung des Managements.



Schweiz

Kein direkter EU-Zwang. ISG, revDSG und faktischer Druck über Partner und Märkte.



Stiftungen & KMU

Sensible Daten, kleine Teams, externe IT. Verantwortung liegt bei Stiftungsrat und GL.



Kunden, Banken, Versicherer

Ausschreibungen, Verträge und Policen verlangen den Nachweis, nicht das Versprechen.

CRISANTO · RECHTSLAGE

Was gilt wo?

Schweiz

Eigenständiges Recht

- revDSG, ISG, KRITIS-Meldepflicht (seit 1.4.2025)
- 24h Meldung ans BACS, 14 Tage Ergänzungsbericht
- NIS2 gilt nicht direkt, wirkt aber faktisch

Liechtenstein

NIS2 vollständig umgesetzt

- CSG seit 1.2.2025 (EWR)
- 24h Frühwarnung, 72h Vorfallmeldung, 1 Monat Bericht an CSIRT.LI
- Management-Schulung ist Pflicht (Art. 20 Abs. 2)

Deutschland

NIS2-pflichtig

- NIS2UmsuCG seit 1.3.2025
- Gleiches 3-Stufen-Meldesystem ans BSI
- Management-Schulung ist Pflicht (Art. 20 Abs. 2)

CRISANTO · DER DOMINO-EFFEKT

NIS2 kommt über den Vertrag ins Haus

1

EU-Unternehmen (KRITIS)

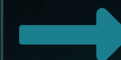
muss gemäss Art. 21 NIS2 die
Sicherheit seiner Lieferkette garantieren



2

Vertragliche Weitergabe

Anforderungen wandern in Verträge mit
Schweizer Zulieferern und
Dienstleistern



3

Schweizer Stiftung / KMU

faktische Pflicht: wer nicht NIS2-ready
ist, verliert den Auftrag

Dazu kommt der inländische Druck: revDSG seit 2023, ISG seit 2024, KRITIS-Meldepflicht seit 2025. Marktforderungen übersteigen zunehmend die reine Inlandsgesetzgebung.

CRISANTO · STIFTUNGEN

Stiftungen: besonders exponiert

13'721

Stiftungen in der Schweiz

24h

Meldefrist bei Cyberangriffen (ISG, BACS)

CHF 100k

Busse gegen die natürliche Person, Art. 74h ISG

31.12.2026

ISMS-Pflicht für betroffene Organisationen

Betroffen ist eine Stiftung, die ...

- sensible Daten verwaltet: Spender, Destinatäre, Gesundheit
- IT- oder Cloud-Services nutzt, oft komplett ausgelagert
- im Gesundheits-, Sozial- oder Finanzsektor tätig ist
- EU-Niederlassungen, Projektträger oder EU-Kunden hat
- ehrenamtliche Räte ohne IT-Kompetenz hat, ohne Aktionäre als Korrektiv

CRISANTO · SANKTIONEN UND HAFTUNG

Was auf dem Spiel steht

EU / LI · WESENTLICH

CHF 10 Mio.

oder 2% des weltweiten Jahresumsatzes

Zwangsgelder bis CHF 100'000 pro Tag, bis 3 Jahre Funktionssperre für das Management

EU / LI · WICHTIG

CHF 7 Mio.

oder 1,4% des weltweiten Jahresumsatzes

Persönliche Haftung Stiftungsrat und GF.
Keine D&O-Deckung bei Vorsatz

SCHWEIZ

CHF 250'000

revDSG, direkt gegen natürliche Personen

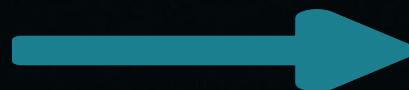
Art. 754 OR: unlimitierte Privathaftung mit Beweislastumkehr. CHF 100'000 bei KRITIS-Nichtmeldung

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

CRISANTO · DER SHIFT

Verantwortung wandert nach oben

«Das macht die IT»



**Geschäftsleitung
Stiftungsrat
Verwaltungsrat**

«Compliance ist nicht die Aufgabe, alles zu wissen. Compliance ist die Pflicht, Risiken angemessen zu erkennen, zu steuern und nachvollziehbar zu handeln.»

MARC · REALITÄTSCHECK

Ein ganz normaler Fall

Eine Stiftung. Spenderdaten, Stiftungsratsunterlagen, Cloud, externe IT. Auf dem Papier alles gut.



Privates Notebook

noch eingeloggt



Ex-Mitarbeiter

hat noch Zugriff



Cloud-Ordner

falsch geteilt



Dienstleister

kompromittiert

Das Risiko war nie unsichtbar. Es war nur nie operationalisiert.

DIE BRÜCKE

Drei Fragen, drei Ebenen

Theoretische Compliance

Welche Pflichten haben wir?

Operative Compliance

Wer macht was, wann, mit welchem Nachweis?

Cyber-Resilienz

Was passiert, wenn trotzdem etwas schiefgeht?

MARC · DAS FUNDAMENT

Die fünf Bausteine



Inventar

Man schützt nur,
was man kennt.



Zugriff

Wer darf was,
warum, wie lange?



Logging

Nachvollziehen,
was passiert ist.



Reaktion

Funktioniert es
unter Stress?



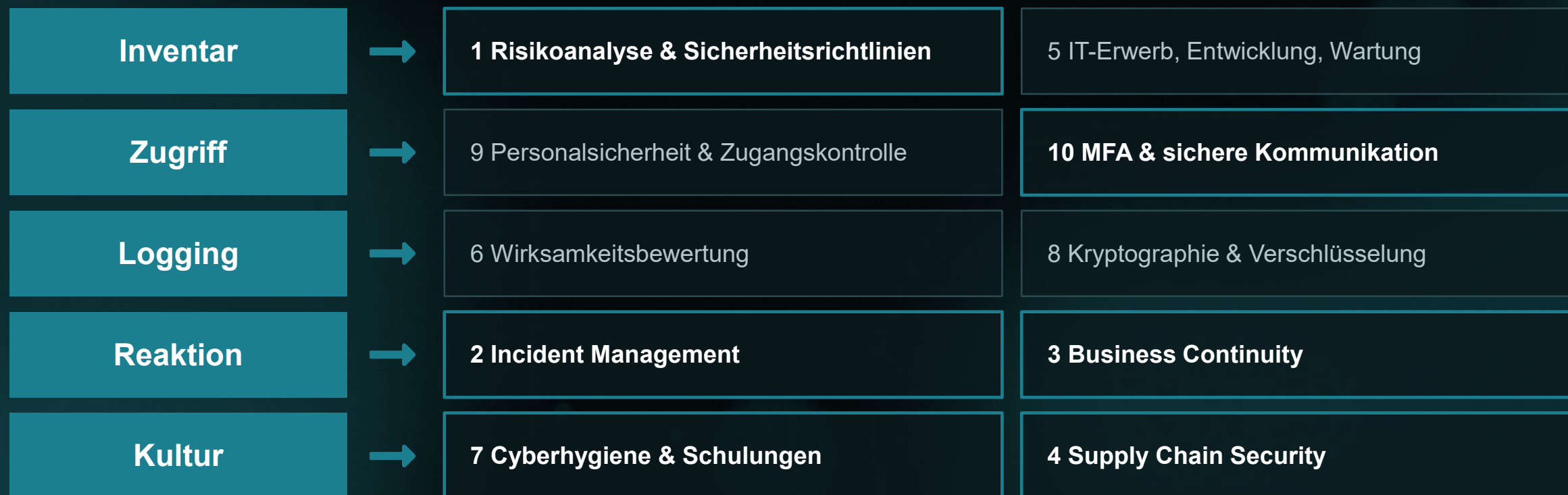
Kultur

Wissen, was tun.
Ohne 80 Seiten.

Eine Organisation ist resilient, wenn sie weiss, was sie besitzt, wer Zugriff hat, was kritisch ist und wie sie unter Druck entscheidet.

MARC · DER ANKER INS GESETZ

Art. 21 NIS2 auf fünf Bausteinen



Zehn Mindestmassnahmen, Art. 21 NIS2. Verbindlich in EU und LI, als Best Practice und Sorgfaltsmassstab in der Schweiz. Hervorgehoben: in Audits am häufigsten unzureichend.

GEMEINSAM · DIE ÜBERSETZUNG

Pflicht → Praxisfrage → Massnahme

Die Pflicht (Crisanto)	Die Praxisfrage (Marc)	Die Massnahme (Marc)
Wir müssen Risiken kennen	Haben wir ein aktuelles Asset- und Dateninventar?	Asset Register, Datenklassifikation, Dienstleisterliste
Wir müssen Zugriff kontrollieren	Wer hat Adminrechte, und warum eigentlich?	MFA, Rollenmodell, Offboarding, privilegierte Konten
Wir müssen Vorfälle melden können	Woran erkennen wir überhaupt einen Vorfall?	Logging, Monitoring, Incident Playbook
Wir müssen Lieferanten steuern	Welche Dienstleister hängen an kritischen Daten?	Vendor Due Diligence, Vertragsklauseln, Zugriffskontrolle
Wir müssen nachweisen können	Wo liegt der Nachweis, wenn jemand fragt?	Tickets, Protokolle, Audit-Trail, Schulungsnachweise

GEMEINSAM · DIE ÜBERSETZUNG

Basic Checks - Beispiel

aphasie.org

Scanne öffentliche DNS-Einträge...

SPF

OK

DKIM

SIGNIERT NICHT

DMARC

FEHLT

MX

Microsoft 365

RISIKO HOCH

Score 4

Absender-Spoofing ist nicht zuverlässig abgesichert.

prixo.ch

Scanne öffentliche DNS-Einträge...

SPF

OK

DKIM

AKTIV

DMARC

NUR MONITORING

MX

Microsoft 365

RISIKO TIEF

Score 1

Grundschutz aktiv. DMARC-Durchsetzung noch ausstehend.

GEMEINSAM · DIE ÜBERSETZUNG

3 Min. Check

<https://emitec-datacom.ch/nis2>



Kostenlosen NIS2-Betroffenheits-Check

Jetzt testen

NIS2-Readiness-Check

Frage 3 von 8

Ist Ihr Unternehmen in der Europäischen Union tätig?

Tochtergesellschaft, Kunden, Zuliefererrolle, EU-Förderprojekte etc.

- ☒ Ja, wir haben eine Tochtergesellschaft in der EU
- ☐ Ja, wir erbringen wesentliche Dienstleistungen für EU-Kunden
- ☐ Ja, wir sind Zulieferer für kritische EU-Infrastruktur
- ☐ Ja, aber nur marginales EU-Geschäft (unter 10% des Umsatzes)
- ☐ Nein, wir sind ausschliesslich in der Schweiz tätig

← Zurück

Weiter →



Vorbereitung dringend empfohlen.

Ihre Angaben deuten darauf hin, dass Ihr Unternehmen entweder bereits von der EU-NIS2-Richtlinie betroffen sein könnte (bei EU-Geschäft) oder von kommenden Schweizer Cyber-Regulierungen erfasst wird.

Konkret bedeutet das

- **EU-Geschäft:** NIS2-Konformität voraussichtlich bereits erforderlich.
- **Nur Schweiz:** Der Bundesrat prüft NIS2-äquivalente Regelungen, Inkrafttreten 2025/2026 erwartet.
- **In beiden Fällen:** Vorbereitung dauert 6 bis 12 Monate und erfordert substanzielle Investitionen.

Risiken bei Nichteinhaltung

- EU-NIS2: Bussen bis EUR 10 Mio. oder 2% des weltweiten Umsatzes.
- Schweiz (ISG Art. 74h): persönliche Bussen bis CHF 100'000.
- **Persönliche Haftung der Geschäftsleitung** in beiden Rechtsräumen möglich.
- Reputationsschaden und Vertrauensverlust bei Kunden, Spendern, Destinatären.

Gut zu wissen: Schweizer Unternehmen mit EU-Tochter oder wesentlichen EU-Dienstleistungen müssen NIS2 direkt umsetzen. Auch rein Schweizer Unternehmen in kritischen Sektoren sollten sich vorbereiten, die Schweiz wird voraussichtlich äquivalente Regeln einführen.

Betroffenheit klären und rechtzeitig starten

Klarheit schaffen über die Auswirkungen von NIS2, ISG und nDSG auf Ihre Organisation.

Vor- und Nachname *

TAKE-AWAY

Der 30-Tage-Startpunkt

Fünf Fragen für die nächsten 30 Tage. Sie entsprechen Phase 1 des profetas Handlungsplans: MFA, Backup-Restore-Test, Verantwortlichkeit in der GL, Notfallkontakte, Shadow IT.

- ☐ Welche Systeme und Daten sind wirklich kritisch?
- ☐ Wer hat Zugriff darauf?
- ☐ Welche externen Dienstleister hängen daran?
- ☐ Wie erkennen wir einen Vorfall?
- ☐ Wer entscheidet im Ernstfall innerhalb der ersten Stunde?

Zielbild: Klarheit

- über Daten
- über Systeme
- über Verantwortlichkeiten
- über Dienstleister
- über Entscheidungswege
- über den Ernstfall



Handlungsfähig im Ernstfall?

Wer entscheidet?

Wer sieht die Logs?

Wer sperrt Zugriffe?

Wer kommuniziert?

Wer dokumentiert?

Crisanto Farese · Marc Lanz

profetas.ch · Stiftungsexperten auf Zeit · Governance · Compliance · Cybersecurity