DISCOVER THE SPIR.iT OF EXCELLENCE.
SURPASS YOUR SUCCESS.

NIS-2 – vom Gesetzestext zur Umsetzung:
Was Unternehmer*innen jetzt konkret tun

Vortrag im Rahmen der Veranstaltung der IHK Regensburg zum Thema:
Neue Cybersicherheitspflichten für Unternehmen – Was Unternehmer*innen jetzt über die neue EU-Richtlinie NIS-2 wissen müssen

Tobias Rademann
8. Juli 2026

Wir ***sind*** betroffen –
was müssen wir jetzt ***konkret*** tun?

Agenda

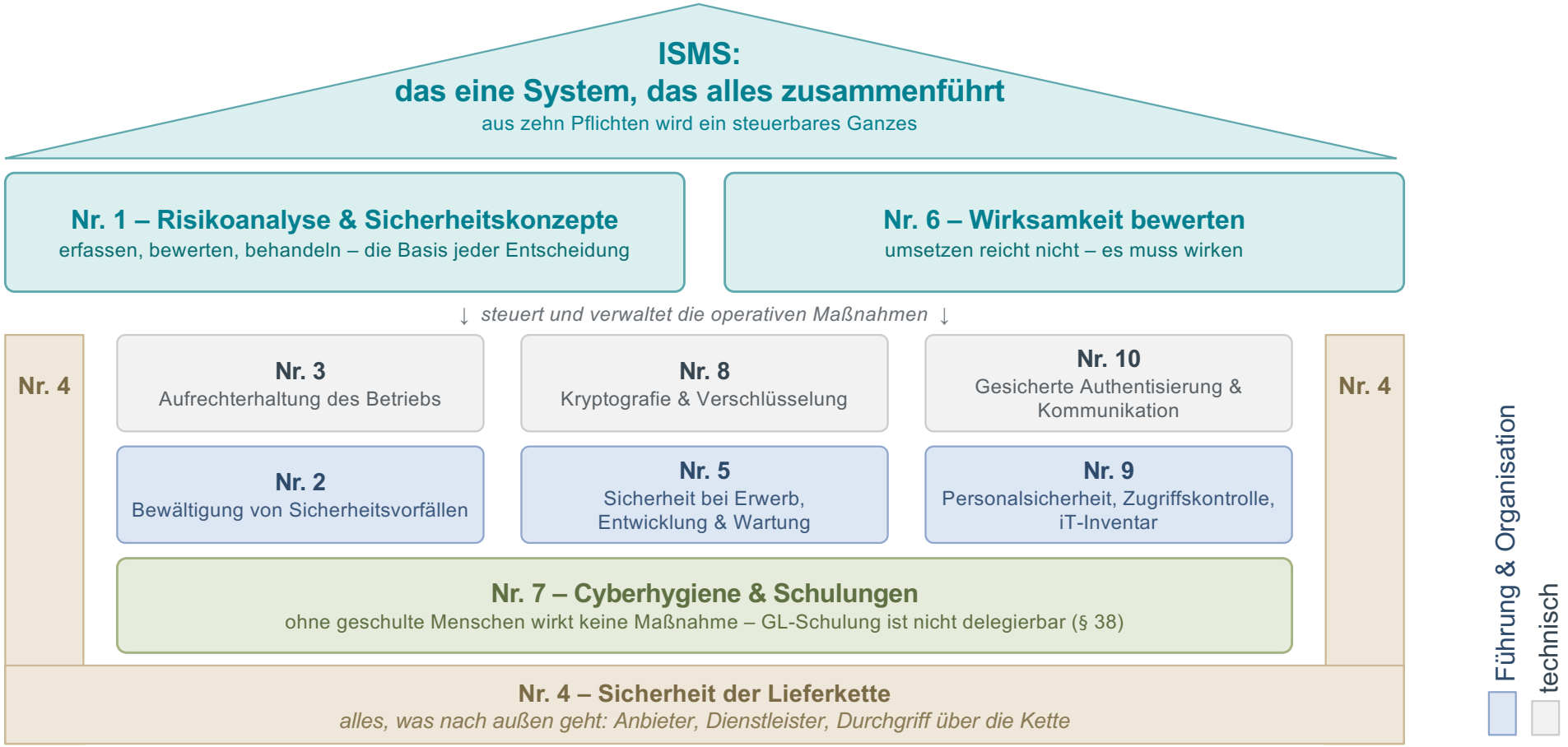
- ✓ Was jetzt auf Sie zukommt
- ✓ Was Sie absichern müssen
- ✓ Zuerst: **registrieren**
- ✓ Wenn es passiert: **melden**
- ✓ Müssen Sie das **nachweisen**?
- ✓ So fangen Sie an
- ✓ Was Sie mitnehmen


Was jetzt auf Sie zukommt

Das verlangt § 30 BSIG von Ihnen

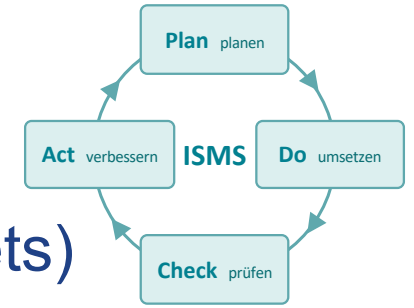
1. **Risikoanalyse & Sicherheitskonzepte**
   Risikobehandlung
2. **Bewältigung von Sicherheitsvorfällen**
   Erkennen, reagieren, wiederherstellen
3. **Aufrechterhaltung des Betriebs**
   Backup, Disaster Recovery, BCM
4. **Sicherheit der Lieferkette**
   Anbieter & Dienstleister
5. **Sicherheit bei Erwerb, Entwicklung & Wartung**
   inkl. Schwachstellenmanagement
6. **Wirksamkeit bewerten**
   Wirkt es wirklich? – regelmäßig überprüfen
7. **Cyberhygiene & Schulungen**
   Basispraktiken + Security-Awareness
8. **Kryptografie & Verschlüsselung**
   Konzepte und Verfahren
9. **Personalsicherheit & Zugriffskontrolle**
   inkl. Personal, Zugriffsrechte, iT-Inventar
10. **Gesicherte Authentisierung & Kommunikation**
    sichere Anmeldung und Kommunikation

Vom Katalog zum System:



Was ist ein ISMS?

- ✓ ISMS = **I**nformations**s**icherheits**m**anagement**s**ystem
- ✓ § 30 nennt ISMS nicht – verlangt aber genau das:
  ein **System**, das **entscheidet, prüft, steuert**
  → Rahmen aus Regeln, Rollen, Abläufen
  – bezogen auf Ihre schützenswerten Werte (Assets)
- ✓ fortlaufender Prozess (kein Projekt)
- ✓ macht Sicherheit steuerbar: Risiko → Maßnahme → Wirksamkeit
- ✓ zuerst Führung, dann Technik



Der PDCA-Zyklus – bekannt aus dem Qualitätsmanagement

ISMS: Ihr Nutzen

zehn Einzelpflichten	einmal absichern	getan
↓	↓	↓
ein steuerbares Ganzes	**dauerhaft wirksam bleiben**	**belegt** dokumentiert, was warum geschieht

Vieles ist bei Ihnen schon da – oft >3 von 10.
Das ISMS macht daraus ein System: bewerten, priorisieren, steuern.

Wer ist verantwortlich?

Das können *andere* für Sie tun:

Umsetzung

Technik · Prozesse · Dokumentation

→ intern oder mit Partnern

Das bleibt bei Ihnen (§ 38):

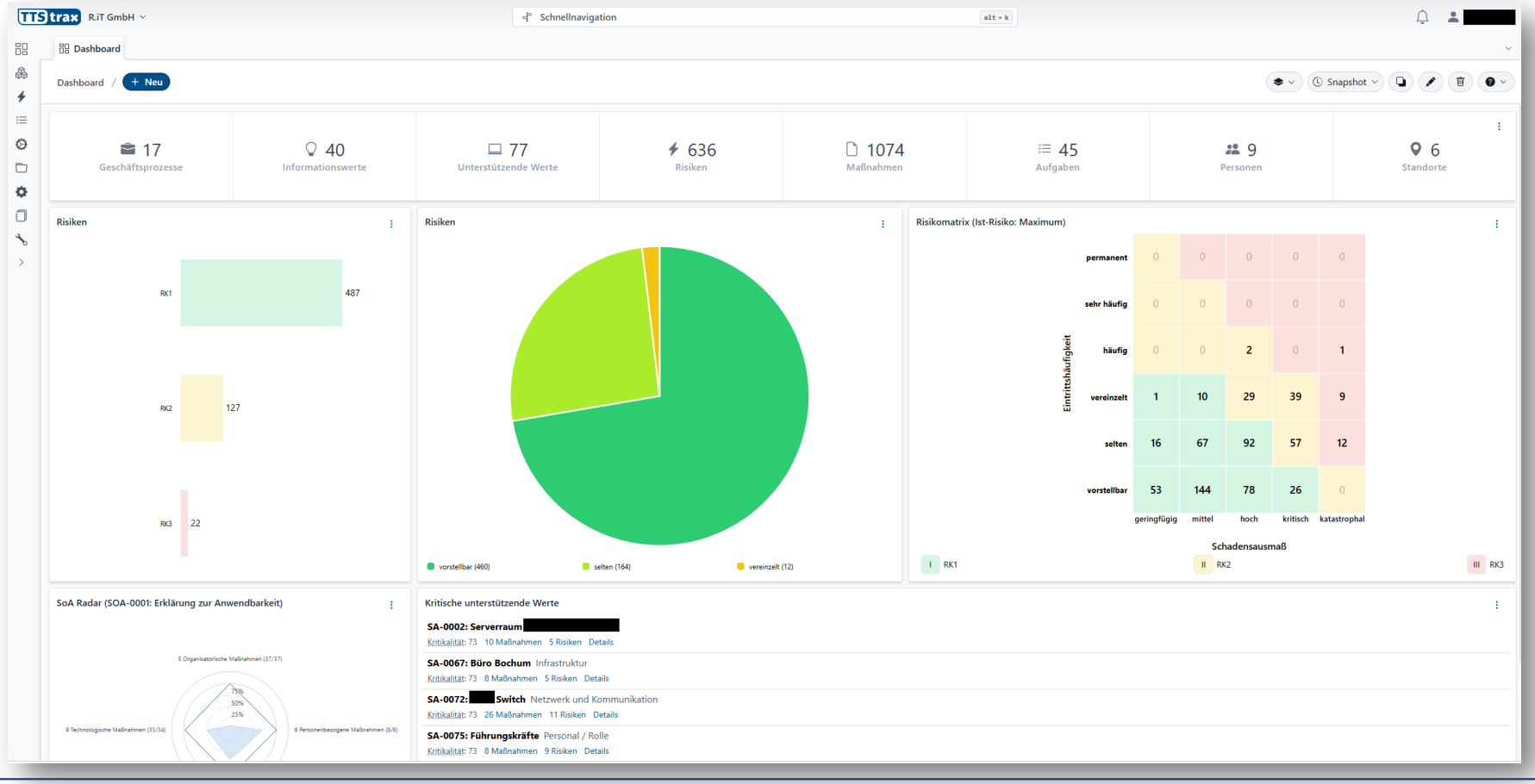
Steuerung

billigen · überwachen · sich schulen

→ persönlich, als Geschäftsleitung

Das ISMS ist Ihr Werkzeug dafür:
Es macht die Steuerung möglich – und belegbar.

ISMS „live“


TTS trax
R.iT GmbH
Schnellnavigation
alt + k
Dashboard
Dashboard / + Neu
Snapshot
17 Geschäftsprozesse
40 Informationswerte
77 Unterstützende Werte
636 Risiken
1074 Maßnahmen
45 Aufgaben
9 Personen
6 Standorte
Risiken
RK1 487
RK2 127
RK3 22
Risiken
vorstellbar (460)
selten (164)
vereinzelt (12)
Risikomatrix (Ist-Risiko: Maximum)
Eintrittshäufigkeit
permanent 0 0 0 0 0
sehr häufig 0 0 0 0 0
häufig 0 0 2 0 1
vereinzelt 1 10 29 39 9
selten 16 67 92 57 12
vorstellbar 53 144 78 26 0
geringfügig mittel hoch kritisch katastrophal
Schadensausmaß
I RK1 II RK2 III RK3
SoA Radar (SOA-0001: Erklärung zur Anwendbarkeit)
5 Organisatorische Maßnahmen (37/37)
8 Technologische Maßnahmen (33/34)
6 Personenbezogene Maßnahmen (8/8)
75%
50%
25%
Kritische unterstützende Werte
SA-0002: Serverraum [redacted]
Kritikalität: 73 10 Maßnahmen 5 Risiken Details
SA-0067: Büro Bochum Infrastruktur
Kritikalität: 73 8 Maßnahmen 5 Risiken Details
SA-0072: [redacted] Switch Netzwerk und Kommunikation
Kritikalität: 73 26 Maßnahmen 11 Risiken Details
SA-0075: Führungskräfte Personal / Rolle
Kritikalität: 73 8 Maßnahmen 9 Risiken Details


Was Sie absichern müssen

Das *System* steht – jetzt die übrigen Handlungsfelder

1 Risikoanalyse & Sicherheitskonzepte ✓ ISMS
Risikobehandlung

2 Bewältigung von Sicherheitsvorfällen
Erkennen, reagieren, wiederherstellen

3 Aufrechterhaltung des Betriebs
Backup, Disaster Recovery, BCM

4 Sicherheit der Lieferkette
Anbieter & Dienstleister

5 Sicherheit bei Erwerb, Entwicklung & Wartung
inkl. Schwachstellenmanagement

6 Wirksamkeit bewerten ✓ ISMS
Wirkt es wirklich? – regelmäßig überprüfen

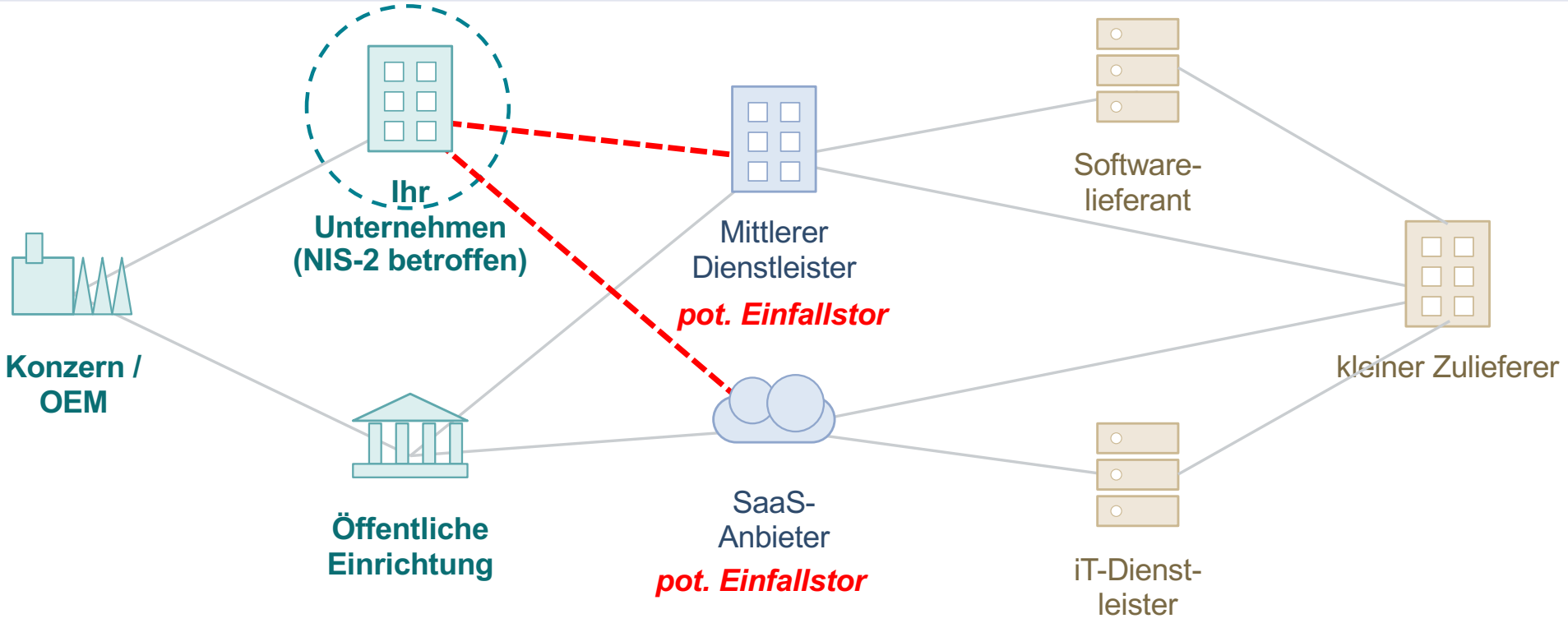
7 Cyberhygiene & Schulungen
Basispraktiken + Security-Awareness

8 Kryptografie & Verschlüsselung
Konzepte und Verfahren

9 Personalsicherheit & Zugriffskontrolle
inkl. Personal, Zugriffsrechte, IT-Inventar

10 Gesicherte Authentisierung & Kommunikation
sichere Anmeldung und Kommunikation

Nr. 4 – Sicherheit der Lieferkette



"Sicherheit der Lieferkette einschließlich …
der Beziehungen zu unmittelbaren Anbietern oder Diensteanbietern"

Nr. 4 – Sicherheit der Lieferkette

Ihr Unternehmen (betroffene Einrichtung)
Pflicht aus Nr. 4, § 30

muss die Lieferkette absichern

Anforderung per Vertrag

Ihre Zulieferer
evtl. nicht durch das Gesetz direkt verpflichtet

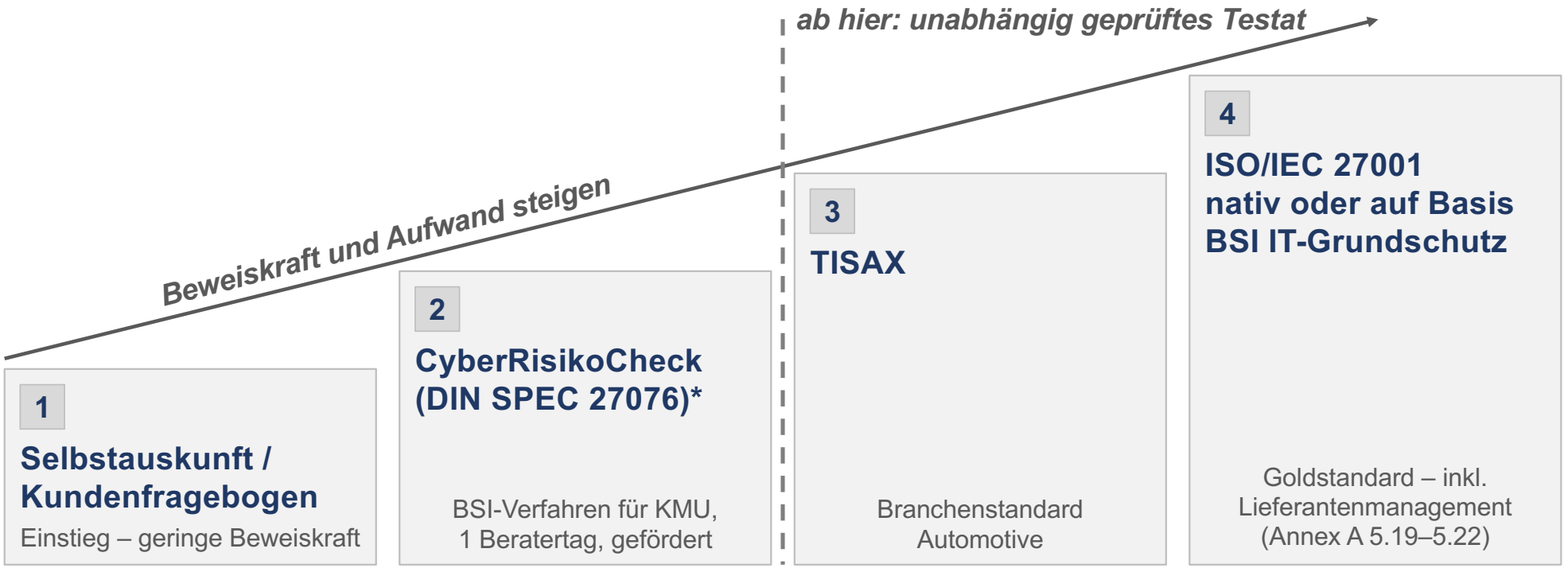
müssen trotzdem Nachweise liefern

reichen weiter an eigene Sub-Lieferanten …

Der eigentliche Hebel

Ob Sie *direkt* betroffen sind oder nicht: Ihre Kunden werden Sicherheit von Ihnen verlangen – und Sie von Ihren Zuliefern

Nr. 4 – Was sind mögliche Nachweise?



Was ausreicht, bestimmt Ihr Kunde – fragen Sie, bevor Sie investieren.

** lt. BSI: Ersteinschätzung, kein NIS-2-Konformitätsnachweis · Quelle: BSI-Infopaket „NIS-2-Lieferkette“ (bsi.bund.de)*

Das *System* steht – jetzt die übrigen Handlungsfelder

7 **Cyberhygiene & Schulungen**
Basispraktiken + Security-Awareness

Nr. 7 – Cyberhygiene & Schulungen

ohne geschulte Menschen wirkt keine Maßnahme!

Mitarbeitende:
erkennen und richtig handeln

- Phishing, Passwörter, Datenumgang etc.
- im Verdachtsfall: sofort intern melden

Geschäftsleitung:
bewerten und steuern können

- Risiken erkennen, einordnen, Folgen fürs Geschäft beurteilen (§ 38 Abs. 3)
- persönlich, nicht delegierbar

☞ der Mensch ist das häufigste Einfallstor

☞ regelmäßig, nicht einmalig – Schulungen & Cyberhygiene!

☞ Nachweise dokumentieren

Das *System* steht – jetzt die übrigen Handlungsfelder

2 **Bewältigung von Sicherheitsvorfällen**
Erkennen, reagieren, wiederherstellen

3 **Aufrechterhaltung des Betriebs**
Backup, Disaster Recovery, BCM

5 **Sicherheit bei Erwerb, Entwicklung & Wartung**
inkl. Schwachstellenmanagement

8 **Kryptografie & Verschlüsselung**
Konzepte und Verfahren

9 **Personalsicherheit & Zugriffskontrolle**
inkl. Personal, Zugriffsrechte, IT-Inventar

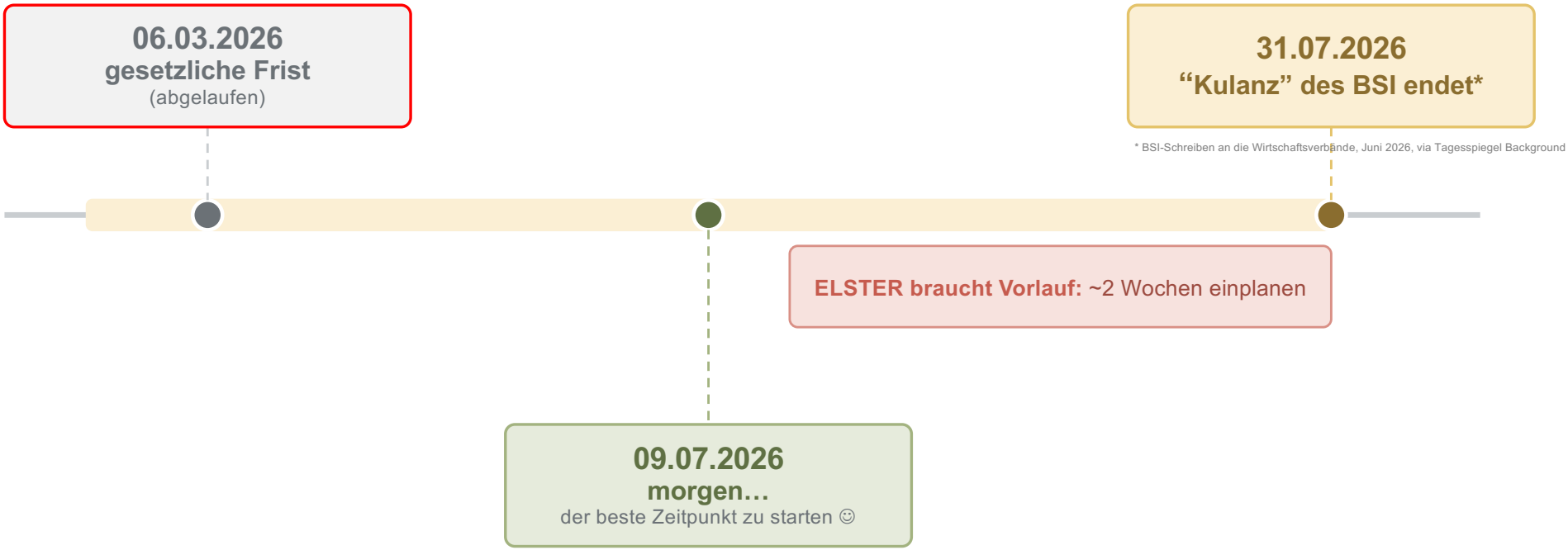
10 **Gesicherte Authentisierung & Kommunikation**
sichere Anmeldung und Kommunikation

die anderen Handlungsfelder

Was das Gesetz fordert *§ 30 BSIG — abstrakt*	Wie Sie es umsetzen können *typische Technik / Organisation*
Nr. 2 – Bewältigung von Sicherheitsvorfällen Erkennen, reagieren, wiederherstellen	EDR/XDR statt Virenschutz, kontinuierliche Angriffserkennung (Detection als Service)
Nr. 3 – Aufrechterhaltung des Betriebs Backup, Disaster Recovery, BCM	Backup-Strategie (3-2-1), Wiederanlaufplan, Notfallübung
Nr. 5 – Sicherheit bei Erwerb, Entwicklung & Wartung inkl. Schwachstellenmanagement	Patch-Management, Netzsegmentierung, regelmäßige Sicherheitsprüfungen (z. B. Pentests, Scans)
Nr. 8 – Kryptografie & Verschlüsselung Konzepte und Verfahren	Festplatten-/Mailverschlüsselung, TLS, Schlüsselverwaltung
Nr. 9 – Personalsicherheit & Zugriffskontrolle inkl. Personal, Zugriffsrechte, IT-Inventar	Least Privilege, Rollenkonzept, Inventarisierung
Nr. 10 – Gesicherte Authentisierung & Kommunikation sichere Anmeldung und Kommunikation	MFA, gesicherte Notfall-kommunikation (Out-of-Band)


Zuerst: registrieren

Registrierungsprozess



Auch verspätet gilt: Registrierung zeigt dem BSI, dass Sie handeln – und ELSTER-Vorlauf heißt: morgen anfangen.

Registrierungsprozess – Anmerkungen

- **Fristversäumnis = Eigenständiger Bußgeldtatbestand:**

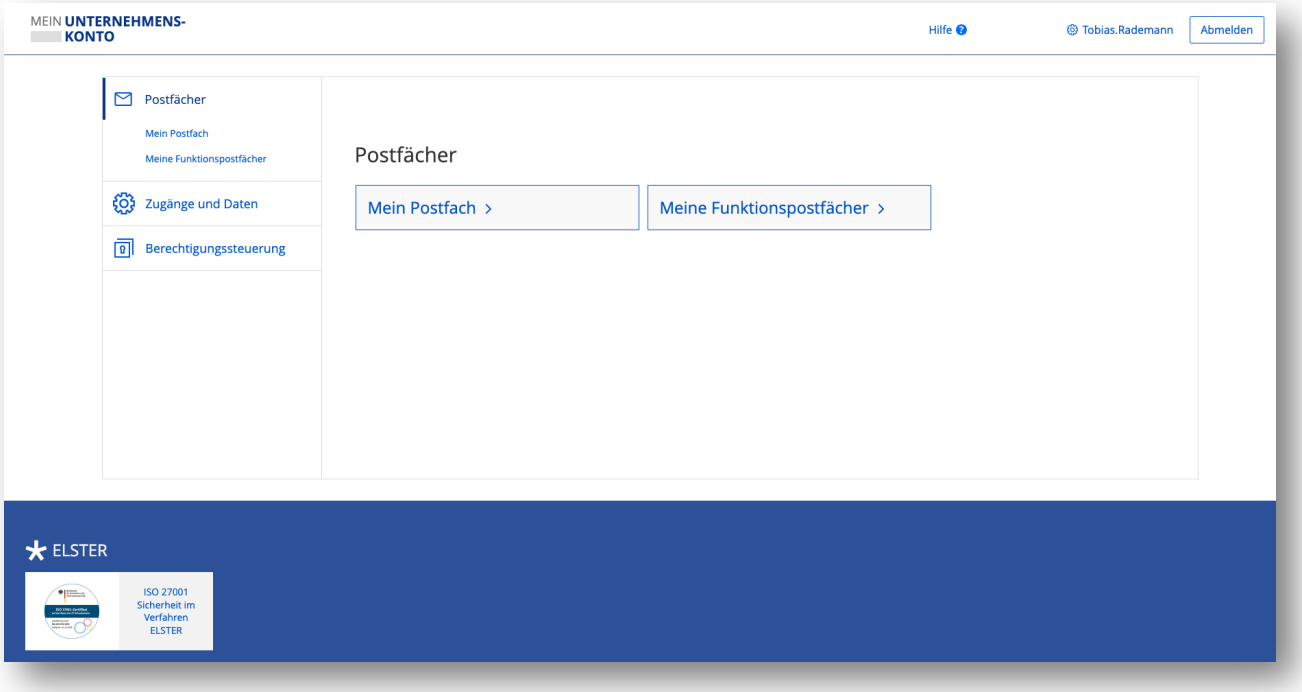
  bis € 500.000 (§ 65)

- **Bereithalten:** Sektor, Größe, Rechtsform, Kontaktstelle(n)

- **Selbsteinstufung:** rechtlich folgenreich – im Zweifel Fachanwalt

Registrierungsprozess: MUK (ELSTER)

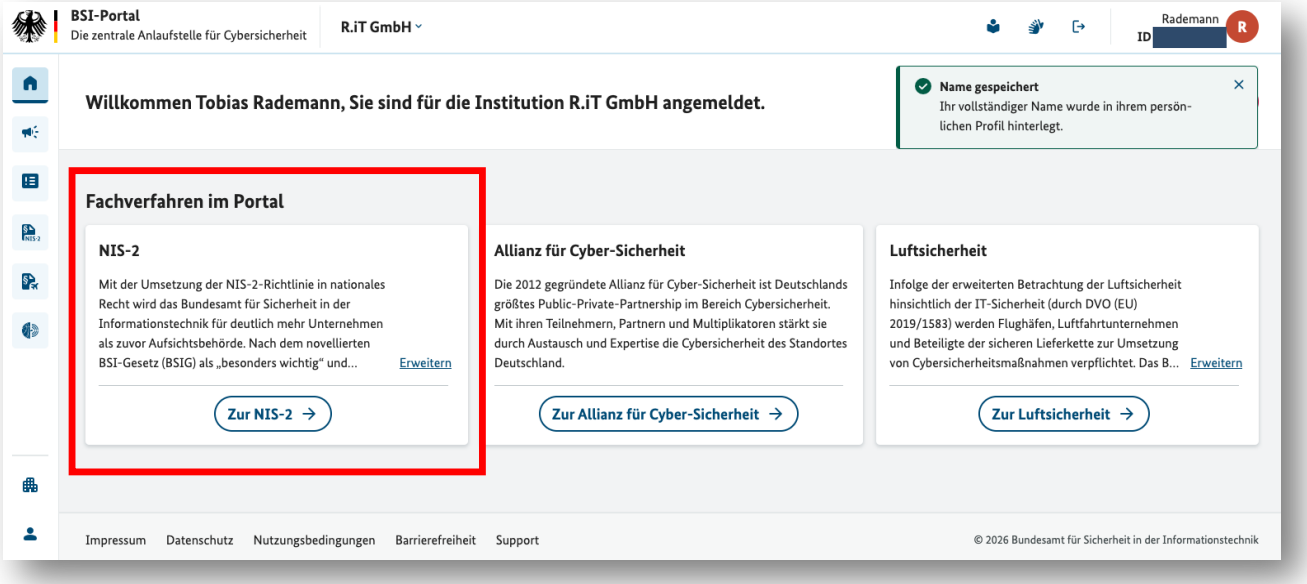
1. Registrierung bei „Mein Unternehmenskonto“ (MUK)
→ https://info.mein-unternehmenskonto.de/



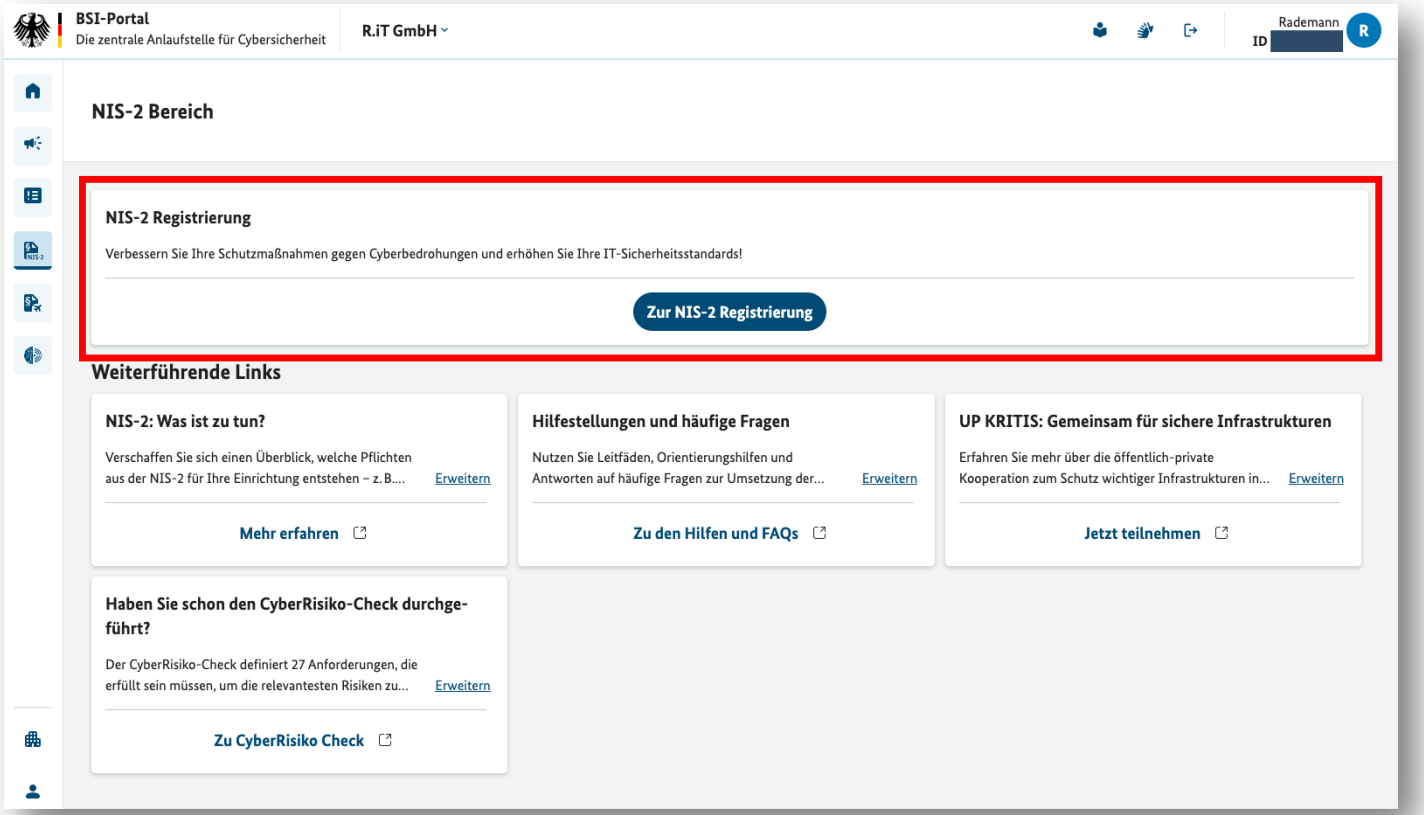
Registrierungsprozess: BSI-Portal

1. *Registrierung bei „Mein Unternehmenskonto“ (MUK)*
   → https://info.mein-unternehmenskonto.de/

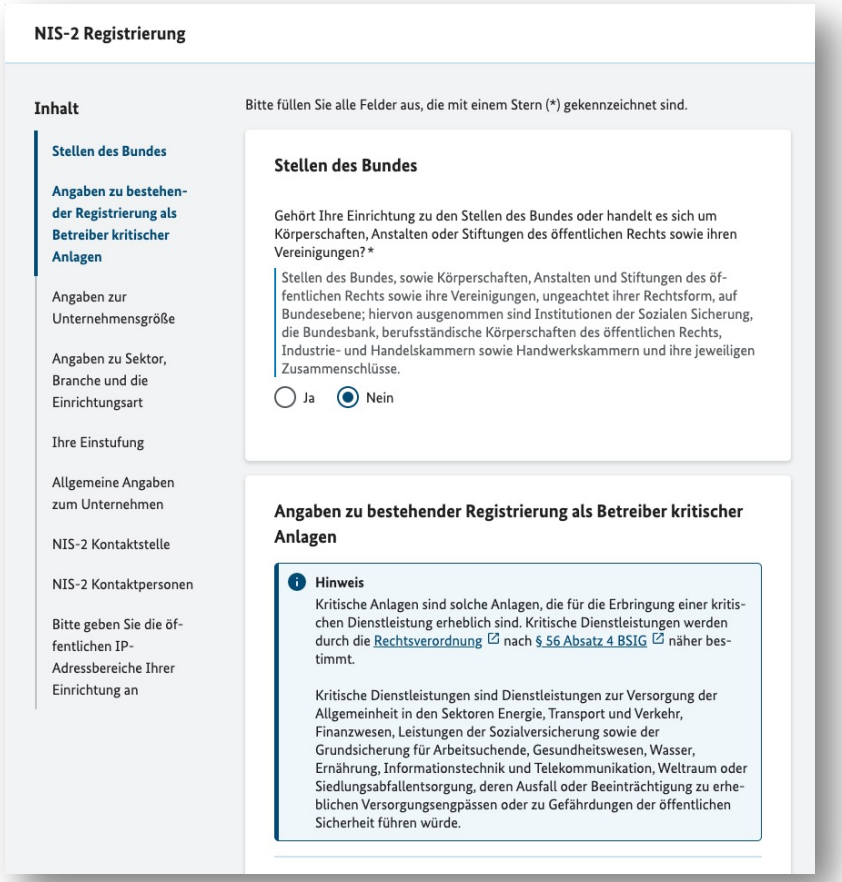
2. **Registrierung im BSI-Portal**
   → https://portal.bsi.bund.de/

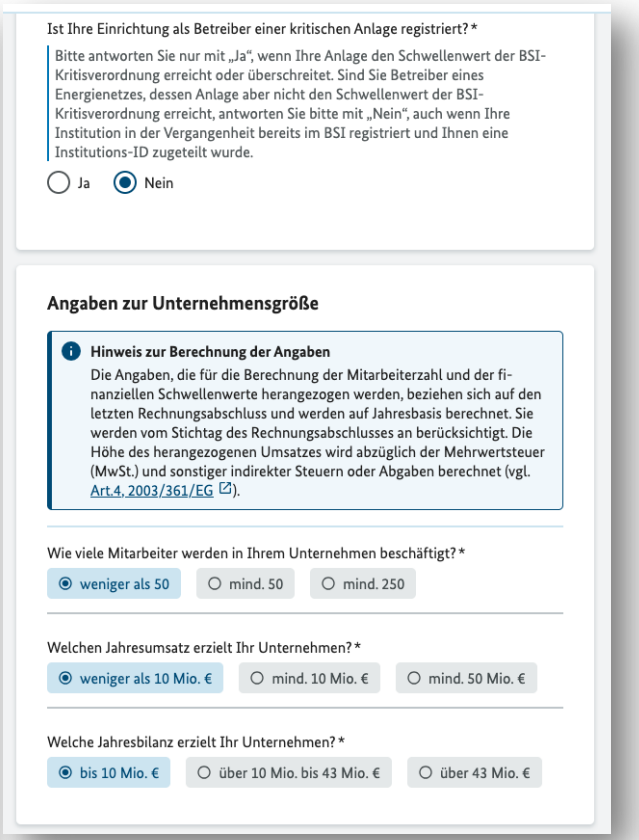


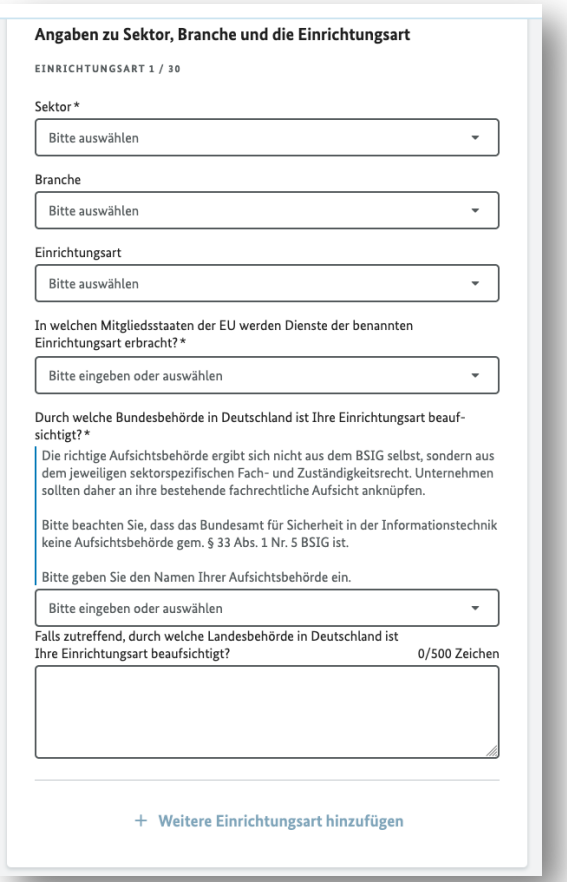
Registrierungsprozess: BSI-Portal / II



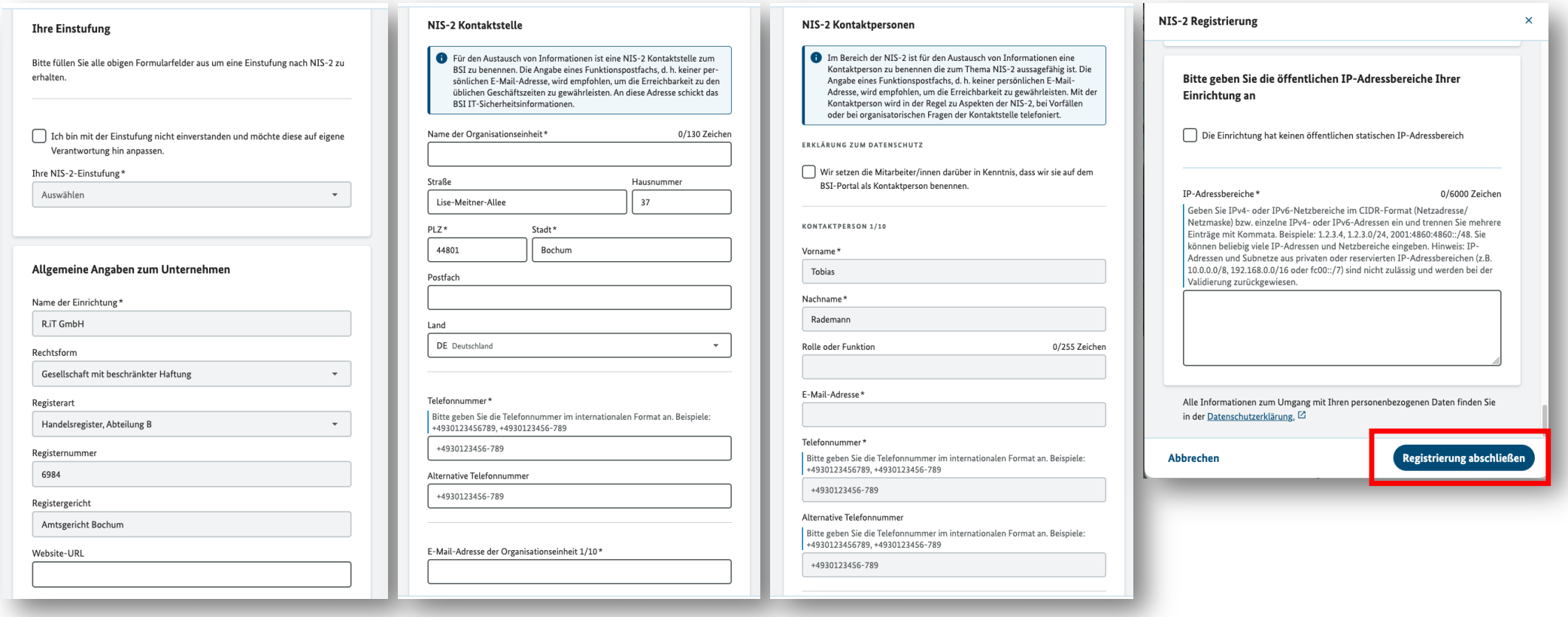
Registrierungsprozess: BSI-Portal / III







Registrierungsprozess: BSI-Portal / IV




Wenn es passiert: melden

Meldefristen für **erhebliche Sicherheitsvorfälle**

Kenntnis des Vorfalls
hier startet die Uhr für Stufe 1+2

Ihre Stufe-2-Meldung
hier startet die Uhr für Stufe 3

24 h

Stufe 1 – Frühwarnung

Erstinformation an das BSI

Frist: ab Kenntnis

72 h

Stufe 2 – bewertende Meldung

aktualisierte Infos + erste Bewertung: Schweregrad & Auswirkungen

Frist: ab Kenntnis

1 Monat

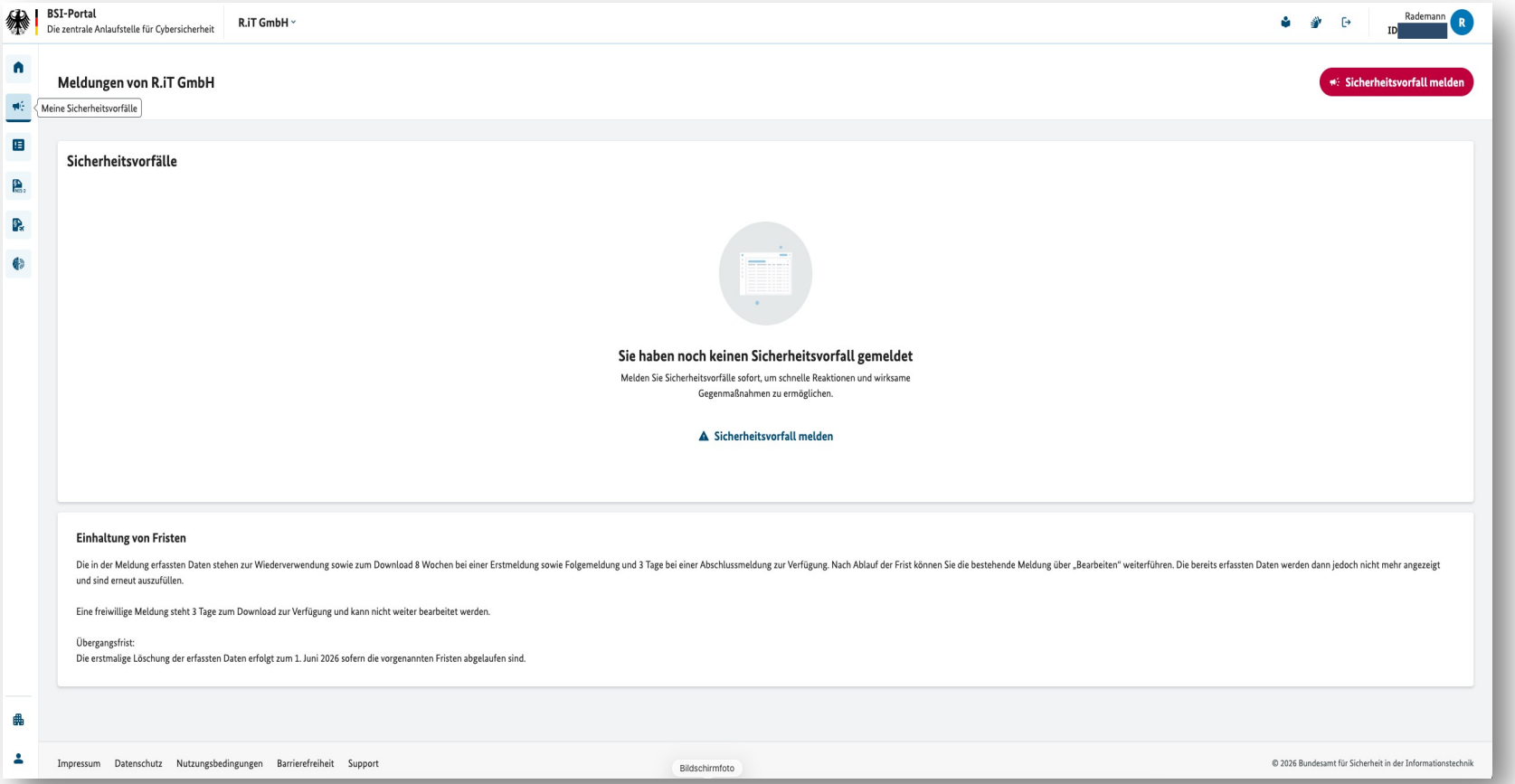
Stufe 3 – Abschlussmeldung

Beschreibung, Ursache, Abhilfemaßnahmen, ggf. Fortschrittsmeldung

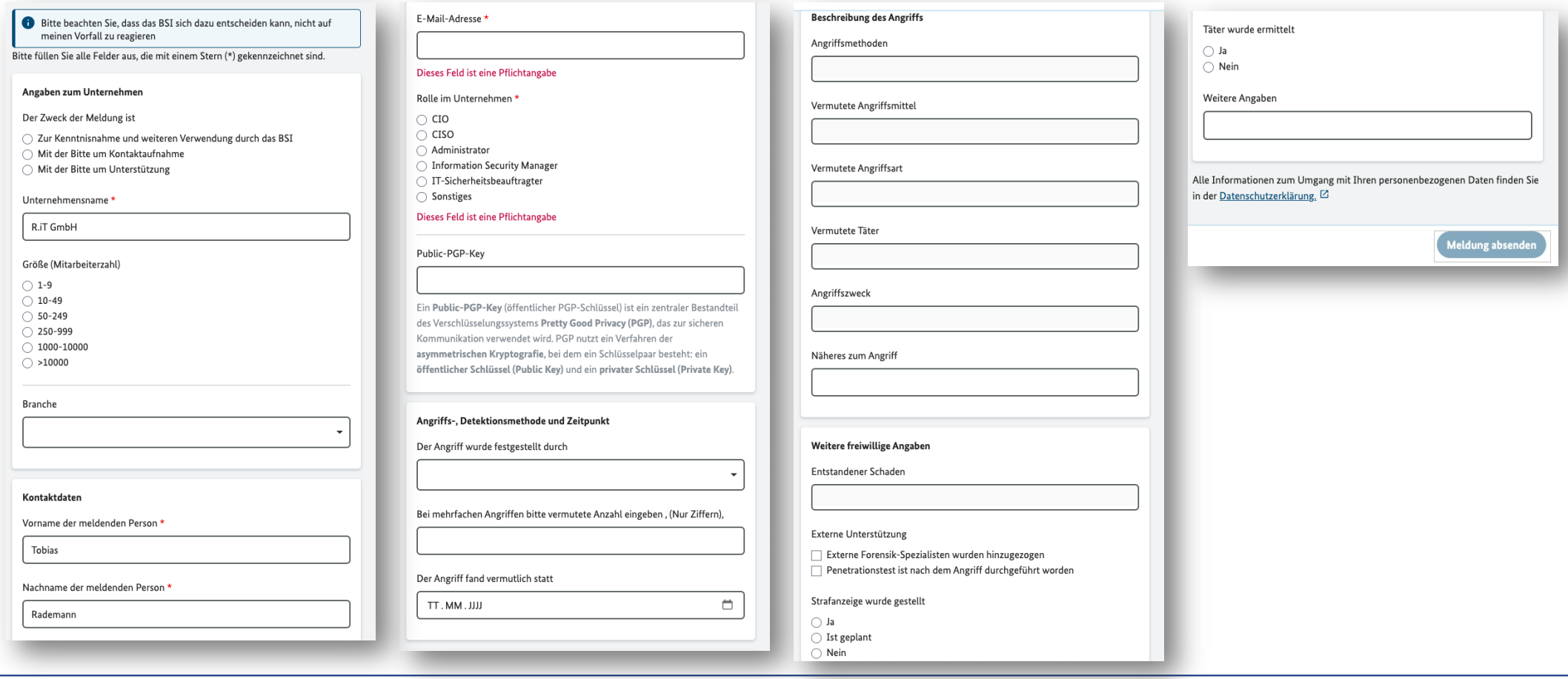
Frist: ab der Stufe-2-Meldung

Drei Stufen, eine Logik: erst warnen, dann bewerten, dann abschließen.

BSI: melden eines Sicherheitsvorfalls



BSI: melden eines Sicherheitsvorfalls



Bitte beachten Sie, dass das BSI sich dazu entscheiden kann, nicht auf meinen Vorfall zu reagieren

Bitte füllen Sie alle Felder aus, die mit einem Stern (*) gekennzeichnet sind.

Angaben zum Unternehmen

Der Zweck der Meldung ist

- Zur Kenntnisnahme und weiteren Verwendung durch das BSI
- Mit der Bitte um Kontaktaufnahme
- Mit der Bitte um Unterstützung

Unternehmensname *

R.iT GmbH

Größe (Mitarbeiterzahl)

- 1-9
- 10-49
- 50-249
- 250-999
- 1000-10000
- >10000

Branche

Kontaktdaten

Vorname der meldenden Person *

Tobias

Nachname der meldenden Person *

Rademann

E-Mail-Adresse *

Dieses Feld ist eine Pflichtangabe

Rolle im Unternehmen *

- CIO
- CISO
- Administrator
- Information Security Manager
- IT-Sicherheitsbeauftragter
- Sonstiges

Dieses Feld ist eine Pflichtangabe

Public-PGP-Key

Ein **Public-PGP-Key** (öffentlicher PGP-Schlüssel) ist ein zentraler Bestandteil des Verschlüsselungssystems **Pretty Good Privacy (PGP)**, das zur sicheren Kommunikation verwendet wird. PGP nutzt ein Verfahren der **asymmetrischen Kryptografie**, bei dem ein Schlüsselpaar besteht: ein **öffentlicher Schlüssel (Public Key)** und ein **privater Schlüssel (Private Key)**.

Angriffs-, Detektionsmethode und Zeitpunkt

Der Angriff wurde festgestellt durch

Bei mehrfachen Angriffen bitte vermutete Anzahl eingeben , (Nur Ziffern),

Der Angriff fand vermutlich statt

TT . MM . JJJJ

Beschreibung des Angriffs

Angriffsmethoden

Vermutete Angriffsmittel

Vermutete Angriffsart

Vermutete Täter

Angriffszweck

Näheres zum Angriff

Weitere freiwillige Angaben

Entstandener Schaden

Externe Unterstützung

- Externe Forensik-Spezialisten wurden hinzugezogen
- Penetrationstest ist nach dem Angriff durchgeführt worden

Strafanzeige wurde gestellt

- Ja
- Ist geplant
- Nein

Täter wurde ermittelt

- Ja
- Nein

Weitere Angaben

Alle Informationen zum Umgang mit Ihren personenbezogenen Daten finden Sie in der Datenschutzerklärung.

Meldung absenden

Melden im Ernstfall: ein Vorlauf, zwei Meldewege

Meldefähig wird man vor dem Vorfall:

Wer den Portalzugang erst im Ernstfall aufbaut (~2 Wochen ELSTER-Vorlauf), hat die 24-Stunden-Frist verloren, bevor er anfängt.

Weg 1: BSI (§ 32 BSIG)

24 h → 72 h → 1 Monat (die Fristen von eben)

Start: Kenntnis des erheblichen Vorfalls

Weg 2: Datenschutzaufsicht (Art. 33 DSGVO)

unverzüglich, spätestens 72 h – sobald personenbezogene Daten betroffen sind (fast immer)

Start: Kenntnis der Verletzung

Zwei Meldungen, zwei Behörden – ein Auslöser: Kenntnis.


Müssen Sie das nachweisen?

NIS-2-Nachweise

Nachweis*pflicht*

- § 39 BSIG
- gilt nur für Betreiber **kritischer Anlagen*** (nicht „besonders wichtige Einrichtungen“!)
- *: Schwelle = Versorgung von mind. ~500.000 Personen

- ISO 27001 kann *Teil* des § 39-Nachweises sein, ihn aber nicht vollständig ersetzen

➔ Audit/Prüfung/Zertifizierung, alle drei Jahre

Nachweis*fähigkeit*

- § 30 BSIG
- gilt für **alle NIS-2-Betroffenen**
- jederzeit belegen können, dass Sie die Maßnahmen umsetzen
- Dokumentation ist die Grundlage
- ein gefülltes, funktionsfähiges und gepflegtes ISMS / ein ISO 27001 Zertifikat helfen, die Nachweisfähigkeit strukturiert zu belegen

➔ Nachweis jederzeit auf Verlangen des BSI


So fangen Sie an

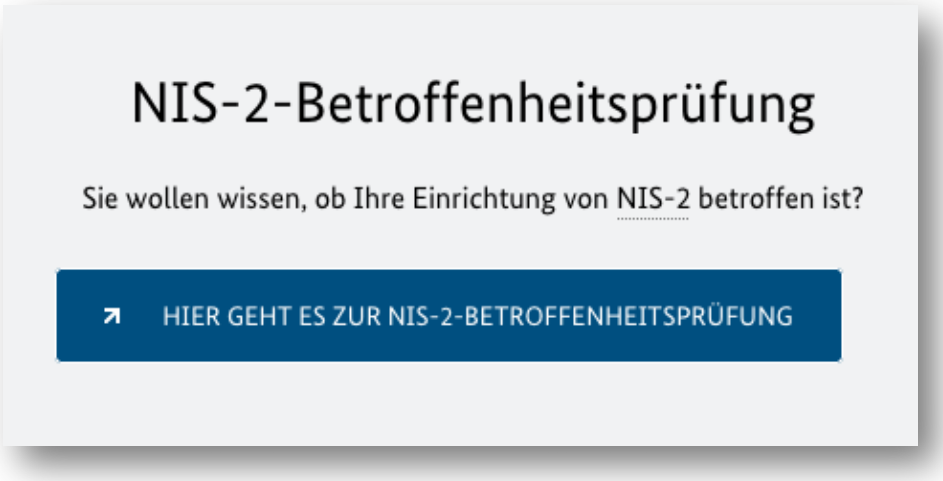
klare, überschaubare Etappen

ISMS entsteht *ISMS wirkt*

	1 Standort	2a Gap-Analyse	2b Quick Wins	3 Umsetzung	4 Betrieb & Optimierung
Ihre Schritte	NIS-2: Betroffenheit & Pflichten klären  *1-2 Wochen*	Abgleich mit § 30, priorisierter Fahrplan  *2-4 Monate*	Sofort-Absicherung: MFA, Backup, Updates  *1-3 Monate*	Technik, Organisation & Prozesse aufbauen  *6-18 Monate*	laufende Steuerung & Verbesserung  *laufend*
Ihr Nutzen	NIS-2 Betroffenheit & Pflichten geklärt	Klarheit über Prioritäten – Sie investieren dort, wo es am meisten wirkt	Sofort höhere Sicherheit	Höheres Schutzniveau – und im Ernstfall handlungs- und nachweisfähig	Dauerhaft wirksam – und der laufende Nachweis Ihrer Sorgfaltspflicht

Ihr Startpunkt morgen früh:

Betroffenheitsanalyse: https://betroffenheitspruefung-nis-2.bsi.de/



Hinweis: Selbsteinschätzung, keine rechtsverbindliche Feststellung

Was Sie mitnehmen

Fazit

1

Ein System statt zehn Aufgaben

Das ISMS führt die zehn Pflichten zu einem steuerbaren Ganzen zusammen.

2

Sie ordnen und verantworten

Die Steuerung bleibt bei Ihnen (§ 38) – umsetzen können andere für Sie, intern oder mit Partnern.

3

Ein Schritt genügt für morgen

Klarheit schaffen, wo Sie stehen – der Rest folgt Etappe für Etappe.

Im Kern ist NIS-2 Risikomanagement –

also eine Ihrer Kernkompetenzen als Unternehmer*in!

Fazit

NIS-2 = Ihre Chance auf Zukunftsfähigkeit:

➔ **Sicherheit**, die den Betrieb trägt

➔ **Vertrauen**, das Aufträge sichert

➔ **Vorsprung im Wettbewerb** – vor allen, die noch zögern

Ihre Fragen

Ihre drei Schritte — scannen & loslegen

1 · Betroffenheit prüfen
betroffenheitspruefung-nis-2.bsi.de

2 · Registrieren (BSI-Portal)
portal.bsi.bund.de

3 · Cheat-Sheet & mehr
rit.de/infocenter

Vielen Dank für Ihre Zeit und Ihre Aufmerksamkeit!

Bei Rückfragen wenden Sie sich gerne an:

DISCOVER THE SPIR.iT OF EXCELLENCE.
SURPASS YOUR SUCCESS.

Tobias Rademann, M.A.
R.iT GmbH • www.RiT.de
NL Süd: Rodinger Str. 15, 93413 Cham
Tel.: (09971) 806 29-0, Fax: -29
Zentrale: Lise-Meitner-Allee 37, 44801 Bochum
Tel.: (0234) 43 88 00-0, Fax: -29

Fotos: Adobe Stock