



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

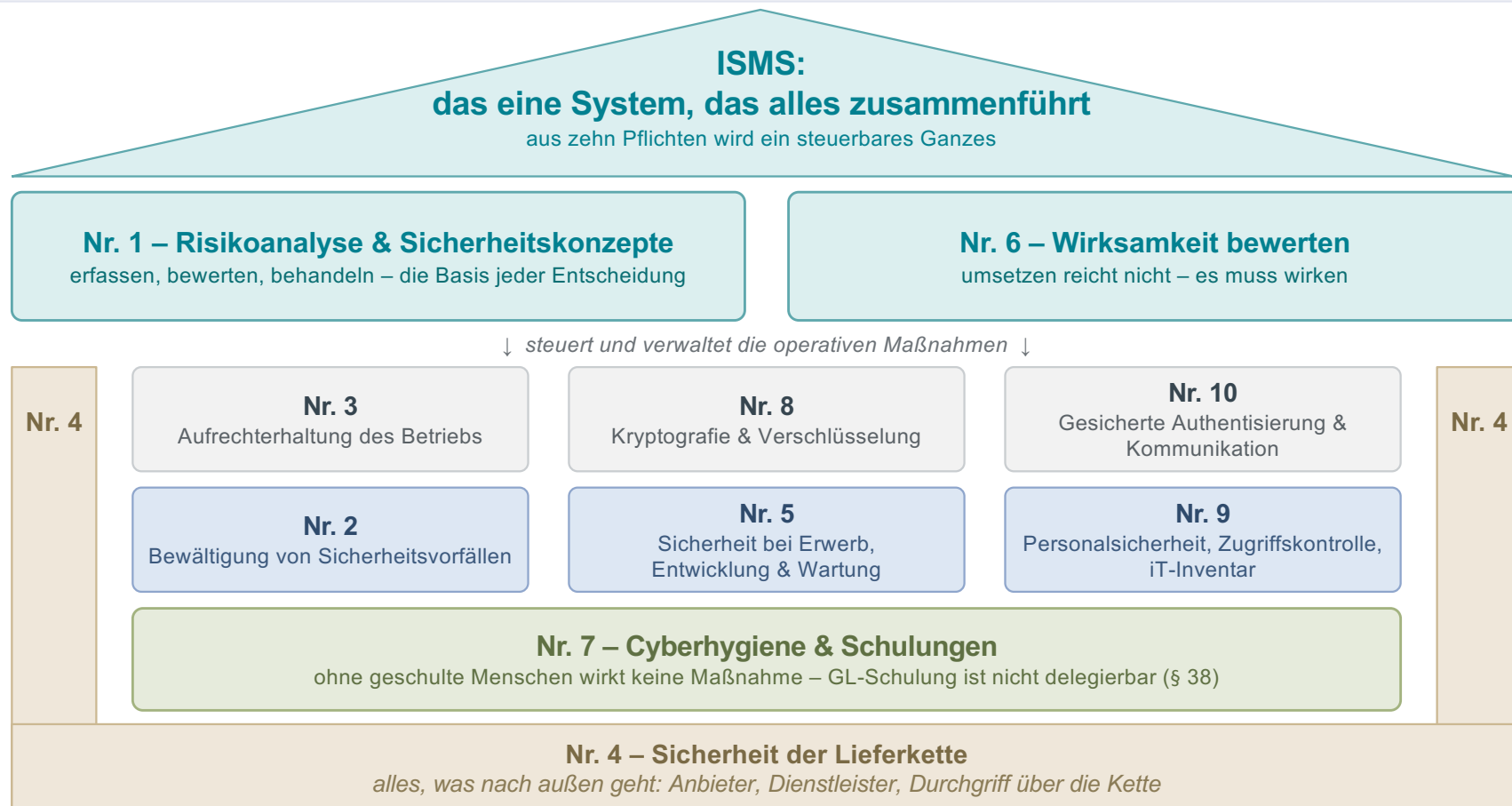
7 Cyberhygiene & Schulungen
Basispraktiken + Security-Awareness

8 Kryptografie & Verschlüsselung
Konzepte und Verfahren

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

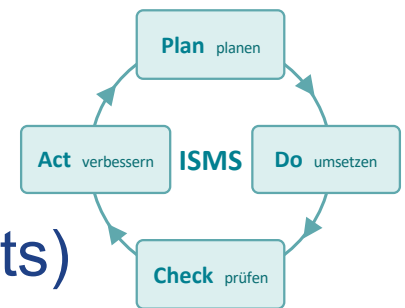
10 Gesicherte Authentisierung & Kommunikation
sichere Anmeldung und Kommunikation

Vom Katalog zum System:



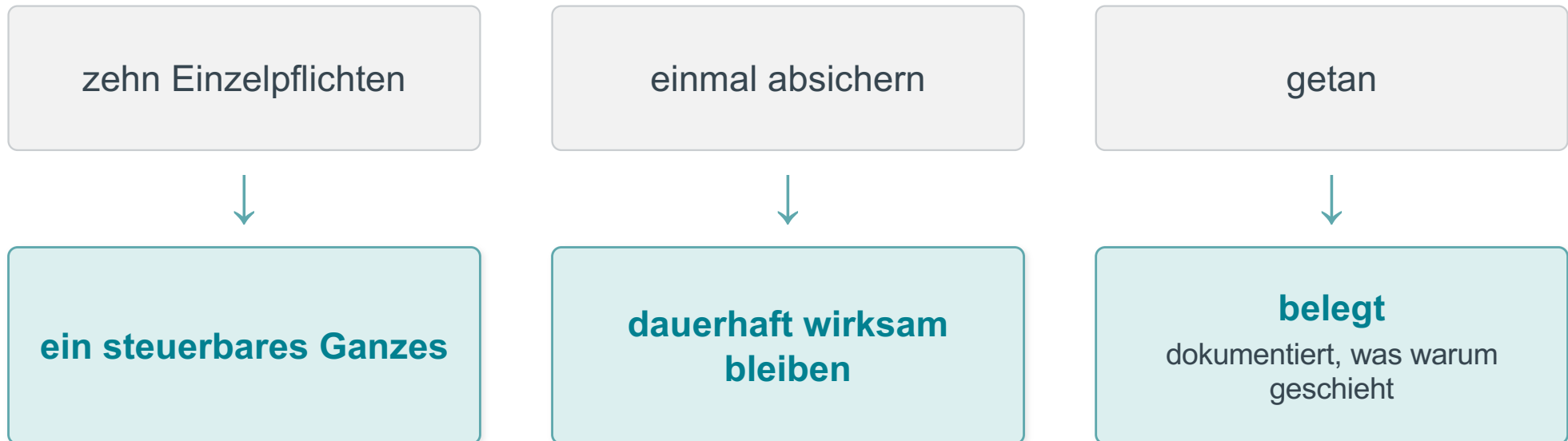
Was ist ein ISMS?

- ✓ ISMS = Informationssicherheitsmanagementsystem
- ✓ § 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



**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

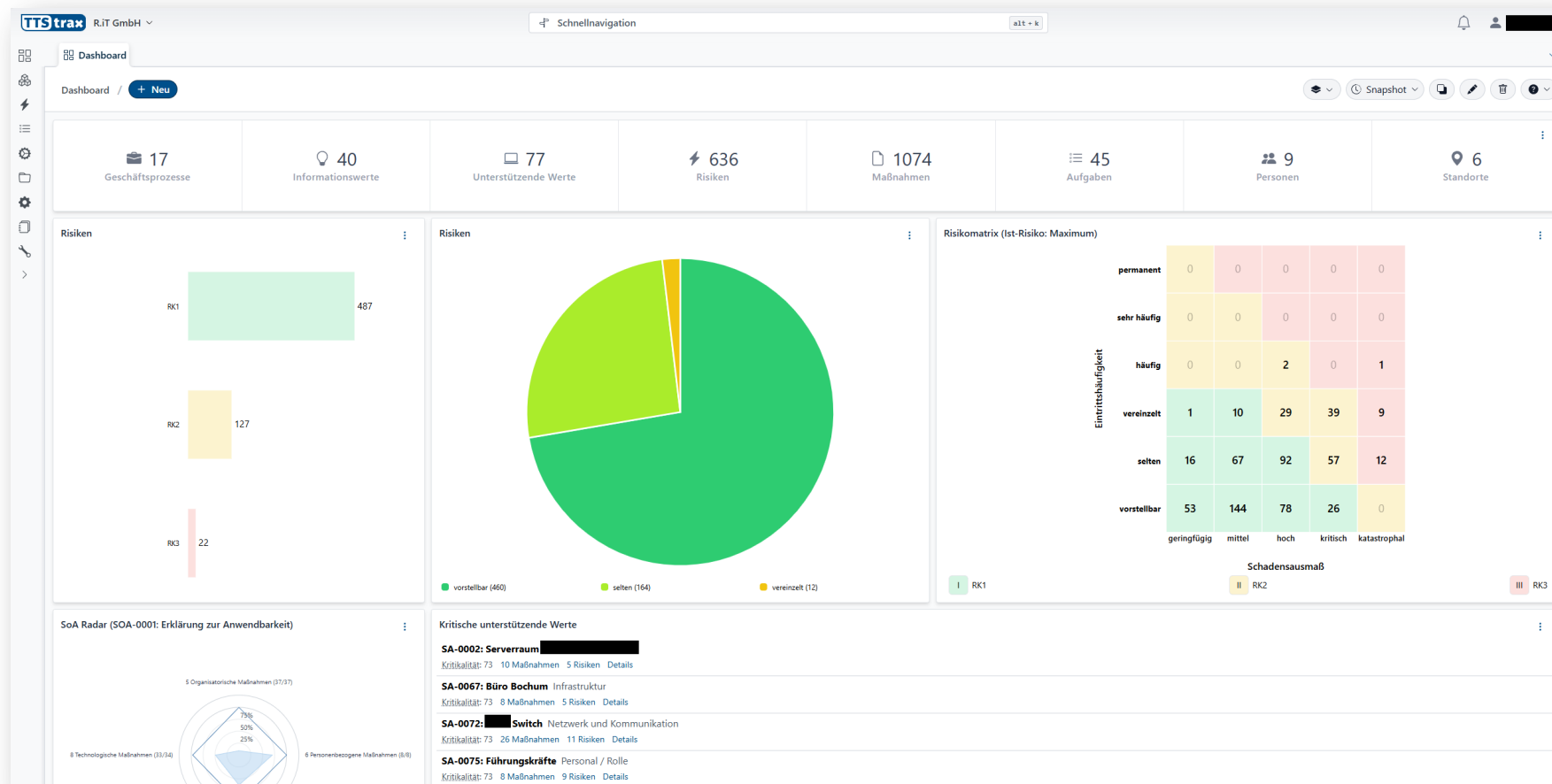
Das bleibt bei Ihnen (§ 38):

Steuerung

billigen · überwachen · sich schulen
→ persönlich, als Geschäftsleitung

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

ISMS „live“





Was Sie absichern müssen

Das *System* steht – jetzt die übrigen Handlungsfelder



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



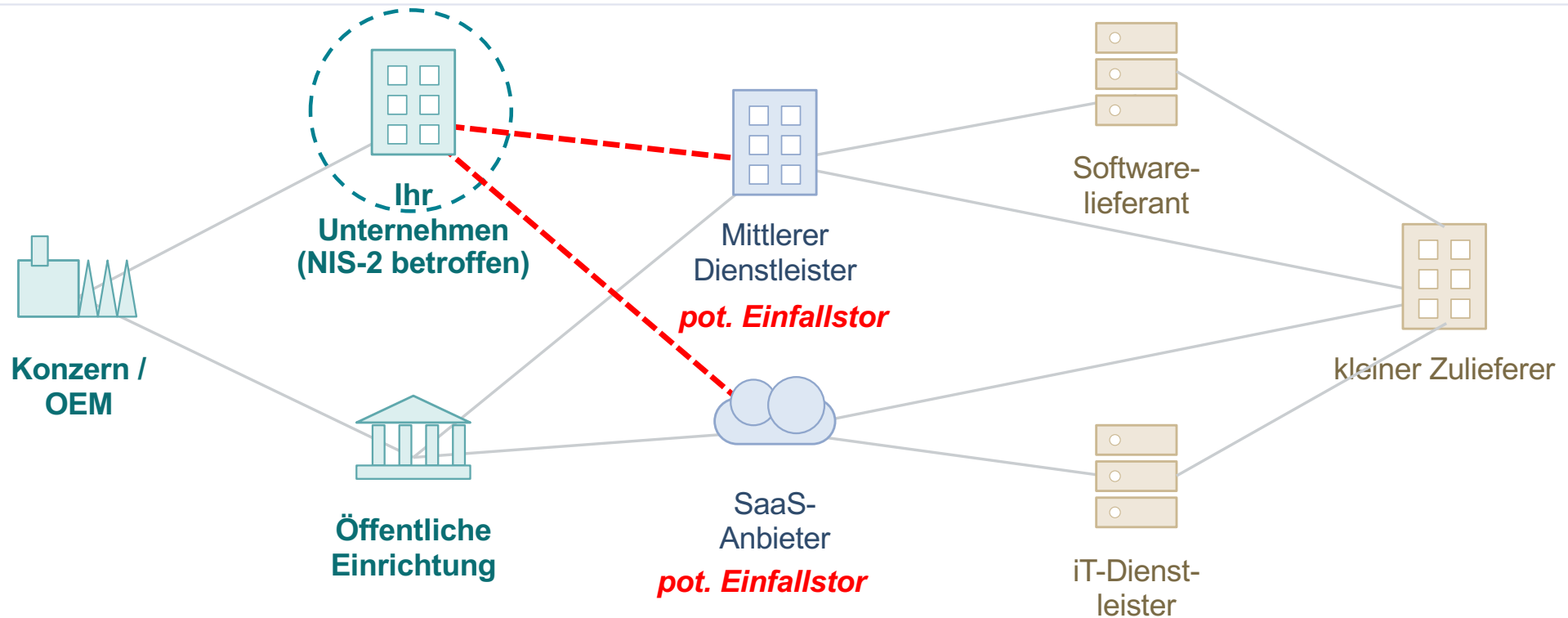
7 Cyberhygiene & Schulungen Basispraktiken + Security-Awareness

8 Kryptografie & Verschlüsselung Konzepte und Verfahren

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

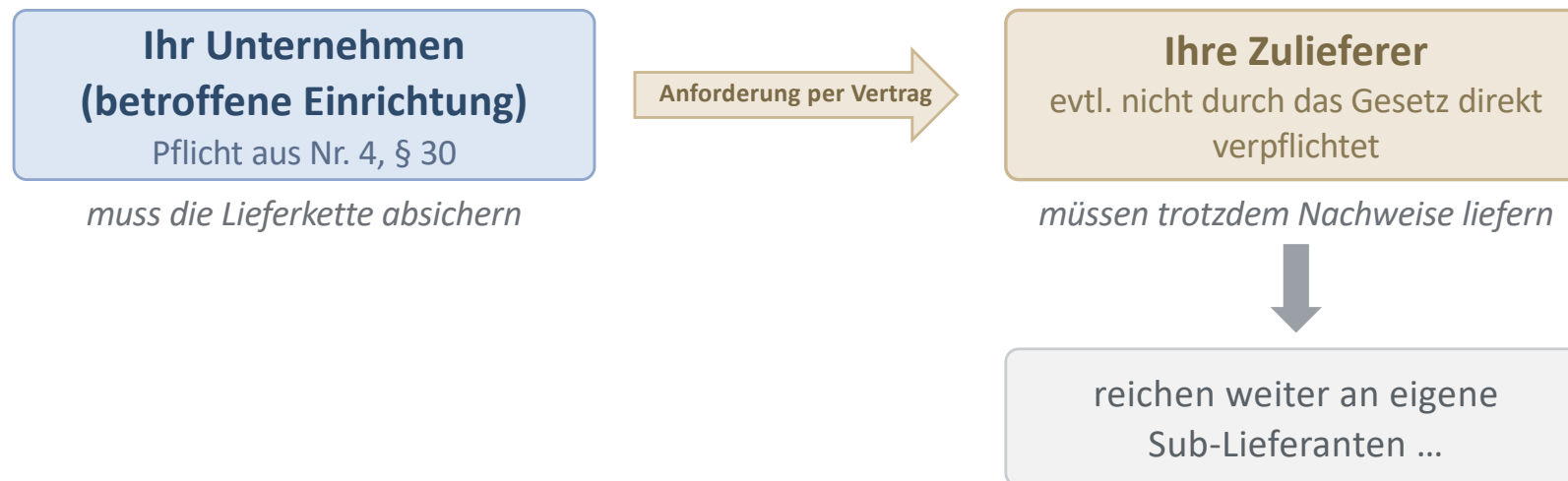
10 Gesicherte Authentisierung & Kommunikation sichere Anmeldung und Kommunikation

Nr. 4 – Sicherheit der Lieferkette



**"Sicherheit der Lieferkette einschließlich ...
der Beziehungen zu unmittelbaren Anbietern oder Diensteanbietern"**

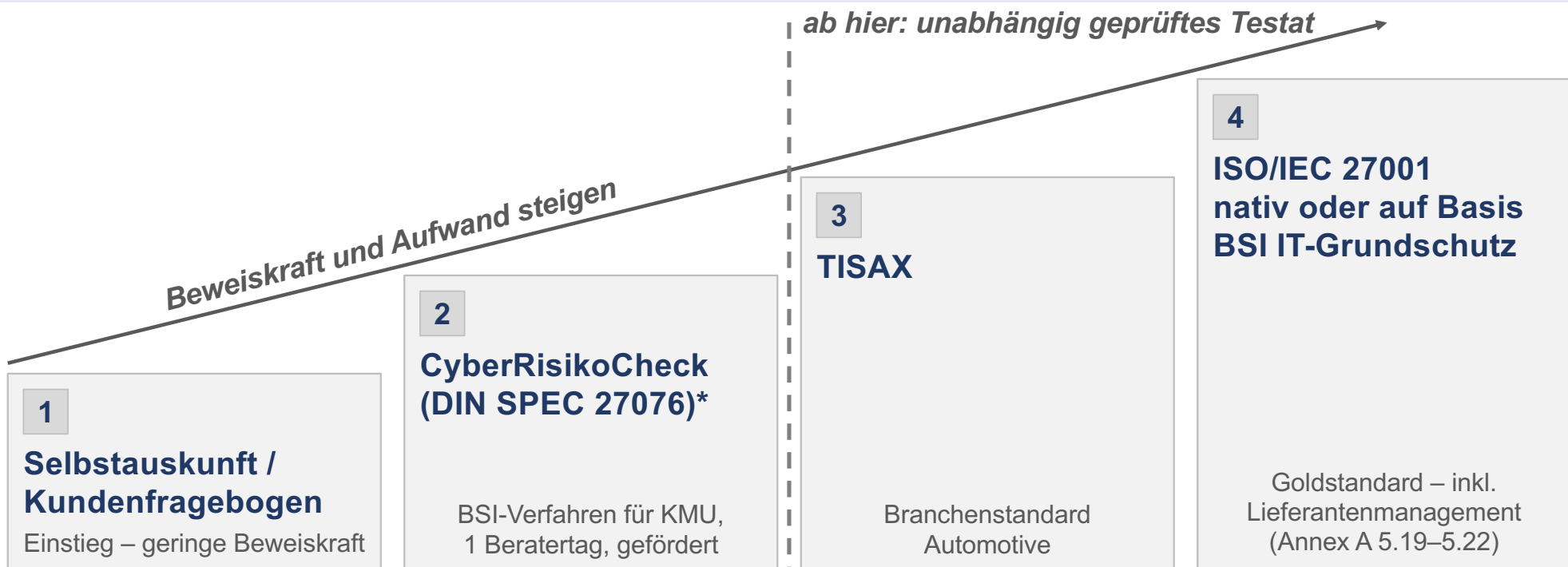
Nr. 4 – Sicherheit der Lieferkette



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

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*

Nr. 2 – Bewältigung von Sicherheitsvorfällen
Erkennen, reagieren, wiederherstellen

Nr. 3 – Aufrechterhaltung des Betriebs
Backup, Disaster Recovery, BCM

Nr. 5 – Sicherheit bei Erwerb, Entwicklung & Wartung
inkl. Schwachstellenmanagement

Nr. 8 – Kryptografie & Verschlüsselung
Konzepte und Verfahren

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

Nr. 10 – Gesicherte Authentisierung & Kommunikation
sichere Anmeldung und Kommunikation

Wie Sie es umsetzen können *typische Technik / Organisation*

EDR/XDR statt Virenschutz, kontinuierliche
Angriffserkennung (Detection as Service)

Backup-Strategie (3-2-1),
Wiederanlaufplan, Notfallübung

Patch-Management, Netzsegmentierung,
regelmäßige Sicherheitsprüfungen (z. B. Pentests, Scans)

Festplatten-/Mailverschlüsselung,
TLS, Schlüsselverwaltung

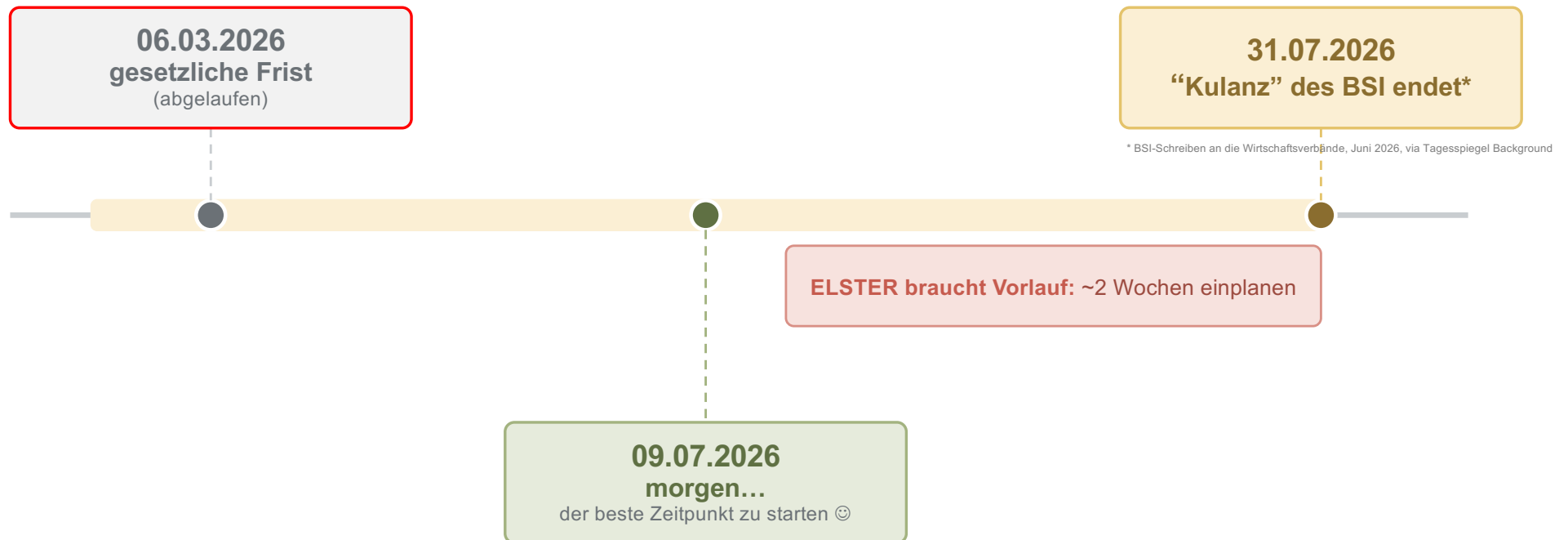
Least Privilege, Rollenkonzept,
Inventarisierung

MFA, gesicherte Notfall-
kommunikation (Out-of-Band)

A photograph of a modern building's entrance. The interior is visible, showing a dark floor with three large, dark, rectangular mats. The entrance is framed by large glass panels and doors. Outside, there is a paved area with some greenery and a modern building in the background. The text "Zuerst: registrieren" is overlaid in white on the floor mats.

Zuerst: registrieren

Registrierungsprozess



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

- **Fristversäumnis = Eigenständiger Bußgeldtatbestand:**

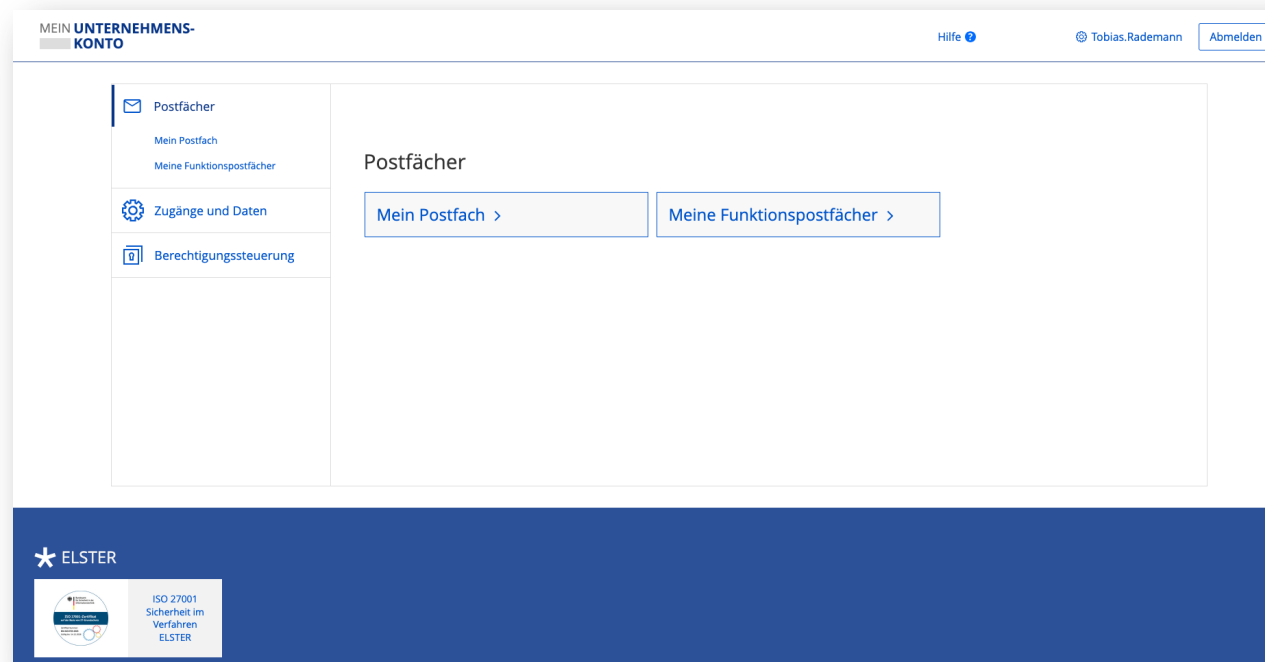
bis € 500.000 (§ 65)

- **Bereithalten:** Sektor, Größe, Rechtsform, Kontaktstelle(n)
- **Selbsteinstufung:** rechtlich folgenreich – im Zweifel Fachanwalt

Registrierungsprozess: MUK (ELSTER)



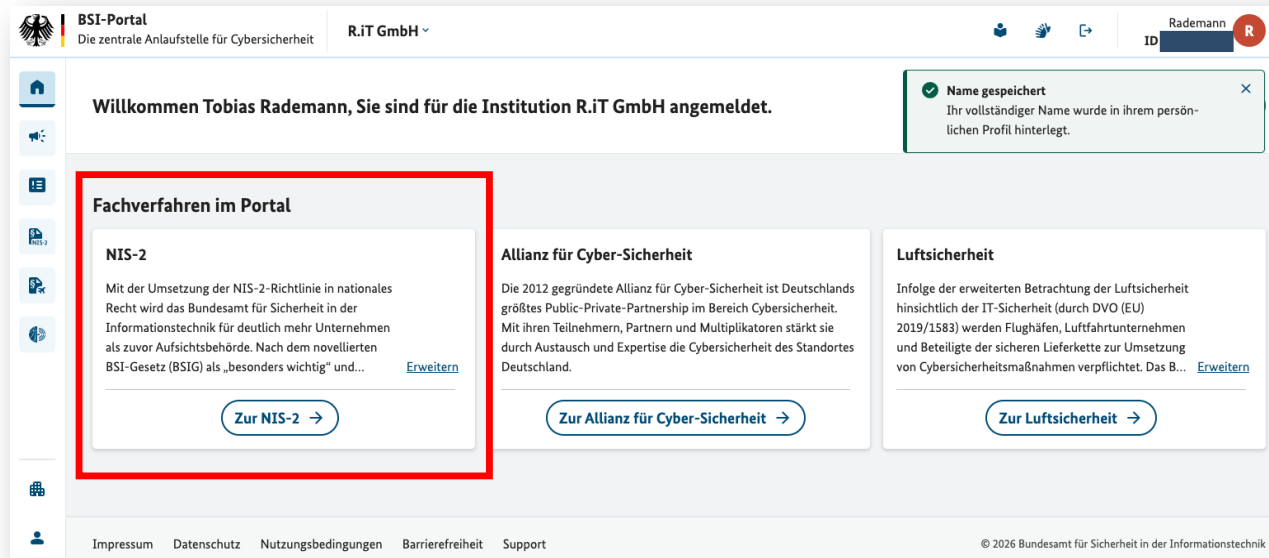
1. Registrierung bei „Mein Unternehmenskonto“ (MUK) → <https://info.mein-unternehmenskonto.de/>



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



The screenshot shows the BSI-Portal interface. At the top, the header includes the BSI logo, the text 'BSI-Portal Die zentrale Anlaufstelle für Cybersicherheit', and the user 'RiT GmbH'. On the right, there is a user profile for 'Rademann' with an ID and a blue 'R' icon. A left sidebar contains navigation icons. The main content area is titled 'NIS-2 Bereich'. A red rectangular box highlights the 'NIS-2 Registrierung' section, which contains the text 'Verbessern Sie Ihre Schutzmaßnahmen gegen Cyberbedrohungen und erhöhen Sie Ihre IT-Sicherheitsstandards!' and a prominent blue button labeled 'Zur NIS-2 Registrierung'. Below this, the 'Weiterführende Links' section features four cards: 'NIS-2: Was ist zu tun?' with a 'Mehr erfahren' link, 'Hilfestellungen und häufige Fragen' with a 'Zu den Hilfen und FAQs' link, 'UP KRITIS: Gemeinsam für sichere Infrastrukturen' with a 'Jetzt teilnehmen' link, and 'Haben Sie schon den CyberRisiko-Check durchgeführt?' with a 'Zu CyberRisiko Check' link. Each card also includes an 'Erweitern' link.

Registrierungsprozess: BSI-Portal / III



NIS-2 Registrierung

Inhalt

- Stellen des Bundes
- Angaben zu bestehender Registrierung als Betreiber kritischer Anlagen
- Angaben zur Unternehmensgröße
- Angaben zu Sektor, Branche und die Einrichtungsart
- Ihre Einstufung
- Allgemeine Angaben zum Unternehmen
- NIS-2 Kontaktstelle
- NIS-2 Kontaktpersonen

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

Stellen des Bundes

Gehört Ihre Einrichtung zu den Stellen des Bundes oder handelt es sich um Körperschaften, Anstalten oder Stiftungen des öffentlichen Rechts sowie ihren Vereinigungen? *

Stellen des Bundes, sowie Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts sowie ihre Vereinigungen, ungeachtet ihrer Rechtsform, auf Bundesebene; hiervon ausgenommen sind Institutionen der Sozialen Sicherung, die Bundesbank, berufsständische Körperschaften des öffentlichen Rechts, Industrie- und Handelskammern sowie Handwerkskammern und ihre jeweiligen Zusammenschlüsse.

☐ Ja ☒ Nein

Angaben zu bestehender Registrierung als Betreiber kritischer Anlagen

Hinweis
Kritische Anlagen sind solche Anlagen, die für die Erbringung einer kritischen Dienstleistung erheblich sind. Kritische Dienstleistungen werden durch die [Rechtsverordnung](#) nach [§ 56 Absatz 4 BSIg](#) näher bestimmt.
Kritische Dienstleistungen sind Dienstleistungen zur Versorgung der Allgemeinheit in den Sektoren Energie, Transport und Verkehr, Finanzwesen, Leistungen der Sozialversicherung sowie der Grundsicherung für Arbeitsuchende, Gesundheitswesen, Wasser, Ernährung, Informationstechnik und Telekommunikation, Weltraum oder Siedlungsabfallentsorgung, deren Ausfall oder Beeinträchtigung zu erheblichen Versorgungsengpässen oder zu Gefährdungen der öffentlichen Sicherheit führen würde.

Ist Ihre Einrichtung als Betreiber einer kritischen Anlage registriert? *

Bitte antworten Sie nur mit „Ja“, wenn Ihre Anlage den Schwellenwert der BSI-Kritischerverordnung erreicht oder überschreitet. Sind Sie Betreiber eines Energienetzes, dessen Anlage aber nicht den Schwellenwert der BSI-Kritischerverordnung erreicht, antworten Sie bitte mit „Nein“, auch wenn Ihre Institution in der Vergangenheit bereits im BSI registriert und Ihnen eine Institutions-ID zugeteilt wurde.

☐ Ja ☒ Nein

Angaben zur Unternehmensgröße

Hinweis zur Berechnung der Angaben
Die Angaben, die für die Berechnung der Mitarbeiterzahl und der finanziellen Schwellenwerte herangezogen werden, beziehen sich auf den letzten Rechnungsabschluss und werden auf Jahresbasis berechnet. Sie werden vom Stichtag des Rechnungsabschlusses an berücksichtigt. Die Höhe des herangezogenen Umsatzes wird abzüglich der Mehrwertsteuer (MwSt.) und sonstiger indirekter Steuern oder Abgaben berechnet (vgl. [Art. 4. 2003/361/EG](#)).

Wie viele Mitarbeiter werden in Ihrem Unternehmen beschäftigt? *

☒ weniger als 50 ☐ mind. 50 ☐ mind. 250

Welchen Jahresumsatz erzielt Ihr Unternehmen? *

☒ weniger als 10 Mio. € ☐ mind. 10 Mio. € ☐ mind. 50 Mio. €

Welche Jahresbilanz erzielt Ihr Unternehmen? *

☒ bis 10 Mio. € ☐ über 10 Mio. bis 43 Mio. € ☐ über 43 Mio. €

Angaben zu Sektor, Branche und die Einrichtungsart

EINRICHTUNGSART 1 / 30

Sektor *

Bitte auswählen

Branche

Bitte auswählen

Einrichtungsart

Bitte auswählen

In welchen Mitgliedsstaaten der EU werden Dienste der benannten Einrichtungsart erbracht? *

Bitte eingeben oder auswählen

Durch welche Bundesbehörde in Deutschland ist Ihre Einrichtungsart beaufsichtigt? *

Die richtige Aufsichtsbehörde ergibt sich nicht aus dem BSIg selbst, sondern aus dem jeweiligen sektorspezifischen Fach- und Zuständigkeitsrecht. Unternehmen sollten daher an ihre bestehende fachrechtliche Aufsicht anknüpfen.

Bitte beachten Sie, dass das Bundesamt für Sicherheit in der Informationstechnik keine Aufsichtsbehörde gem. § 33 Abs. 1 Nr. 5 BSIg ist.

Bitte geben Sie den Namen Ihrer Aufsichtsbehörde ein.

Bitte eingeben oder auswählen

Falls zutreffend, durch welche Landesbehörde in Deutschland ist Ihre Einrichtungsart beaufsichtigt? 0/500 Zeichen

+ Weitere Einrichtungsart hinzufügen

Registrierungsprozess: BSI-Portal / IV



Ihre Einstufung

Bitte füllen Sie alle obigen Formularfelder aus um eine Einstufung nach NIS-2 zu erhalten.

☐ Ich bin mit der Einstufung nicht einverstanden und möchte diese auf eigene Verantwortung hin anpassen.

Ihre NIS-2-Einstufung *

Auswählen

Allgemeine Angaben zum Unternehmen

Name der Einrichtung *

R.IT GmbH

Rechtsform

Gesellschaft mit beschränkter Haftung

Registerart

Handelsregister, Abteilung B

Registernummer

6984

Registergericht

Amtsgericht Bochum

Website-URL

NIS-2 Kontaktstelle

1 Für den Austausch von Informationen ist eine NIS-2 Kontaktstelle zum BSI zu benennen. Die Angabe eines Funktionspostfachs, d. h. keiner persönlichen E-Mail-Adresse, wird empfohlen, um die Erreichbarkeit zu den üblichen Geschäftszeiten zu gewährleisten. An diese Adresse schickt das BSI IT-Sicherheitsinformationen.

Name der Organisationseinheit * 0/130 Zeichen

Straße Hausnummer

Lise-Meitner-Allee 37

PLZ * Stadt *

44801 Bochum

Postfach

Land

DE: Deutschland

Telefonnummer *

Bitte geben Sie die Telefonnummer im internationalen Format an. Beispiele: +4930123456789, +4930123456-789

+4930123456-789

Alternative Telefonnummer

+4930123456-789

E-Mail-Adresse der Organisationseinheit 1/10 *

NIS-2 Kontaktpersonen

1 Im Bereich der NIS-2 ist für den Austausch von Informationen eine Kontaktperson zu benennen die zum Thema NIS-2 aussagefähig ist. Die Angabe eines Funktionspostfachs, d. h. keiner persönlichen E-Mail-Adresse, wird empfohlen, um die Erreichbarkeit zu gewährleisten. Mit der Kontaktperson wird in der Regel zu Aspekten der NIS-2, bei Vorfällen oder bei organisatorischen Fragen der Kontaktstelle telefoniert.

ERKLÄRUNG ZUM DATENSCHUTZ

☐ Wir setzen die Mitarbeiter/innen darüber in Kenntnis, dass wir sie auf dem BSI-Portal als Kontaktperson benennen.

KONTAKTPERSON 1/10

Vorname *

Tobias

Nachname *

Rademann

Rolle oder Funktion 0/255 Zeichen

E-Mail-Adresse *

Telefonnummer *

Bitte geben Sie die Telefonnummer im internationalen Format an. Beispiele: +4930123456789, +4930123456-789

+4930123456-789

Alternative Telefonnummer

Bitte geben Sie die Telefonnummer im internationalen Format an. Beispiele: +4930123456789, +4930123456-789

+4930123456-789

NIS-2 Registrierung

Bitte geben Sie die öffentlichen IP-Adressbereiche Ihrer Einrichtung an

☐ Die Einrichtung hat keinen öffentlichen statischen IP-Adressbereich

IP-Adressbereiche * 0/6000 Zeichen

Geben Sie IPv4- oder IPv6-Netzbereiche im CIDR-Format (Netzadresse/Netzmaske) bzw. einzelne IPv4- oder IPv6-Adressen ein und trennen Sie mehrere Einträge mit Kommata. Beispiele: 1.2.3.4, 1.2.3.0/24, 2001:4860:4860::/48. Sie können beliebig viele IP-Adressen und Netzbereiche eingeben. Hinweis: IP-Adressen und Subnetze aus privaten oder reservierten IP-Adressbereichen (z.B. 10.0.0.0/8, 192.168.0.0/16 oder fc00::/7) sind nicht zulässig und werden bei der Validierung zurückgewiesen.

Alle Informationen zum Umgang mit Ihren personenbezogenen Daten finden Sie in der [Datenschutzerklärung](#).

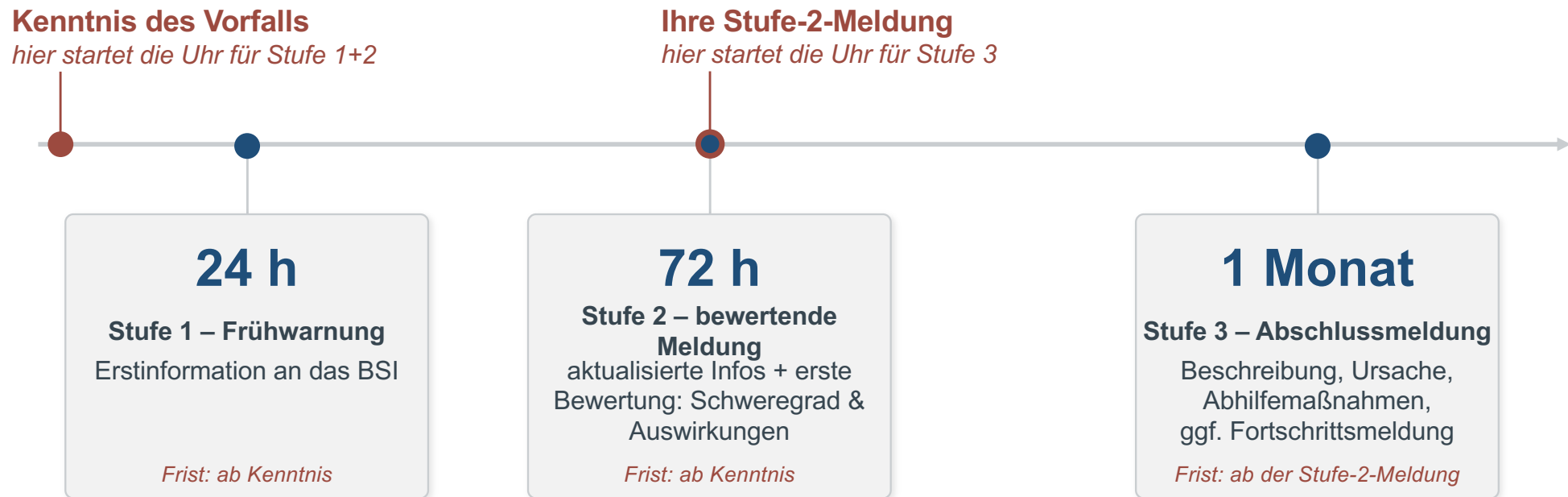
Abbrechen

Registrierung abschließen



Wenn es passiert: melden

Meldefristen für erhebliche Sicherheitsvorfälle



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

BSI: melden eines Sicherheitsvorfalls



The screenshot shows the BSI-Portal interface for a user named Rademann R. The page title is 'Meldungen von RiT GmbH'. A sidebar on the left contains navigation icons. The main content area is titled 'Sicherheitsvorfälle' and features a large circular graphic with a calendar icon. Below this, a message states: 'Sie haben noch keinen Sicherheitsvorfall gemeldet. Melden Sie Sicherheitsvorfälle sofort, um schnelle Reaktionen und wirksame Gegenmaßnahmen zu ermöglichen.' A button labeled 'Sicherheitsvorfall melden' is provided. A section titled 'Einhaltung von Fristen' contains text about data retention and reporting deadlines. The footer includes links for 'Impressum', 'Datenschutz', 'Nutzungsbedingungen', 'Barrierefreiheit', and 'Support', along with a 'Bildschirmfoto' button and a copyright notice for the Bundesamt für Sicherheit in der Informationstechnik (BSI) from 2026.

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 *

RiT 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?

Nachweis**p**flicht

- § 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**f**ähigkeit

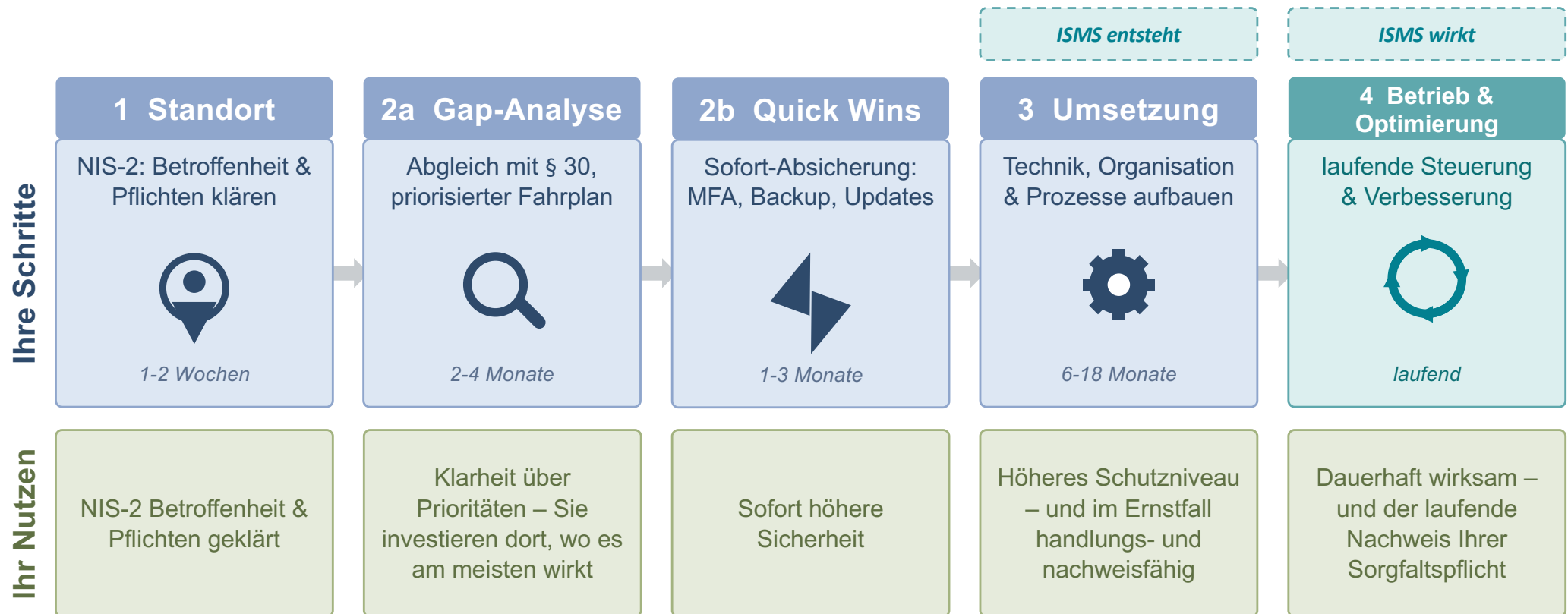
- § 30 BSIG
- gilt für **alle NIS-2-Betroffenen**
- jederzeit belegen können, dass Sie die
Maßnahmen umsetzen
- Dokumentation ist die Grundlage
- ein gefülltes, funktionsfähiges und
gepflegtes ISMS / ein ISO 27001 Zertifikat
helfen, die Nachweisfähigkeit strukturiert zu
belegen

➔ Nachweis jederzeit auf Verlangen des BSI



So fangen Sie an

klare, überschaubare Etappen



Ihr Startpunkt morgen früh:



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

NIS-2-Betroffenheitsprüfung

Sie wollen wissen, ob Ihre Einrichtung von NIS-2 betroffen ist?

➤ [HIER GEHT ES ZUR NIS-2-BETROFFENHEITSPRÜFUNG](https://betroffenheitspruefung-nis-2.bsi.de/)

Hinweis: Selbsteinschätzung, keine rechtsverbindliche Feststellung



Was Sie mitnehmen

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!

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