fellner wratzfeld partner

NIS2 Readiness

Regulierung verstehen, Umsetzung gestalten

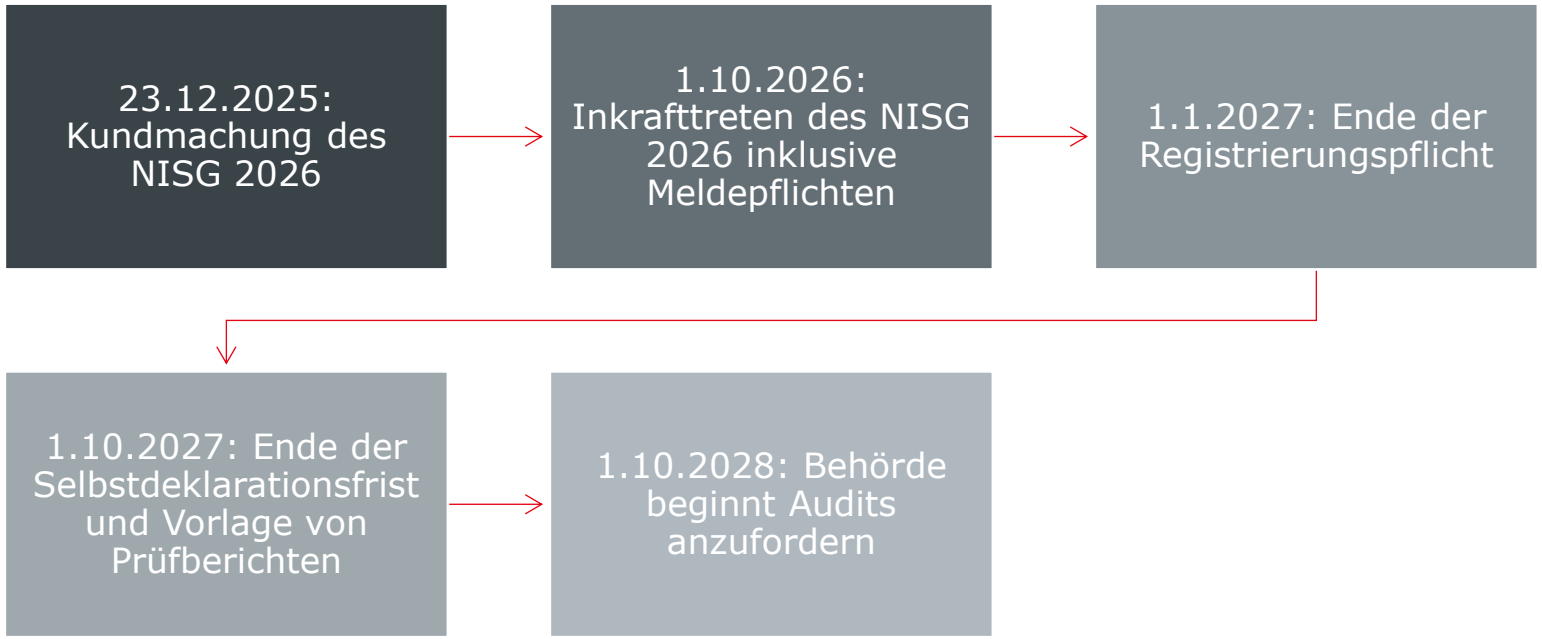
Bernhard Scherzer

Programm / Themenbereiche

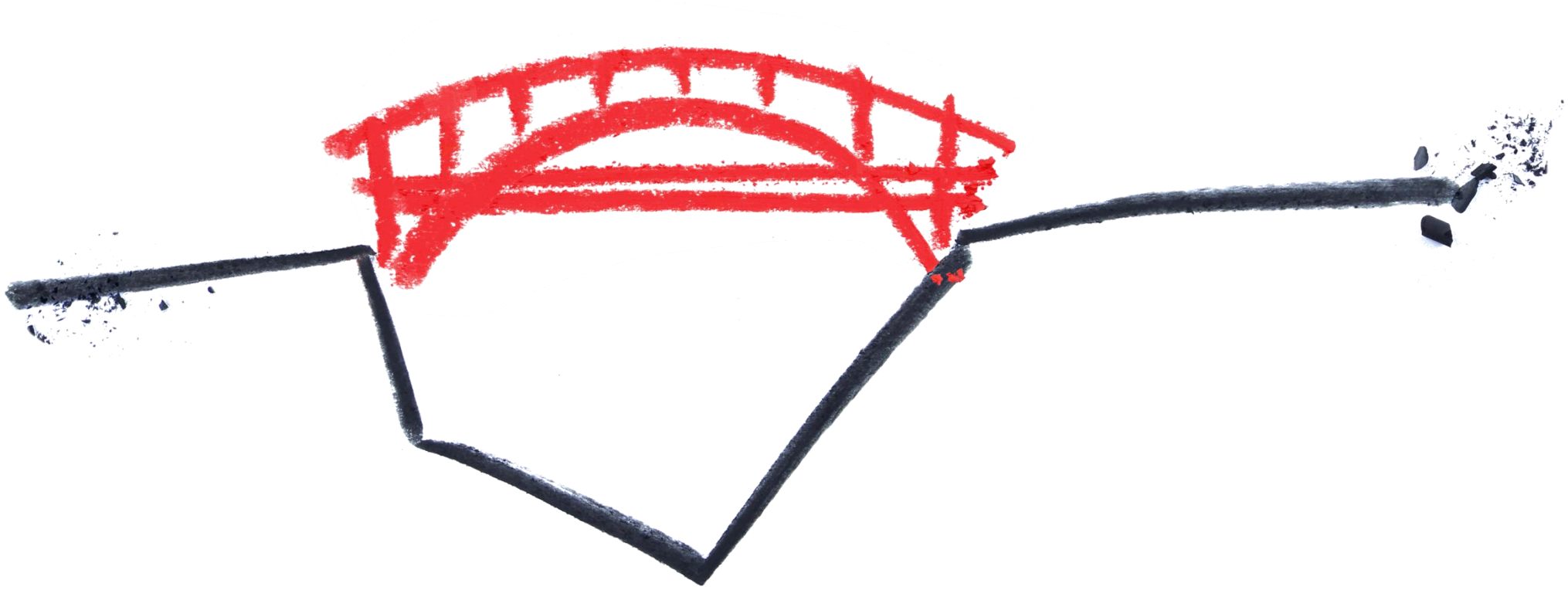
- Status Quo und Timeline
- Anwendungsbereich: Wer ist betroffen?
- NIS2 Umsetzung im Unternehmen
  - Selbsteinstufung und Registrierungspflicht
  - Risikomanagementmaßnahmen
  - Pflichten der Führungsebene
  - Berichtspflichten
  - Sanktionen
- Roadmap Compliance

Status Quo und Timeline

Timeline Umsetzung NIS-2-RL durch das NISG 2026



Anwendungsbereich: Wer ist betroffen?



Wer ist betroffen?

Das 2-Säulen-Modell

- Ratio legis: Regulierung solcher Einrichtungen, dir für das Funktionieren der Gesellschaft kritisch sind
- Sehr umfangreich – Großteil der gesamten Wirtschaft betroffen
- „Wesentliche" und „Wichtige" Einrichtungen in insgesamt 18 Sektoren und Teilsektoren (§ 2 NISG und Anlagen 1 und 2 zum NISG)
- Die Einstufung als wesentliche oder wichtige Einrichtung folgt einer Kombination aus Sektorzuordnung und Unternehmensgröße (Mitarbeiter; Umsatz oder Bilanzsumme)
    - Wesentliche Einrichtung: insbesondere große Unternehmen in den in Anlage 1 genannten Sektoren
    - Wichtige Einrichtungen: insbesondere große und mittlere Unternehmen in den in den Anlagen 1 und 2 genannten Sektoren, sofern keine wesentlichen Einrichtungen
- Pflicht zur Zusammenrechnung im Konzern

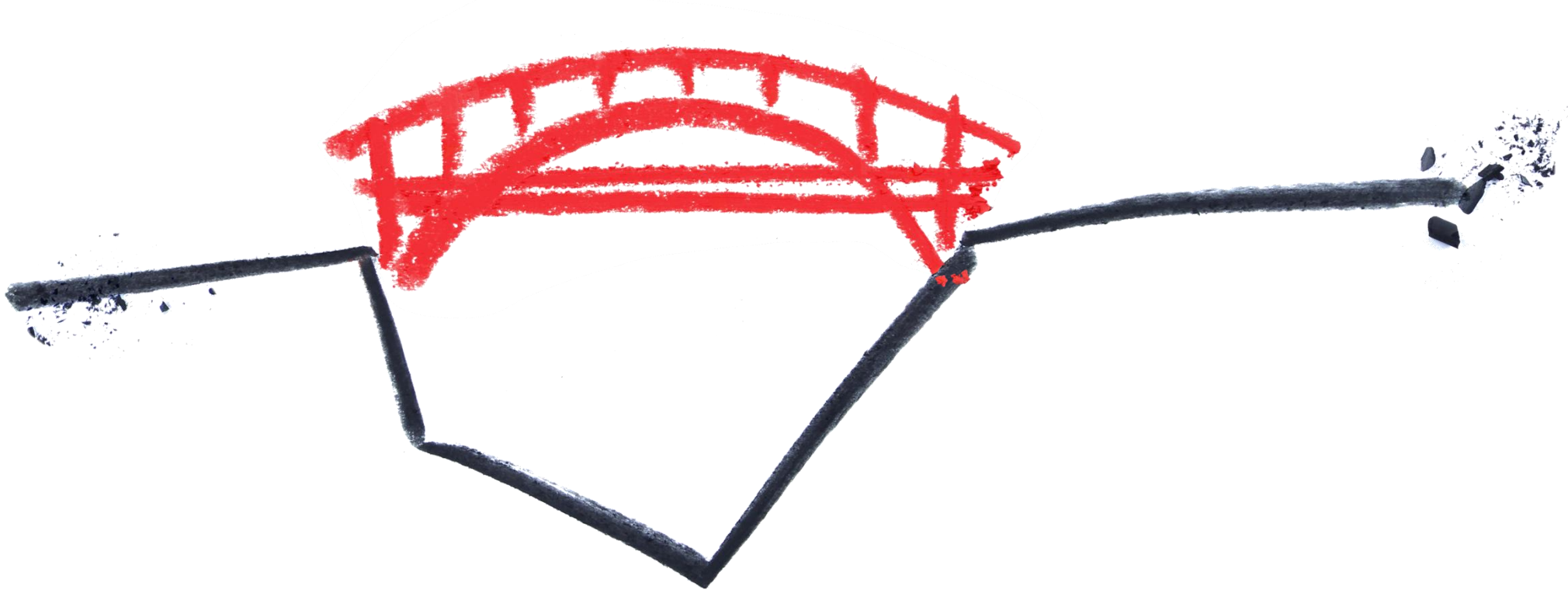
Wer ist betroffen?

Anlage 1

Anlage 2

„**KMU Empfehlung**" der Kommission linked enterprises & partner enterprises	Öffentliche Verwaltung auf Bundesebene (excl. Zentralbanken, Verteidigung, nationale Sicherheit) Unterkategorien: (i) QTSPs; (ii) DNS providers;, (iii) TLD Namenregister	Digitale Infrastruktur Unterkategorien: Anbieter von: (i) Öffentlich zugänglichen ECN; (ii) Öffentlich zugänglichen ECS	Digitale Infrastruktur Unterkategorien: nicht qualifizierte Vertrauensdienste-anbieter	Energie Verkehr	Weltraum Gesund-heit	Bankwesen Finanzmarkt IKT Dienste Trink- und Abwasser	Forschung Chemische Stoffe Warenher-stellung Digitale Dienste	Abfall Lebens-mittel Post	Öffentliche Verwaltung auf Landes-ebene	Domain-namen-registrierungsdienste
groß >= 250 oder > 50 Mio.	wesentlich	wesentlich	wesentlich	wesentlich			wichtig		wichtig	Einstufung gem § 24 NISG 2026
mittel <= 50-249 oder > 10 Mio.	wesentlich	wesentlich	wichtig	wichtig			wichtig		wichtig	
klein <= 49 und <= 10 Mio.	wesentlich	wichtig	wichtig	N/A			N/A		wichtig	

Umsetzung im Unternehmen



Umsetzung im Unternehmen

Selbsteinstufung und Registrierungspflicht

- Selbsteinstufung durch jeden Rechtsträger separat
  - Jeder Rechtsträger muss für sich selbst beurteilen, ob er auf Basis der Anlage 1 oder Anlage 2 sowie der Unternehmensgröße (Mitarbeiter; Umsatz oder Bilanzsumme) als „wesentliche" oder „wichtige" Einrichtung gilt.
- Keine Teil- oder Bereichsausnahmen für Nebentätigkeiten oder interne Abteilungen
- Registrierung bei der Cybersicherheitsbehörde
  - Nach der Selbsteinstufung muss sich jeder Rechtsträger bei der Cybersicherheitsbehörde registrieren.
- Kein Konzernprivileg - Jeder Rechtsträger separat
  - Die Registrierungspflicht gilt pro Rechtsträger (gemäß der einrichtungsbezogenen Einstufung)

Die „Konzernfalle“: Intra-Group-IT-Servcies

- Weite Definition „Anbieter verwalteter Dienste“ (managed services provider)
- Jede Art von Verwaltung von IT-Assets gelten als „managed services“
  - IT-Services
  - Von der Konzerngesellschaft für andere Konzerngesellschaften verwaltete Computerhardware
  - Hotline etc
- Kein Konzernprivileg: Die konzerninterne Erbringung von managed services wird so behandelt, als ob sie am freien Markt angeboten würden, weshalb die bloße konzerninterne Erbringung von managed services eine Regulierung auslösen kann.

Umsetzung im Unternehmen

Risikomanagementmaßnahmen

NISG regelt detailliert, was gefordert ist, dazu zählen unter anderem:

- Vulnerability Management: Umsetzung regelmäßiger Sicherheitsaktualisierung und Maßnahmen zur Behebung von Schwachstellen (inkl. Patch-Management) Notfall- und Krisenmanagement
- Reduktion von Angriffsflächen durch Maßnahmen der Cyberhygiene, insbesondere Verwaltung von Software, Diensten und Benutzerberechtigungen
- Sicherheitsmaßnahmen für Endgeräte, Netzwerke und Cloud-Umgebungen im Rahmen der Vorgaben zu Entwicklung, Erwerb und Wartung von Netz- und Informationssystemen
- Lieferkettensicherheit:
  - Vertragliche Vereinbarungen mit direkten Lieferanten/Dienstleistern
  - Gesamte Lieferkette vertraglich berücksichtigen
- Awareness und Schulungen

Umsetzung im Unternehmen

Governance-Pflichten der Führungsebene

- Aktive Überwachung und Sicherstellung der Compliance
- Schulungen
  - verpflichtende Cybersicherheitsschulungen für Leitungsorgane
- Bereitstellung der notwendigen Ressourcen
- Die Pflichten (Verantwortlichkeit) der Leitungsorgane sind nicht delegierbar.

Umsetzung im Unternehmen

Berichtspflichten

- Berichtspflicht nach Kenntnisnahmen eines „*erheblichen*“ Cybersicherheitsvorfalls
  - Ein Cybersicherheitsvorfall ist *erheblich*, wenn er konkrete Auswirkungen auf die Erbringung der regulierten Tätigkeit hat oder gehabt haben könnte:
    - Bspw. wenn er schwerwiegende Betriebsstörungen der erbrachten Dienste der Einrichtung oder schwerwiegende finanzielle Verluste für die betreffende Einrichtung verursacht hat oder verursachen kann, oder
    - andere natürliche oder juristisch Personen durch erhebliche materielle oder immaterielle Schäden beeinträchtigt hat oder beeinträchtigen kann.
  - Welche Geschäftsabteilung und welche Systeme sind betroffen? Berühren diese den regulierten Bereich?
- Empfänger des Berichts ist das zuständige Computer Emergency Response Team (CSIRT), das den Bericht an die Cybersicherheitsbehörde weiterleitet.

Umsetzung im Unternehmen

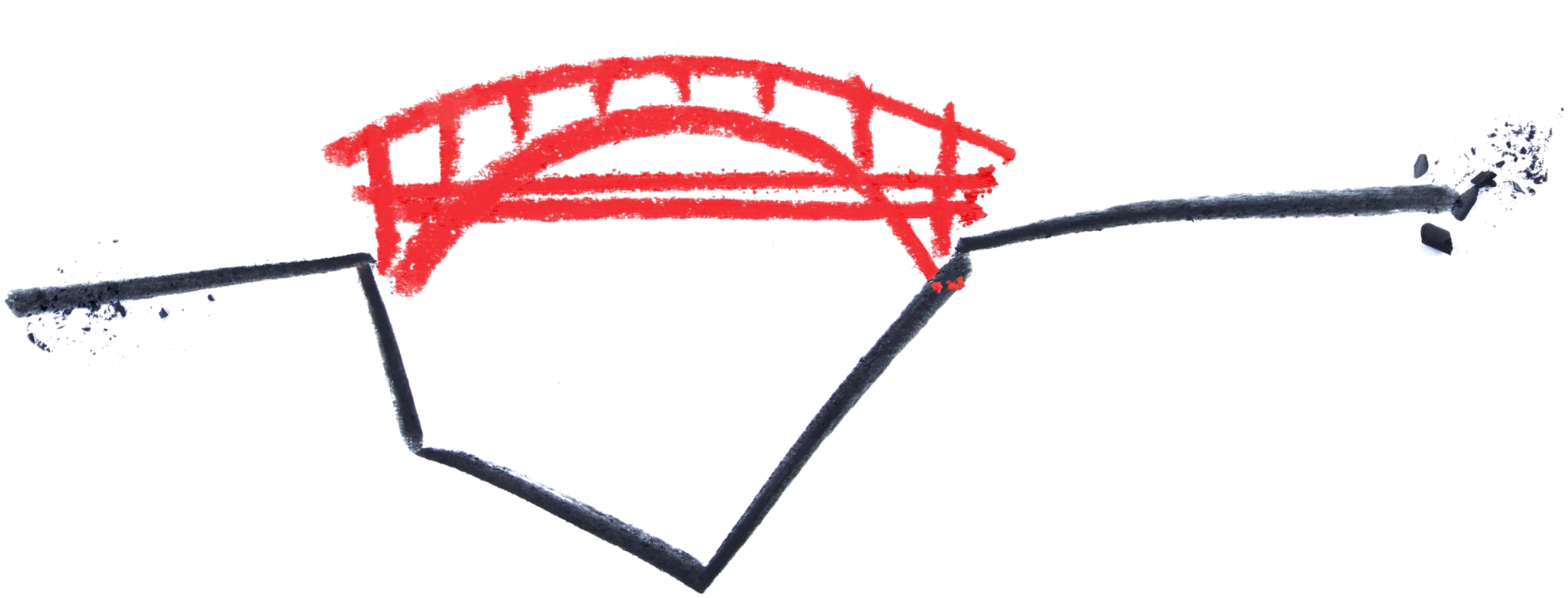
Berichtspflichten

- Fristen für Berichtspflichten an Behörde nach Kenntnisnahme:
  - 24 Stunden: Binnen 24 Stunden muss eine Frühwarnung an das zuständige Computer Emergency Response Team (CSIRT) ergehen. Diese enthält eine Ersteinschätzung und Verdachtsmomente, insb hinsichtlich rechtswidriger Handlungen und grenzüberschreitender Auswirkungen.
  - 72 Stunden: Nach drei Tagen ist dem CSIRT die eigentliche, zu diesem Zeitpunkt so detailliert wie mögliche Meldung mit einer aktualisierten Bewertung von Schweregrad und Auswirkungen zu übermitteln.
  - 1 Monat: Spätestens einen Monat nach Übermittlung der 72-Stunden-Meldung ist dem CSIRT der Abschlussbericht zu übermitteln.
- Bei erheblichen Vorfällen, sofern die Erbringung des jeweiligen Dienstes beeinträchtigt wurde, müssen die Empfänger der regulierten Dienste unverzüglich über den Vorfall unterrichtet werden, soweit möglich inkl aller Maßnahmen oder Abhilfemaßnahmen, die sie selbst als Reaktion darauf ergreifen können.

fellner wratzfeld partner

Sanktionen

Geldbußen und operative Zwangsmaßnahmen



Sanktionen

Geldbußen

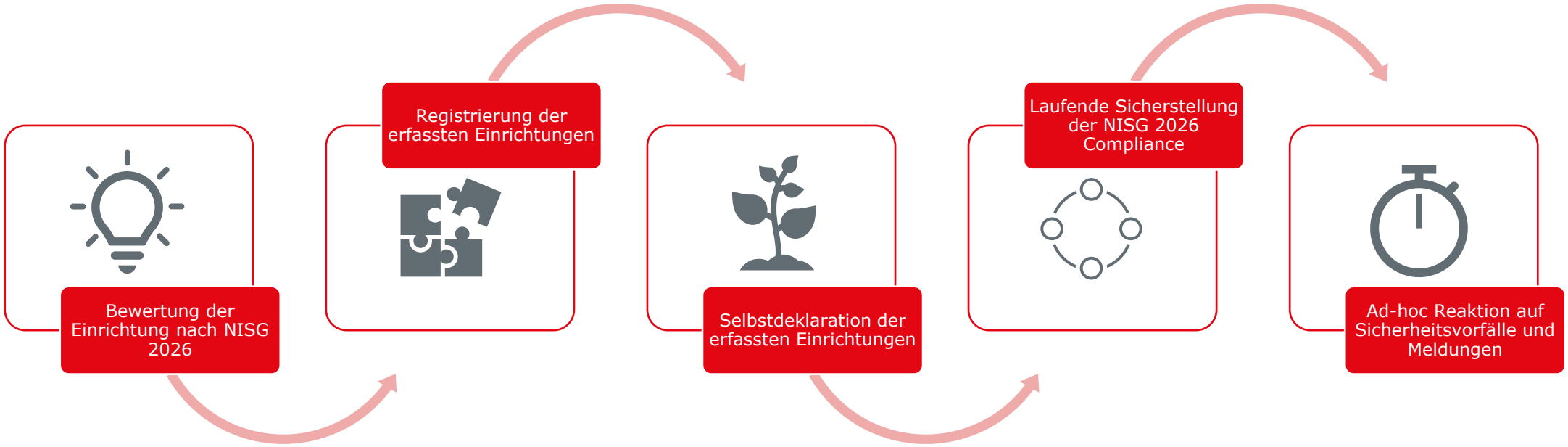
- Wesentliche Einrichtungen: Höchststrafen bis zu EUR 10 Mio oder 2 % des weltweiten Vorjahresumsatzes.
- Wichtige Einrichtungen: Höchststrafen bis zu EUR 7 Mio oder 1,4 % des weltweiten Vorjahresumsatzes.
- Strafdrohung bis EUR 50.000,-- (im Wiederholungfall EUR 100.000,--) ua bei verspäteter/unrichtiger Registrierung oder Selbstdeklaration
- Subsidiäre Haftung der Geschäftsführung

Sanktionen

Operative Zwangsmaßnahmen

- Wesentliche Einrichtungen:
  - Behördliche Anordnung von Maßnahmen zur Verhütung/Behebung eines Cybersicherheitsvorfalls
  - Benennung eines Überwachungsbeauftragten
  - Temporäre Aussetzung der Zertifizierung oder Genehmigung
  - Vorübergehende Untersagung der Wahrnehmung von Leitungsaufgaben durch Leitungsorgane/rechtliche Vertreter
- Wichtige Einrichtungen:
  - Behördliche Anordnung von Maßnahmen zur Verhütung/Behebung eines Cybersicherheitsvorfalls

Compliance Roadmap



Vortragende

Bernhard Scherzer
Rechtsanwalt
T: +43 1 53770-453
E: bernhard.scherzer@fwp.at

Zum Juristenprofil
Zum LinkedIn Profil

Josef Peer
Partner
T: +43 1 53770-463
E: josef.peer@fwp.at

Zum Juristenprofil
Zum LinkedIn Profil

Kontakt

Fellner Wratzfeld & Partner
Schottenring 12
1010 Vienna

+43 (1) 537 70-0

office@fwp.at

www.fwp.at