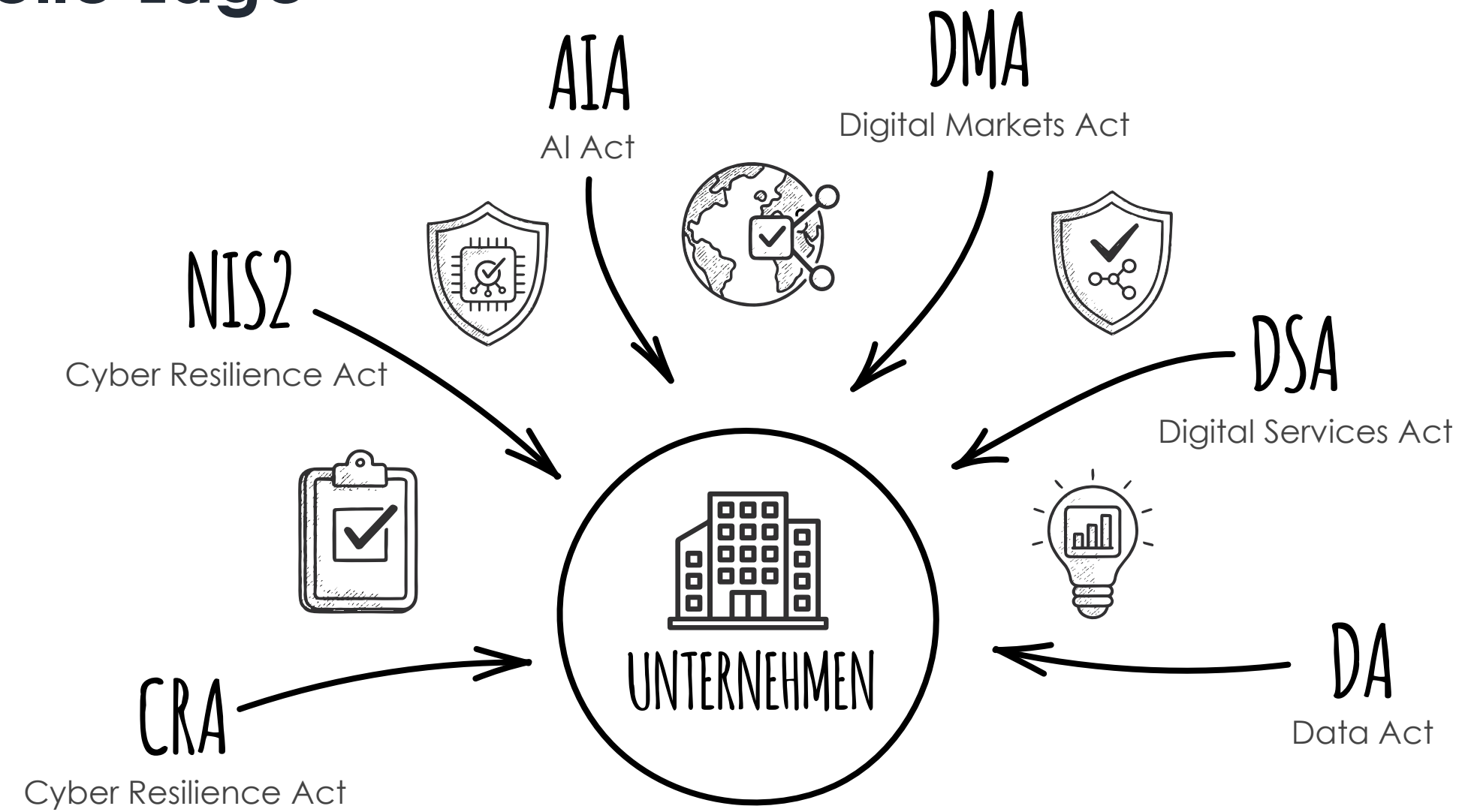
amerdis
CONSULTING & IT-SOLUTIONS

Aktuelles aus der Welt der **IT-Sicherheitsregulatorik**

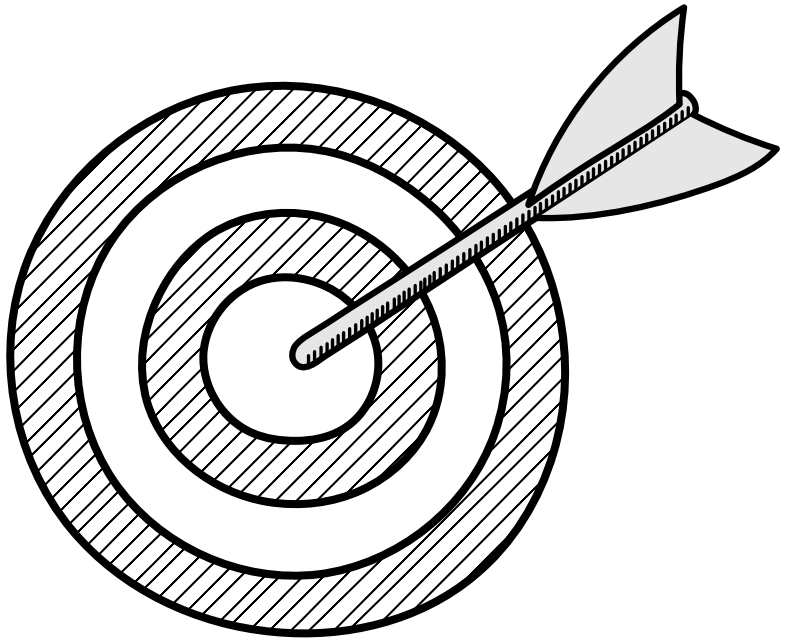
AGENDA

1. **Aktuelle Lage:** EU Technologie Regulierung
2. **Überblick über NIS2**
3. **NIS2:** Betroffene Unternehmen & Anforderungen
4. **NIS2:** Was wird gefordert?
5. **Sanktionen und Meldepflichten**
6. **Cyber Resilience Act (CRA)**
7. **Vergleich NIS2 vs. CRA**
8. **Auswirkungen auf Unternehmen**
9. **Vorgehensmodell**

Aktuelle Lage



Überblick NIS2

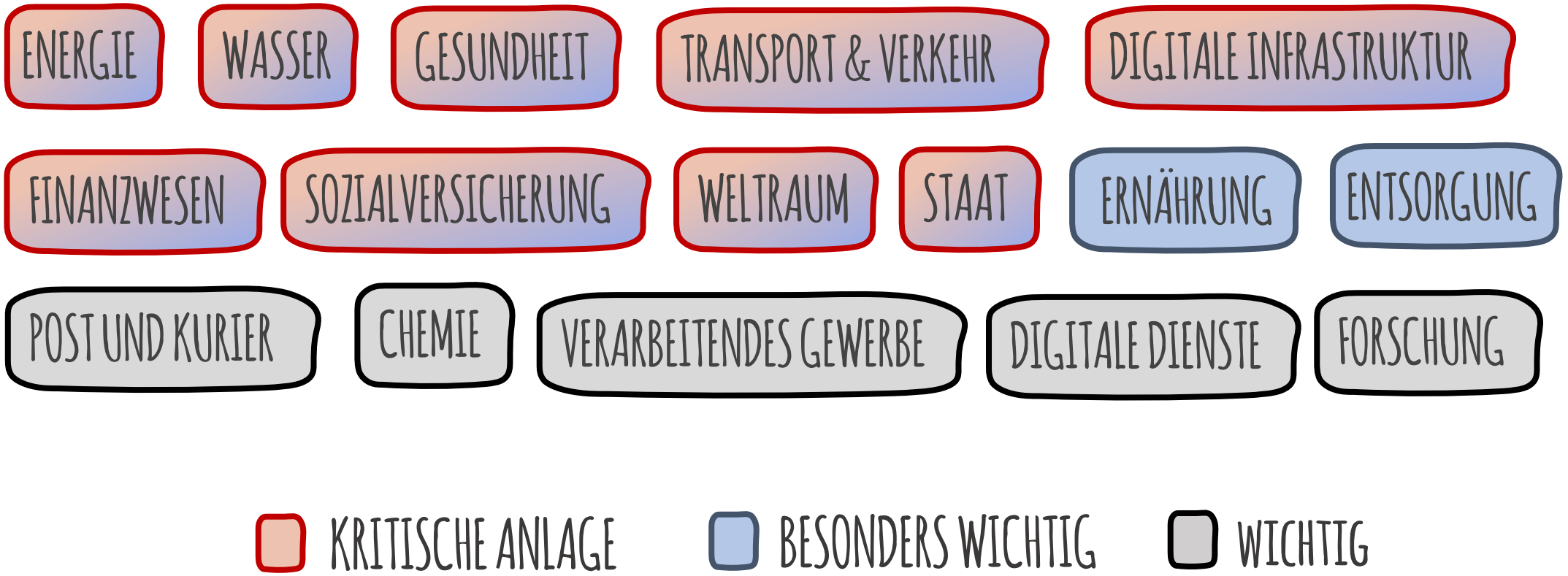


- Richtlinie: verabschiedet Dezember 2023, muss durch nationale Gesetze durch die Mitgliedstaaten umgesetzt werden
- Nationale Implementierung in Deutschland jüngst verabschiedet.

- Wesentlicher Inhalt (aus der Perspektive der Wirtschaft):
  Anforderung für Unternehmen die für die Allgemeinheit wichtige Dienste anbieten, **angemessene IT-Sicherheitsmaßnahmen** umzusetzen.
  Ebenso wurde eine Geschäftsführerhaftung nun gesetzlich festgelegt

NIS2: Betroffene Unternehmen

» Mit der EU NIS2-Umsetzung und dem KRITIS-Dachgesetz ändern sich Sektoren und Betreiber ab 2025, es kommen Tausende mittlere und Großunternehmen als Einrichtungen dazu.

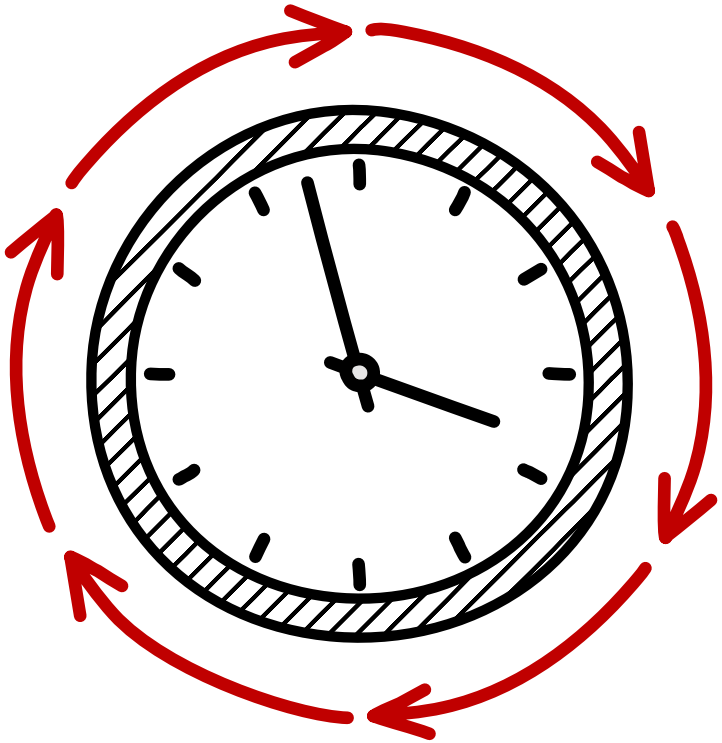


NIS2: Was wird von der Wirtschaft gefordert

Art. 21 NIS2 – Risikomanagementmaßnahmen im Bereich der Cybersicherheit:

- Wesentliche und wichtige Einrichtungen müssen technische, operative und organisatorische Maßnahmen ergreifen, um Risiken für Netz- und Informationssysteme zu beherrschen und Sicherheitsvorfälle zu minimieren.
- angemessene TOMs
- Fokus: Risikomanagement
- Angemessenheitsprinzip

NIS2: Sanktionen, Meldepflichten

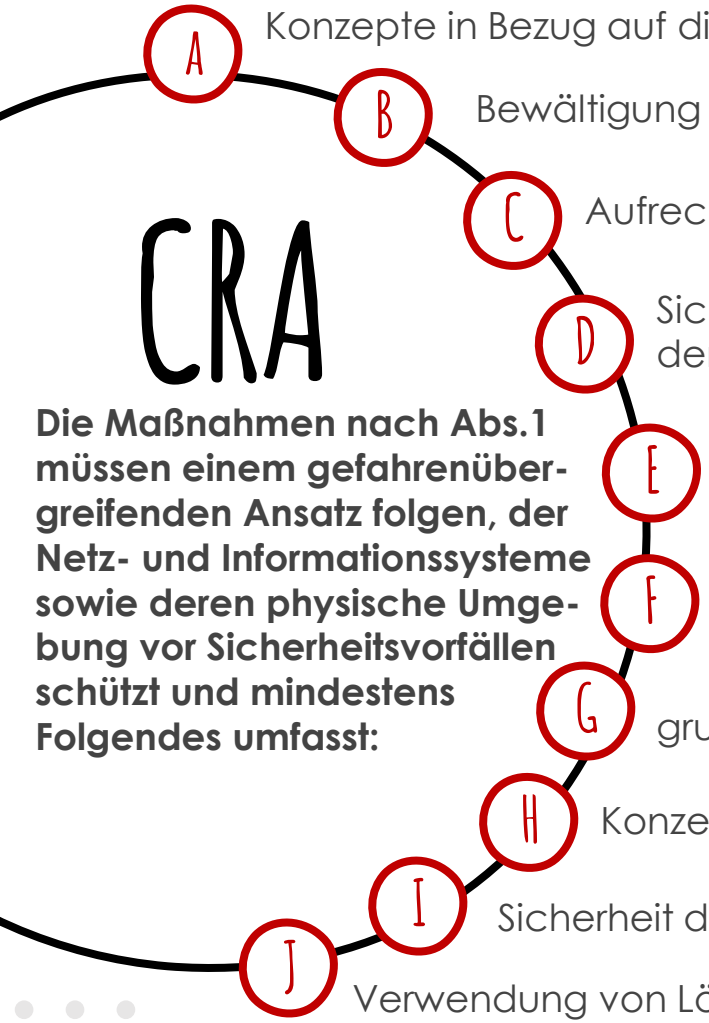


- **Meldepflichten:** Sicherheitsvorfälle müssen binnen 24 Stunden als Frühwarnung gemeldet werden, gefolgt von einem ausführlichen Bericht innerhalb von 72 Stunden und einem Abschlussbericht nach einem Monat.

- **Sanktionsrahmen:** Bei Verstößen drohen erhebliche Geldbußen, für „wichtige Einrichtungen“ bis zu 7 Mio. € oder 1,4 % des weltweiten Jahresumsatzes, für „wesentliche Einrichtungen“ bis zu 10 Mio. € oder 2 %. **Ebenso hat die Aufsicht das Recht, bei Verstößen die Umsetzung konkreter Maßnahmen anzuweisen.**

- **Persönliche Verantwortlichkeit:** Geschäftsleitungen haften für die Umsetzung von Sicherheitsmaßnahmen und können bei Pflichtverstößen persönlich sanktioniert werden (z. B. Schulungspflichten, Aufsichtspflichten).

Cyber Resilience Act (CRA)



Die Maßnahmen nach Abs.1 müssen einem gefahrenüber-greifenden Ansatz folgen, der Netz- und Informationssysteme sowie deren physische Umge-bung vor Sicherheitsvorfällen schützt und mindestens Folgendes umfasst:

A Konzepte in Bezug auf die Risikoanalyse und Sicherheit für Informationssysteme

B Bewältigung von Sicherheitsvorfällen

C Aufrechterhaltung des Betriebs, Backup-Management, Notfallwiederherstellung, Krisenmanagement

D Sicherheit der Lieferkette einschließlich sicherheitsbezogener Aspekte der Beziehungen zwischen den einzelnen Einrichtungen und ihren unmittelbaren Anbietern oder Diensteanbietern

E Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von Netz- und Informationssystemen, einschließlich Management und Offenlegung von Schwachstellen

F Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen im Bereich der Cybersicherheit

G grundlegende Verfahren im Bereich der Cyberhygiene und Schulungen im Bereich der Cybersicherheit

H Konzepte und Verfahren für den Einsatz von Kryptografie und gegebenenfalls Verschlüsselung

I Sicherheit des Personals, Konzepte für die Zugriffskontrolle und Management von Anlagen

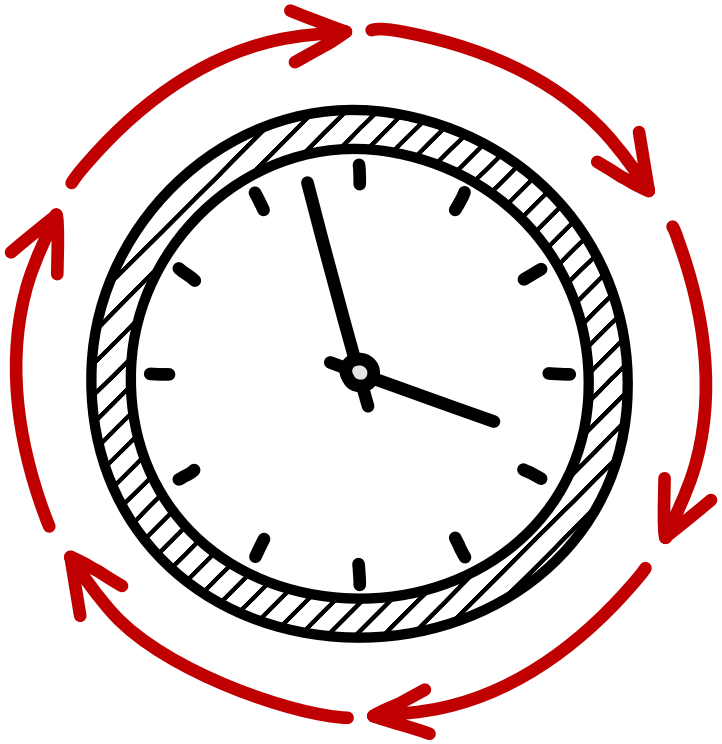
J Verwendung von Lösungen zur Multi-Faktor-Authentifizierung oder kontinuierlichen Authentifizierung, gesicherte Sprach-, Video- und Textkommunikation sowie ggf. gesicherte Notfallkommunikationssysteme innerhalb der Einrichtung

CRA: Shortfacts

- In Kraft getreten am 10. Dezember 2024
- Wesentlicher Inhalt: Angemessenes IT-Sicherheitsniveau für Digitale Produkte bzw. Produkte mit digitalen Elementen.
- Produktsicherheitsrecht, quasi das CE-Kennzeichen für Digitale Produkte

CRA: Sanktionen, Meldepflichten

- **Sicherheitsanforderungen:** Hersteller müssen für vernetzte Produkte (sowohl Hardware als auch Software) während des gesamten Lebenszyklus Sicherheits-by-Design, Risikomanagement, Schwachstellenhandling und regelmäßige Updates gewährleisten.



- **Meldepflichten:** Ausnutzbare Sicherheitslücken und schwerwiegende Vorfälle müssen innerhalb von 24 Stunden an die ENISA gemeldet werden; zudem besteht eine Pflicht zur schnellen Bereitstellung von Sicherheitsupdates für Nutzer.

- **Sanktionen:** Bei Verstößen drohen hohe Bußgelder – je nach Schwere bis zu 15 Mio. € oder 2,5 % des weltweiten Jahresumsatzes des Unternehmens. **Wesentlicher ist, die Möglichkeit Produkte die Marktzulassung zu entziehen.**

Vergleich NIS2 vs. CRA

NIS2

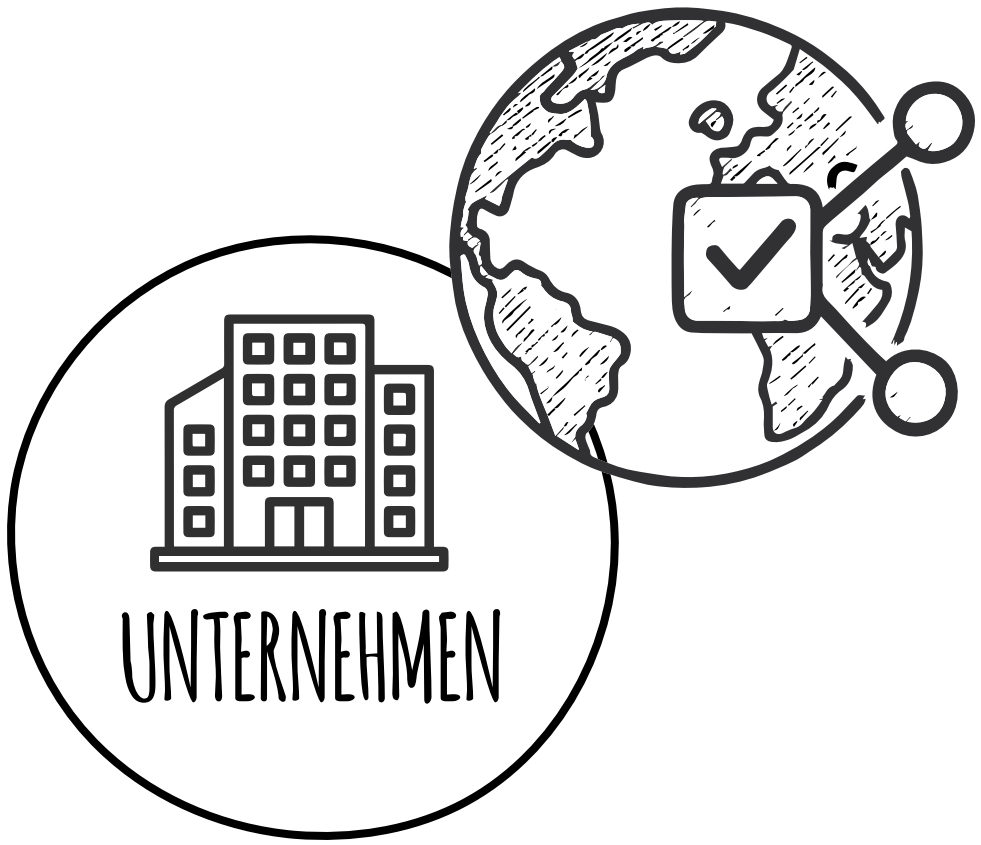
- Wesentlicher Scope ist die Sicherheit der Unternehmens-IT

CRA

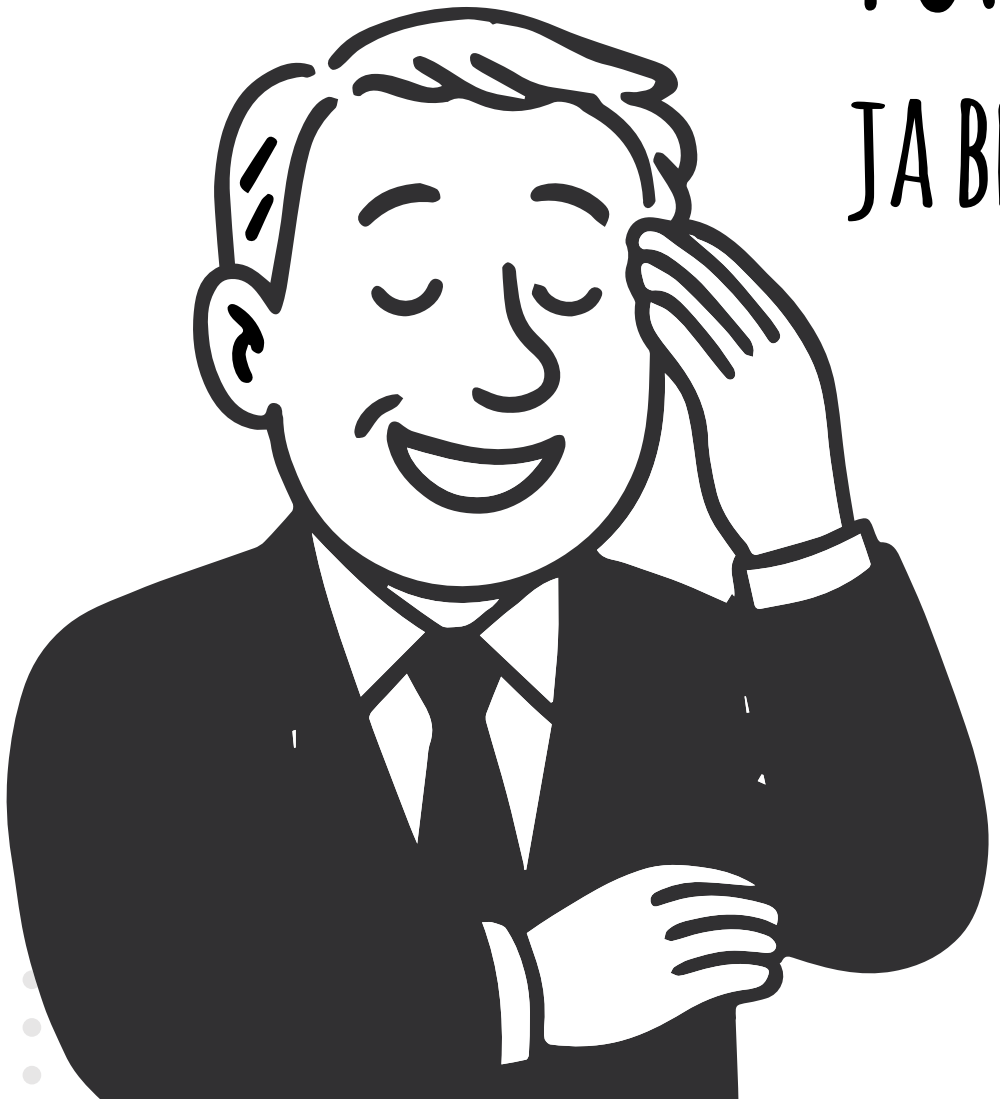
- Wesentlicher Scope ist die die IT-Sicherheit von Produkten

Selbst wenn beide Gesetze im Wesentlichen Vorgaben zur Cybersicherheit machen, ist der Bezugspunkt ein anderer. Praktisch bedeutet dies, dass Unterschiedliche Bereiche im unternehmen für die Umsetzung verantwortlich sind: IT-Sicherheit ist nicht automatisch nur Sache des CISO

Was bedeutet dies für mein Unternehmen?



- Die Anforderungen von NIS2 decken sich weitesgehend mit denen, etablierter Sicherheits Standards (wie ISO27001, IT-Grundschutz etc.)
- Weiterhin besteht im Unternehmen ein Eigeninteresse an einer soliden IT-Sicherheit. Anders (wie bzw. bei der DSGVO) besteht demnach weniger ein Interessens-konflikt zwischen Adressaten und Regulator.
- **Also: im Optimal-Fall bedeuten die neuen Regelungen nur etwas Dokumentationsaufwand, um das Bestehen einer soliden IT-Sicherheitsstruktur der Aufsicht gegenüber nachzuweisen.**



PUH, DENN IHR UNTERNEHMEN IST JA BEREITS IT-SICHERHEITSTECHNISCH TIP TOP AUFGESTELLT.

ODER?

ODER?

NIS2 Common Misconceptions

- Empirisch zeigt sich: bei genauerem Hinsehen ist die IT-Sicherheit oft dann doch nicht so gut aufgestellt wie gedacht.

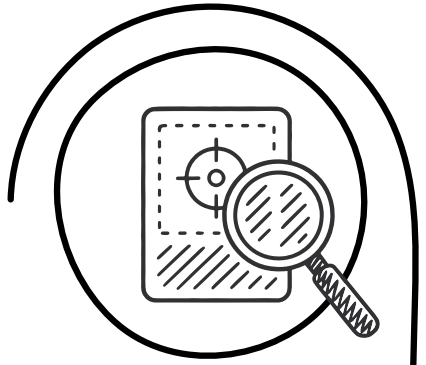
- **Man kann Regulatorik hier als freundlichen Schubs und Chance sehen: sie gibt Anlass liegen gebliebene Hausaufgaben (Phrasenalarm) mit Deadline endlich anzugehen.**

- „Wir sind ja ISO 27001 Zertifiziert, daher sind wir fein“: Grundsätzlich ja. Eine ISO oder IT-Grundschutzzertifizierung deckt 99% der NIS2 Anforderungen ab. **Wichtig ist jedoch: Welchen Scope bildet die Zertifizierung ab?** Sind sämtliche Systeme die zur Erbringung des wesentlichen Dienstes eingesetzt werden umfasst? Beispiel: Die ISO Zertifizierung eines S-Bahn Betreibers umfasst nur die IT nicht die OT.

Vorgehensmodell

Wichtig:
Das Thema IT-Sicherheit ist „Chefsache“ (auch Regulatorisch)

1. SCOPE

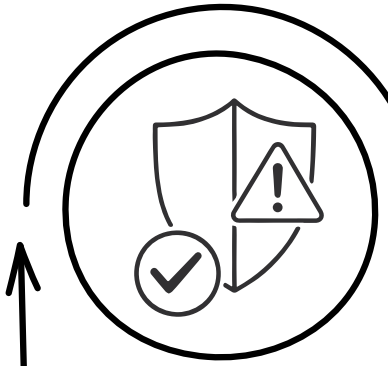


Der genaue Geltungsbereich wird festgelegt, um klar zu bestimmen, welche Systeme, Prozesse und Dienste unter die Anforderungen fallen.

2. GAP ANALYSE

Herausforderung: Identifizierte Gaps erfordern oft Abteilungs-übergreifende Maßnahmen ⇒ hoher Koordinations-aufwand

3. RISIKO-MANAGEMENT



Alle relevanten Risiken bewerten und priorisieren, um geeignete technische, organisatorische und operative Maßnahmen abzuleiten.

4. MAßNAHMENPLAN

Die definierten Sicherheitsmaßnah men werden strukturiert implementiert und dokumentiert, um die regulatorischen Vorgaben zu erfüllen.

5. MONITORING

Kontinuierlicher Überwachungs- und Verbesserungs-prozess stellt sicher, dass Sicherheits-niveau, Compliance und Meldepflichten dauerhaft eingehalten werden.

amerdis
CONSULTING & IT-SOLUTIONS

amerdis GmbH

Wienburgstraße 207

48159 Münster

Tel + 49 251 489 570-0

info@amerdis.de

www.amerdis.de