secunet

EU NIS-2 und CRA – Maßnahmen und Strategien für Industrie-unternehmen

Webinar

7. November 2023

secunet

(New) European Legislation on Security

Überblick

Alexander Schlensog
Division Industry
Essen, den 08.11.2023

Über secunet.

Deutschlands führendes Cybersecurity Unternehmen.

Digitale Souveränität und Schutz vor Cyberangriffen

Mission

Wir stärken die digitale Souveränität von Regierungen, Unternehmen und der Gesellschaft, indem wir die effektivsten IT-Sicherheitslösungen anbieten.

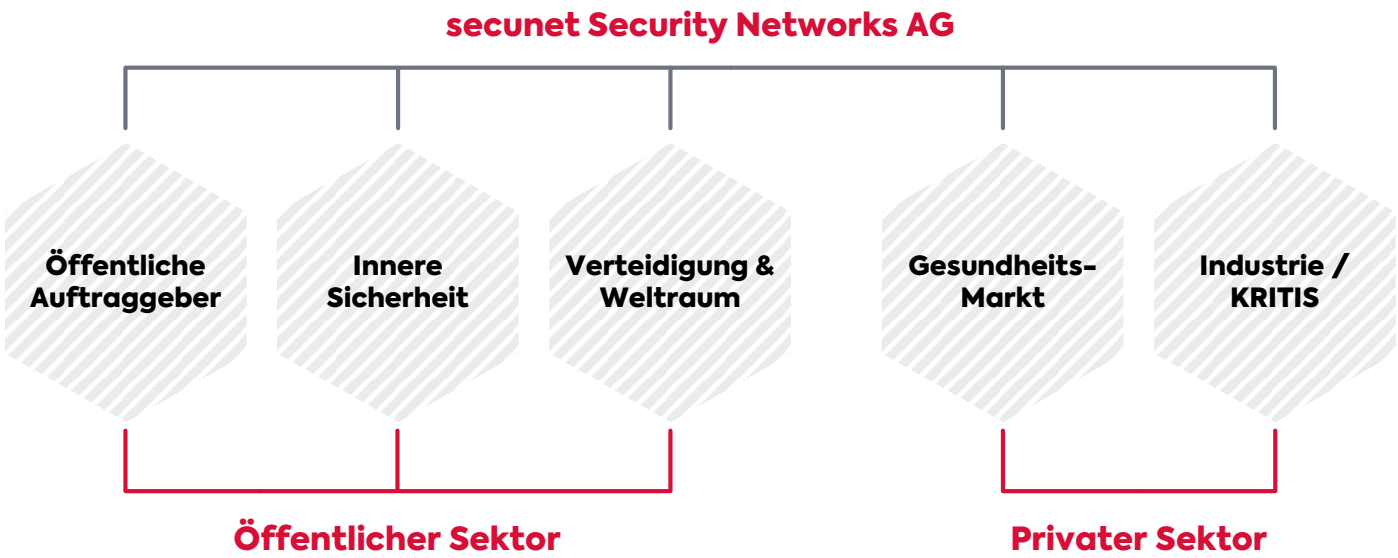
Vision

Wir glauben, dass sichere IT-Infrastrukturen das essentielle Rückgrat für den Datenschutz in unserer vernetzten Welt bilden.

secunet

secunet ist Deutschlands führendes Cybersecurity-Unternehmen. Wir schützen digitale Infrastrukturen und Identitäten.

secunet auf einen Blick –
25 Jahre Kompetenz in IT-Security



- 1.100 Mitarbeiter
- 13 Standorte
- 347 Mio. Euro Konzernumsatz in 2022
- > 500 Kunden, u.a. Bundesministerien EU und > 20 DAX-Konzerne
- Hauptaktionär: Giesecke + Devrient (75%)

Sicherheitspartner der Bundesrepublik Deutschland

Joint Venture

SecuStack
Cloud-Betriebssystem

Tochtergesellschaften

stashcat
Sicherer Business-Messenger

SysEleven
Cloud & Managed Kubernetes

Referenzen Industry (Auszug)

Sicherheitspartner der Bundesrepublik Deutschland.

Stand: Juli 2023

Agenda

01 Einleitung

02 Fokus EU NIS-2 (+ Diskussionspapier u. Werkstattgespräch BMI)

03 Fokus EU CRA

04 Fokus EU RCE

05 Was ist jetzt zu tun?

06 Wie kann secunet helfen?

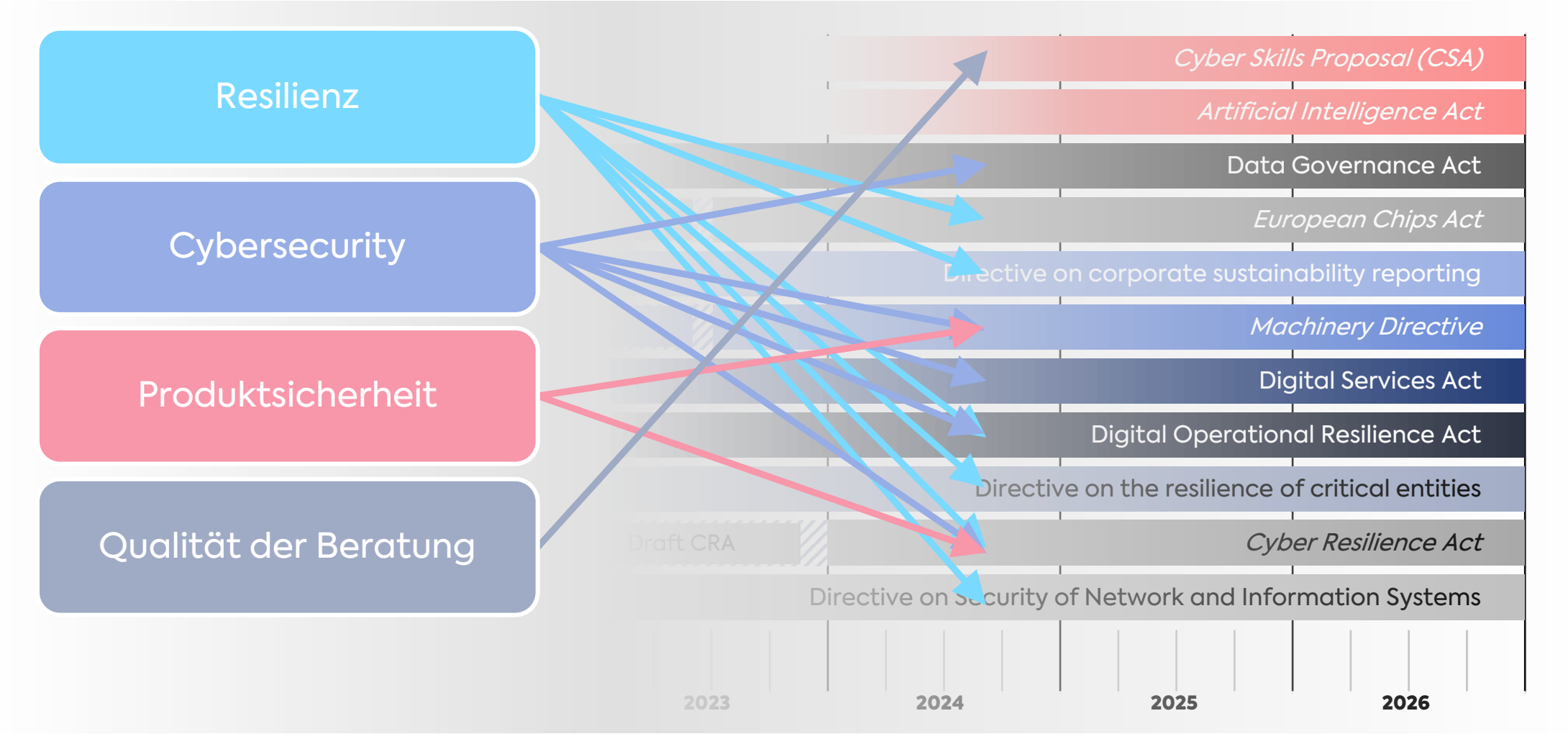
01

Einleitung

Übersicht über die neue europäische Sicherheitsgesetzgebung

Grundlagen zur Digitalen Zukunft Europas (Auszug)

Regulierungsdruck auf Industrie, Produkte und Dienstleistungen



Aktuelle Entwicklung und Zielrichtung der neuen Europäischen Security-Gesetzgebung

EU Directive on Security of Network and Information Systems (EU NIS-2 Directive)

Hoher gemeinsamer Level an Cybersecurity in der EU; neue Behörden und Befugnisse; Neuordnung und Erweiterung der betroffenen Sektoren

In Kraft seit 16.01.2023

EU Cyber Resilience Act (EU CRA)

Pflichten für Hersteller, Importeure und Distributoren von Produkten mit digitalen Elementen mit dem Ziel Anwender und die Lieferkette durch Sicherheitsprozesse und –elemente zu sichern

Gesetzgebungsprozess

EU Directive on the resilience of critical entities (EU RCE Directive)

Pflichten für Betreiber kritischer Einrichtungen mit dem Ziel der Stärkung der Resilienz; andere Begriffsdefinition; Ausweitung der Sektoren

In Kraft seit 16.01.2023

02

Überblick EU NIS-2

EU Directive on Security of Network and Information Systems

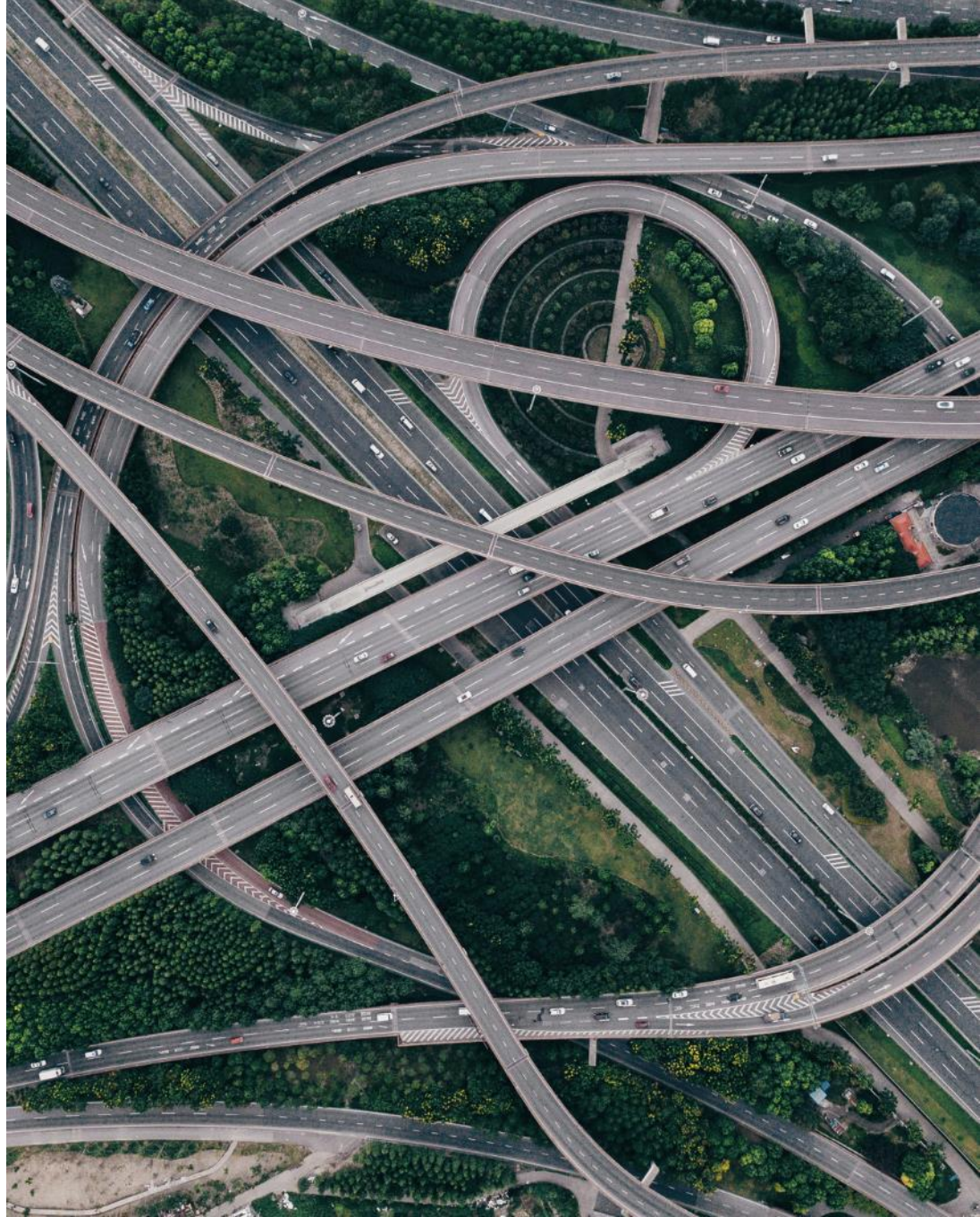
EU NIS-2

Überblick über das Gesetz

- EU **Directive** on Security of **N**etwork and **I**nformation **S**ystems (Directive (EU) 2022/2555)
- Schaffung eines hohes Cybersicherheitsniveaus auf EU-Ebene und Stärkung des Binnenmarktes
- Antwort auf steigende Bedrohungslage im Cyberraum und Notwendigkeit einer konsolidierten Handlungsfähigkeit auf EU-Ebene
- Weiterentwicklung der 2016 erlassenen EU NIS-Richtlinie (IT-Sicherheitsgesetz ist die nationale Umsetzung)
- Status: **In Kraft** seit 16. Januar 2023
- **Muss** innerhalb von 21 Monaten **in nationales Recht überführt werden** (Umsetzungsgesetz [NIS2UmsuCG] „löst“ IT-SiG 2 ab)

EU NIS-2
Ziele des Gesetzes

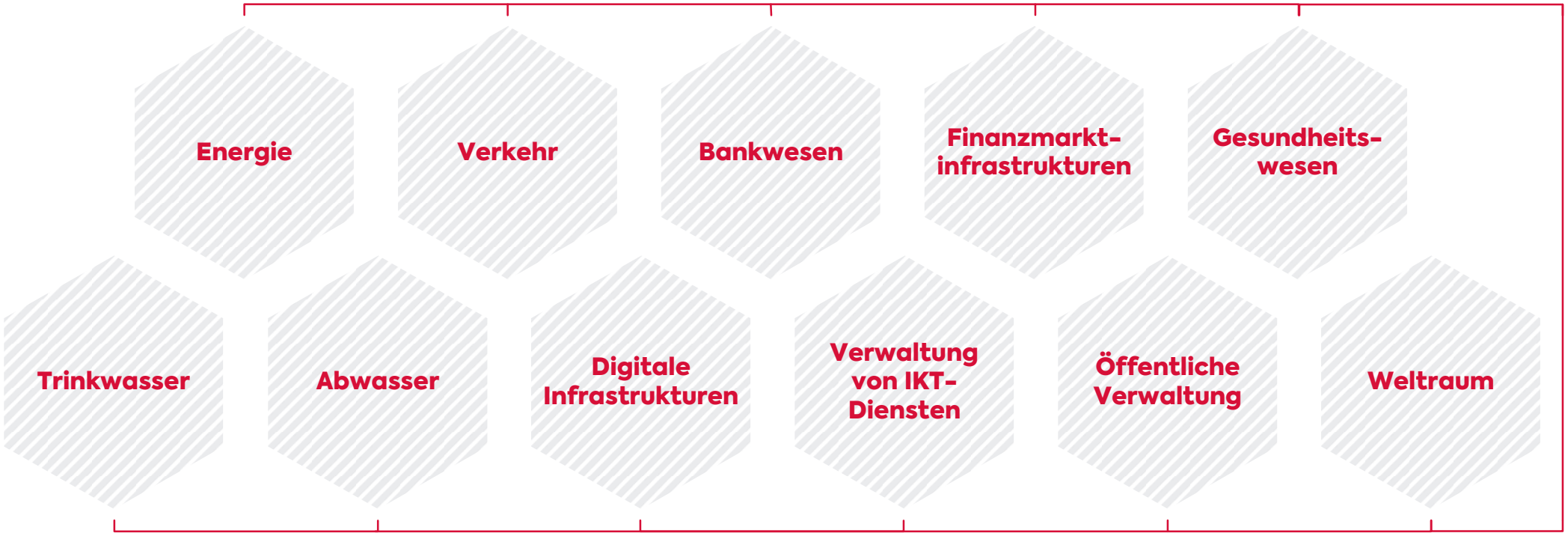
- **Übergeordnetes Ziel**
  - Verbesserung des Cybersicherheitsniveaus; Schaffung eines hohen gemeinsamen Niveaus zur Stärkung des Binnenmarktes
- **Strategische Ziele**
  - Verabschiedung nationaler Cybersicherheitsstrategien
  - Förderung der Zusammenarbeit der EU-Länder
  - Regelung von Zuständigkeiten
  - Schaffung neuer Organe
- **Ausweitung der Regelung**
  - **flächendeckenden Anwendung** auf große Teile der Wirtschaft, kein alleiniger Fokus mehr auf KRITIS-Unternehmen (siehe Anhang I und II)
- **Vorgaben zum Risikomanagement**
  - Leitungsorgane verpflichten; Stand der Technik einhalten
  - **Schutz u. Kopplung von „digitaler“ und „physischer“ Welt**
  - Minimalkonsens



EU NIS-2

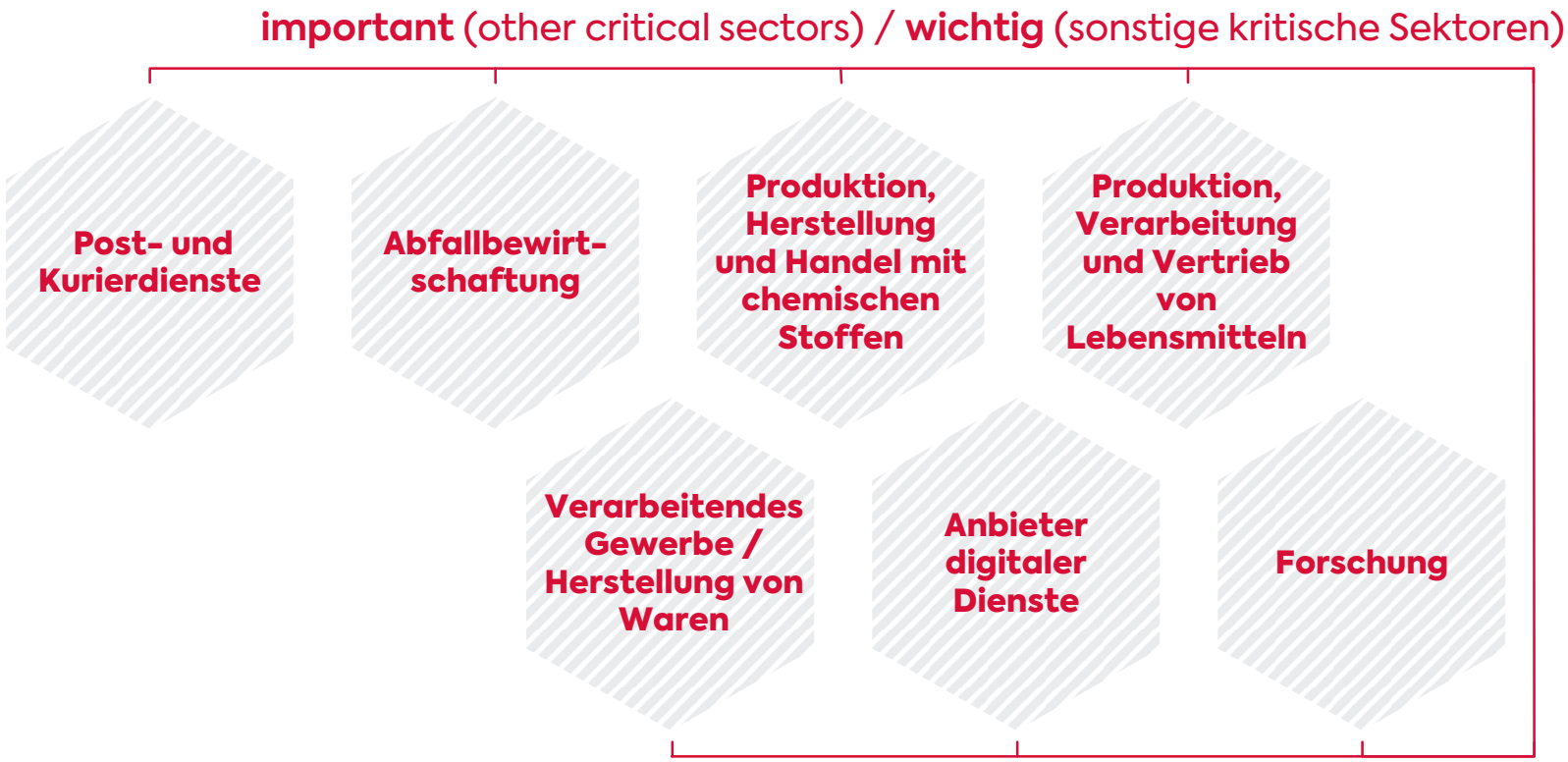
Zielgruppen des Gesetzes: **wesentliche Sektoren**

essential (sectors with high criticality) / **wesentlich** (Sektoren mit hoher Kritikalität)



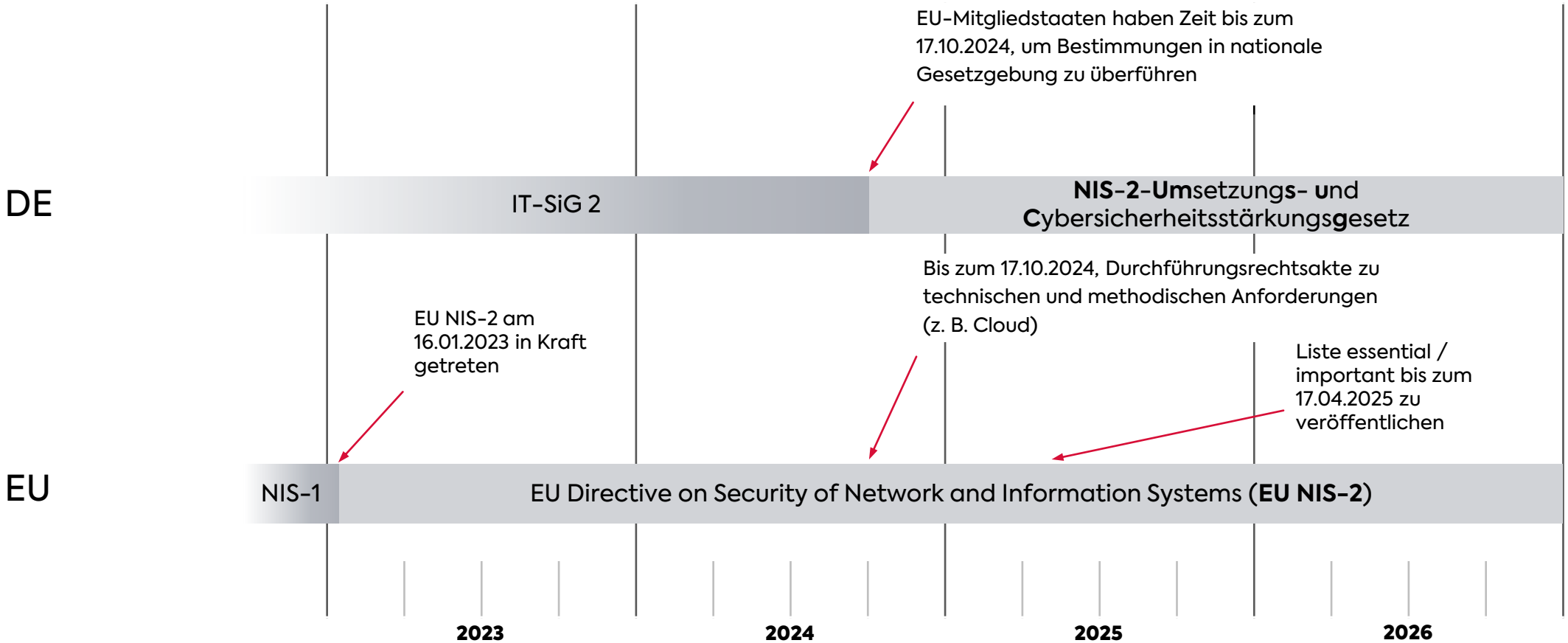
EU NIS-2

Zielgruppen des Gesetzes: **wichtige Sektoren**



EU NIS-2

Zeitlicher Ablauf und Fristen



EU NIS-2

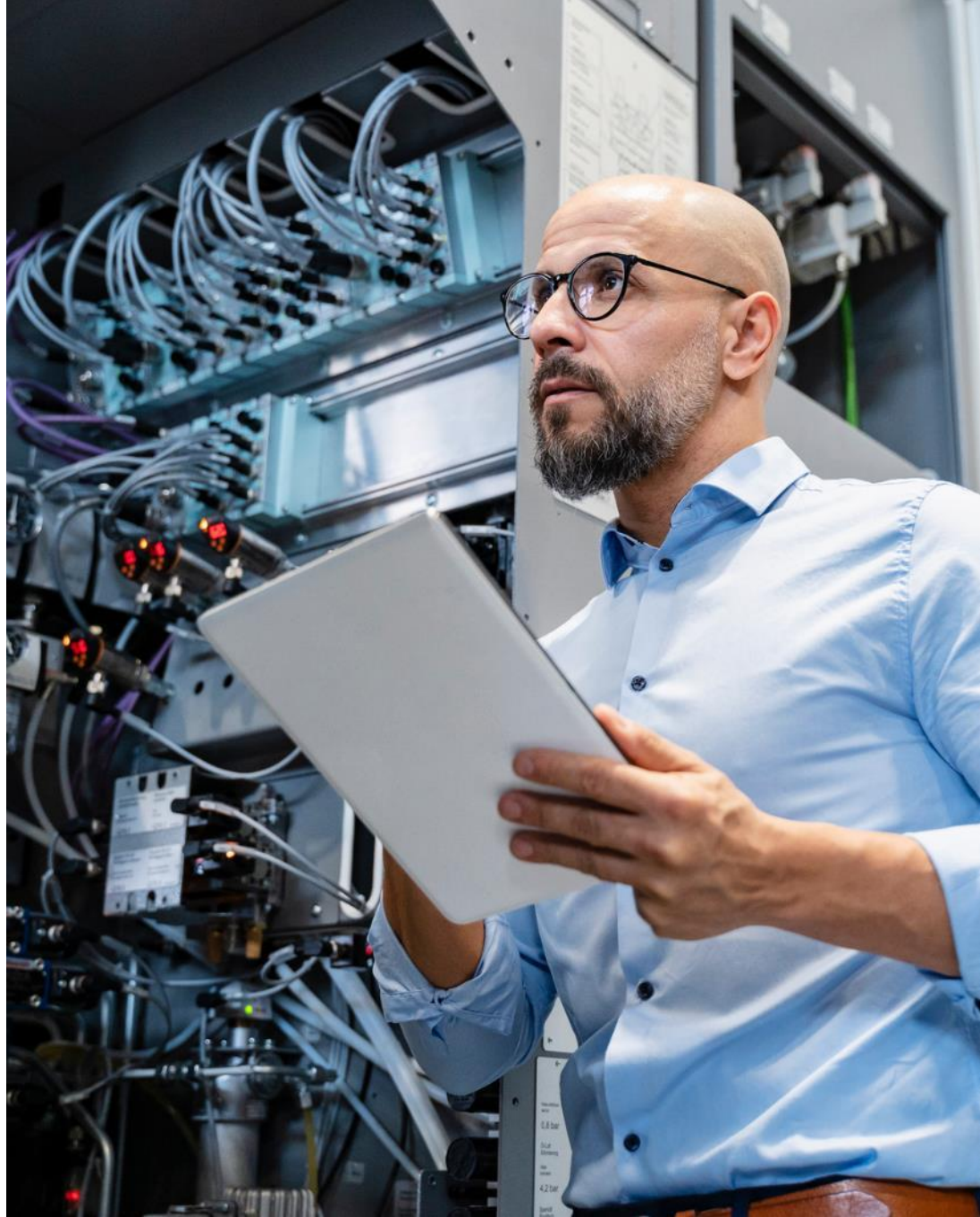
Pflichten für die Staaten

- Entwicklung nationale **Cybersicherheitsstrategie**
- Einbezug von Cybersicherheit in **Lieferkette** von IKT
- **Offenlegung** von **Schwachstellen**
- Einrichtung von Notfallteams (CSIRT)
- **Bewältigung** massiver **Cybersicherheitsvorfälle**

EU NIS-2

Behördliche Befugnisse

- Auftrag zu **wirksamer** und **risikobasierter Beaufsichtigung**
  „Wirksam, verhältnismäßig und abschreckend“
- **Umfassende Kompetenzen** wie Vor-Ort-Kontrollen, Überprüfungen (Stichproben), regelmäßige Sicherheitsprüfungen, Informations- und Datenzugang
- **Behördliche Befugnisse** wie Warnungen, Anweisungen, Geldbußen, vorübergehender Ausschluss von Leitungspersonen, Haftungsrecht gilt unverändert fort



02

Überblick NIS2UmsuCG

NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz

NIS2UmsuCG

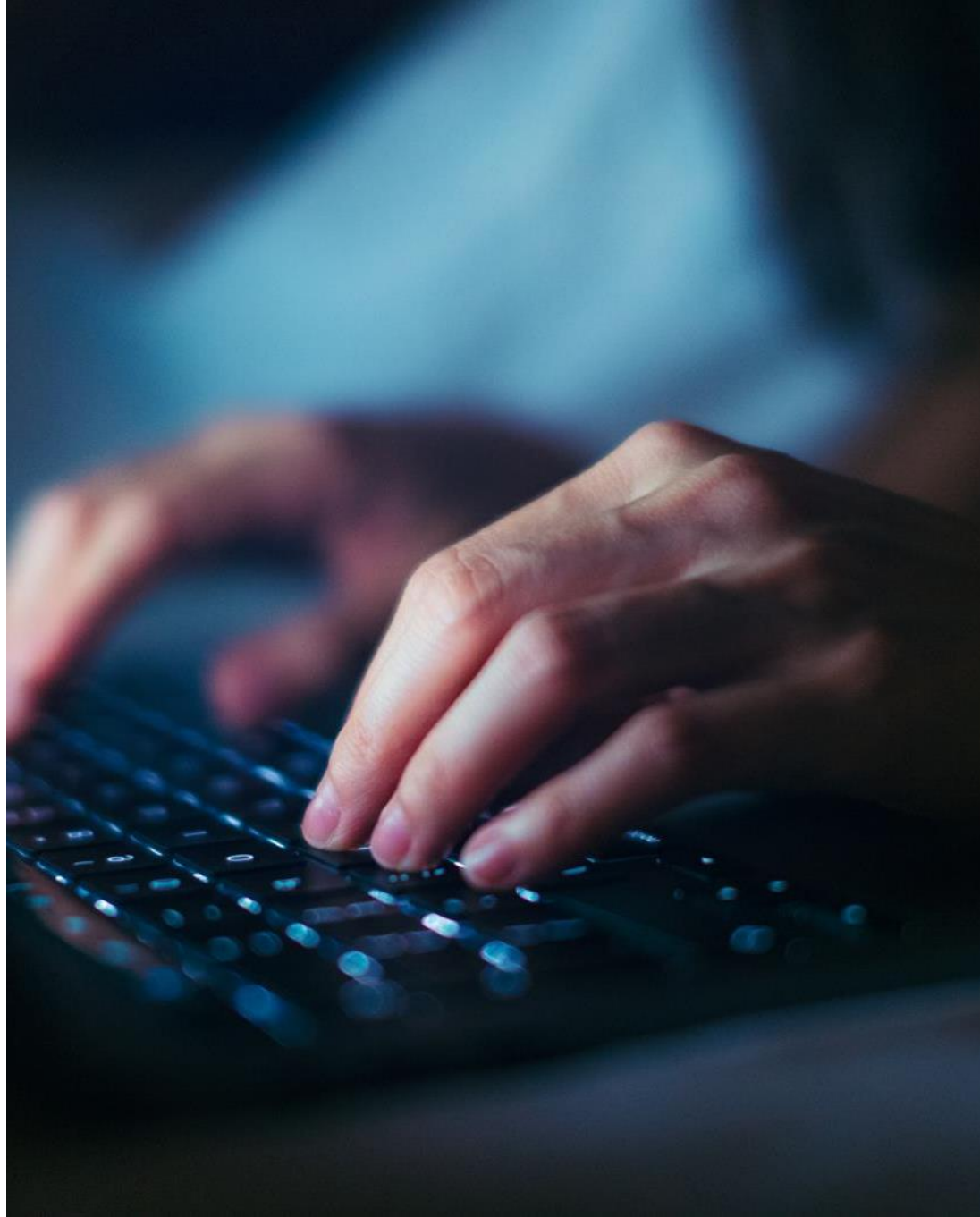
Definitionen

Besonders wichtige Einrichtungen (Auszug)

- **Bestimmte Einrichtungen** (Anlage 1) mit >=250 MA oder Umsatz >50 Mio. Euro und Jahresbilanz >43 Mio. Euro
- **Betreiber kritischer Anlagen**

Wichtige Einrichtungen (Auszug)

- **Bestimmte Einrichtungen** (Anlage 1 u. 2) mit >=50 MA oder Umsatz und Bilanz >10 Mio. Euro



NIS2UmsuCG

Eingriffsmöglichkeit (allgemein)

- BSI kann vom **Hersteller betroffener Systeme** die Mitwirkung verlangen
- BSI kann **Einrichtungen anweisen**, über **Sicherheitsvorfälle zu informieren** (auch die Öffentlichkeit)
- BSI kann **Nachweise** zur Erfüllung der gesetzlichen Anforderungen **und** die **Beseitigung von Mängeln verlangen**

NIS2UmsuCG

Eingriffsmöglichkeit

- BSI kann besonders wichtige Einrichtungen verpflichten, **Audits**, **Prüfungen** oder **Zertifizierungen** durchführen zu lassen
- BSI kann von besonders wichtigen Einrichtungen Nachweise und weitergehende Informationen bis zur **Mängelbeseitigung** dazu **verlangen**
- BSI kann **Einhaltung** des Gesetzes **selbst überprüfen** und dazu Unterstützung, **Zutritt** und **Auskunft** zu **verlangen**
- BSI kann für bestimmten Zeitraum Einrichtungen einen **Überwachungsbeauftragten** benennen
- BSI kann bei Unterlassung in Bezug Anordnungen die Aufsicht bitten **Betriebsgenehmigungen** auszusetzen und **Leitungsaufgaben** untersagen

NIS2UmsuCG
Anforderungen

- Verpflichtung eignete, verhältnismäßige u. wirksame **technische** u. **organisatorische Maßnahmen** um Störungen gering zu halten
- **Stand der Technik**
- Aufbau **Risikomanagement**
  - Mindestmaßnahmen + risikobasierte Maßnahmen
  - Incident Management, ITIL-Prozesse
  - Notfall- u. Krisenmanagement
  - Lieferkettensicherheit
  - Einkauf, Entwicklung u. Pflege; Schwachstellenmgmt.
  - Awareness u. Schulungen
  - Kryptografie, MFA, Zugriffskontrolle
  - Management von Anlagen

NIS2UmsuCG
Anforderungen

- Registrierungspflicht
- Pflicht zur Teilnahme am Informationsaustausch
- Unverzügliche Meldung von Vorfällen

BSI Information Sharing Portal

- Systeme zur Angriffserkennung
  (ist zudem Teil der ISO 27001:2022
  z. B. Annex 8.15, 8.16 und 8.21)

NIS2UmsuCG

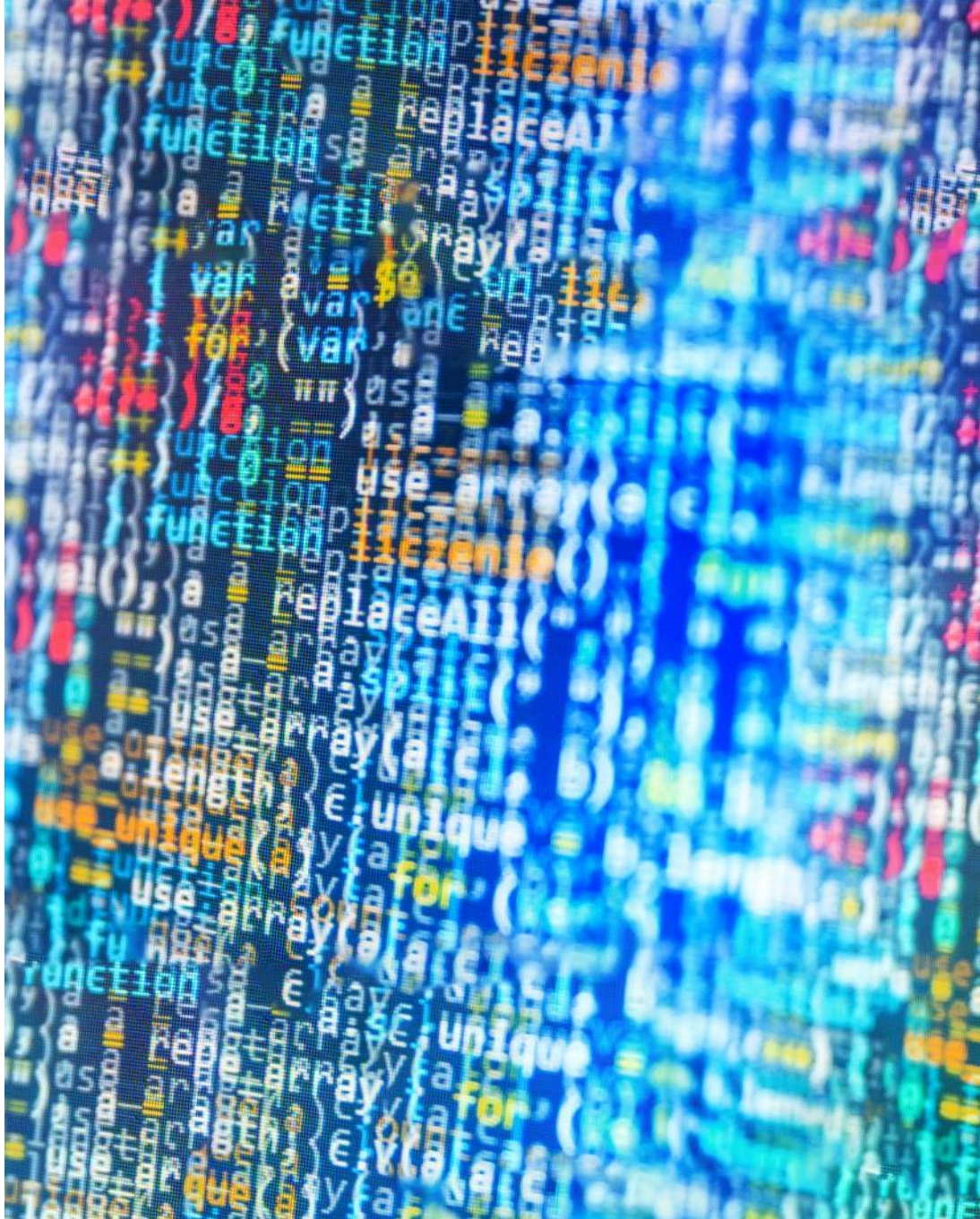
Sanktionen

Ordnungswidrigkeiten bei Verstoß gegen Pflichten (z. B. unterlassene Meldungen, Unvollständigkeit, Nichterreichbarkeit)

Geldbußen bis zu 2 Millionen Euro

Geldbußen bei wichtigen Einrichtungen bis zu 7 Millionen Euro oder 1,4% des weltweiten Umsatzes

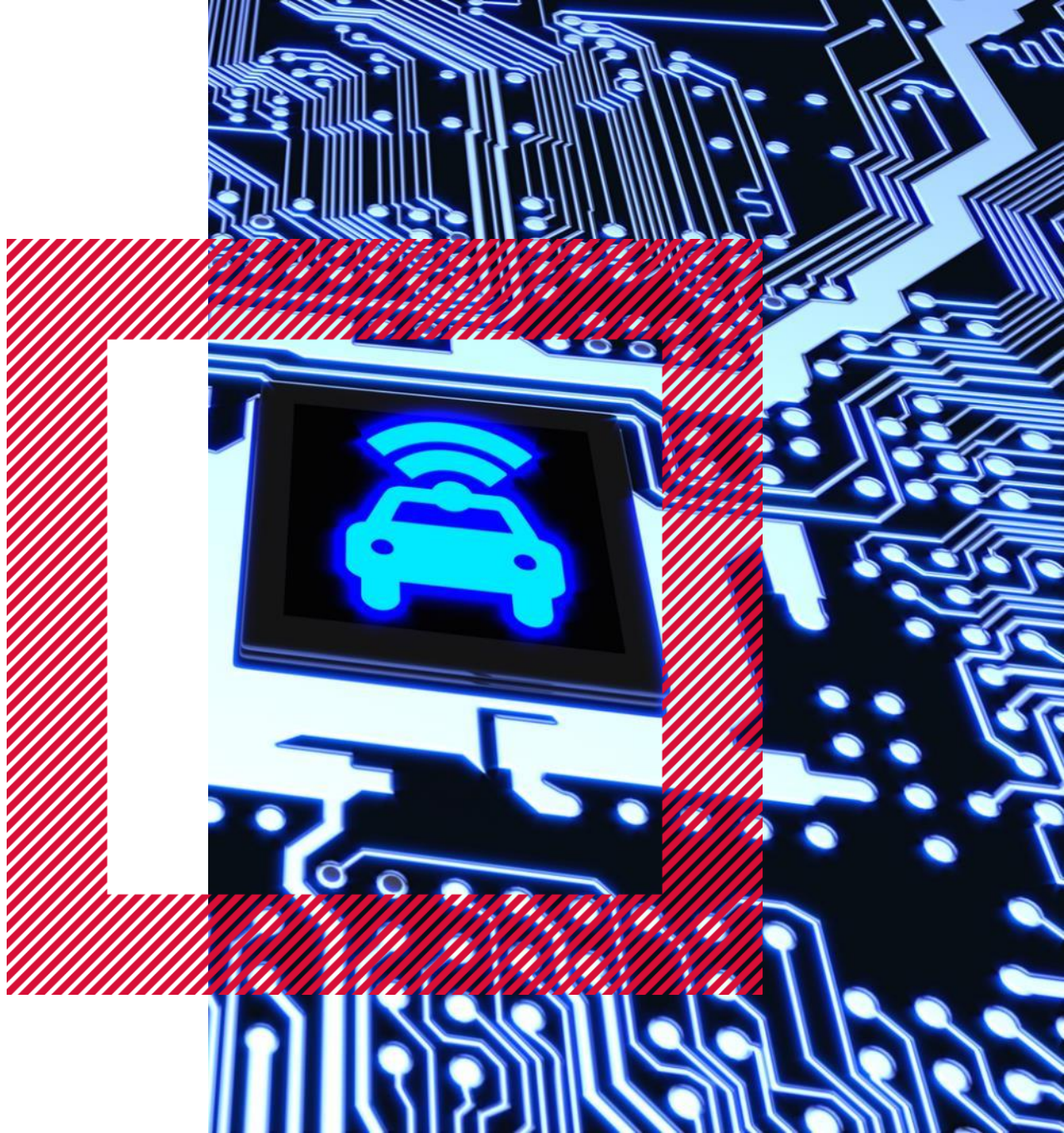
Geldbußen bei besonders wichtigen Einrichtungen bis zu 10 Millionen Euro oder 2% des weltweiten Umsatzes



03

Überblick EU CRA

EU Cyber Resilience Act



EU CRA
Überblick über das Gesetz

- EU **C**yber **R**esilience **A**ct (CRA)
- Status: Aktuell Gesetzesentwurf
- Soll Anfang 2024 in Kraft treten, wirksam ab 12 bis 24 Monate nach Inkrafttreten
- Vorbeugung von Cyberkriminalität durch Stärkung der Cybersicherheit für vernetzte Produkte über die Lieferkette bzw. im gesamten Lebenszyklus
- Ziel ist es, End-Verbraucher und Unternehmen vor Produkten mit unzureichenden IT-Sicherheitsfunktionen zu schützen
- „Secure by Design and Default“

EU CRA

Anwendungsbereich des Gesetzes

- Hersteller von **Hardware** und/oder **Software**
- Hersteller von Produkten, die solche Komponenten enthalten und **in** der **EU vertrieben** werden
- Differenziert in zwei Kategorien gemäß der möglichen Auswirkungen
  - Produkte, welche größere Wirtschaftsbereiche betreffen, sind strengere Vorschriften geplant (z. B. IoT oder Mobilfunk)
  - Liste noch nicht abschließend definiert bzw. bekannt

EU CRA

Anforderungen an Cybersicherheit (Annex I)

Sicherheitsanforderungen

- Risikobasiertes Niveau an Sicherheit (Entwurf, Entwicklung und Produktion)
- Produkte werden ohne bekannte ausnutzbare Schwachstellen ausgeliefert
- Basierend auf Risikobewertung und wo anwendbar:
  - **Sichere Standardkonfiguration**
  - Schutz vor unbefugtem Zugriff (z. B. Kontrolle und IAM)
  - **Verschlüsselung** und **Manipulationsschutz** (z.B. Daten und andere, in flight und at rest); Datenschutzkonformität
  - Verfügbarkeit gewährleisten (DOS)
  - Eigene negative Auswirkungen minimieren
  - **Angriffsoberfläche minimieren**
  - Exploitation mitigation mechanisms nutzen
  - Logdaten zu und **Monitoring** von eigenen Aktivitäten
  - Schwachstellenmanagement, ggf. automatische Updates

Umgang mit Schwachstellen

- Schwachstellen und **Komponenten identifizieren** und **dokumentieren** (Software-Stückliste und Abhängigkeiten)
- **Unverzügliche Behebung** von **Schwachstellen** (Bereitstellung von Patches)
- Tests und **Überprüfung** der **Produktsicherheit**
- **Veröffentlichung** von Schwachstellen (im Detail)
- Politik zur koordinierten Offenlegung von Sicherheitslücken
- Bereitstellung von Kontaktadressen zur Meldung von Schwachstellen und andere Maßnahmen zur Erleichterung der Weitergabe von Informationen
- Sichere **Verteilung** von **Softwarepatches**
- Unverzügliche und kostenfreie Bereitstellung von Softwarepatches und Informationen zu Handlungsweisen

EU CRA

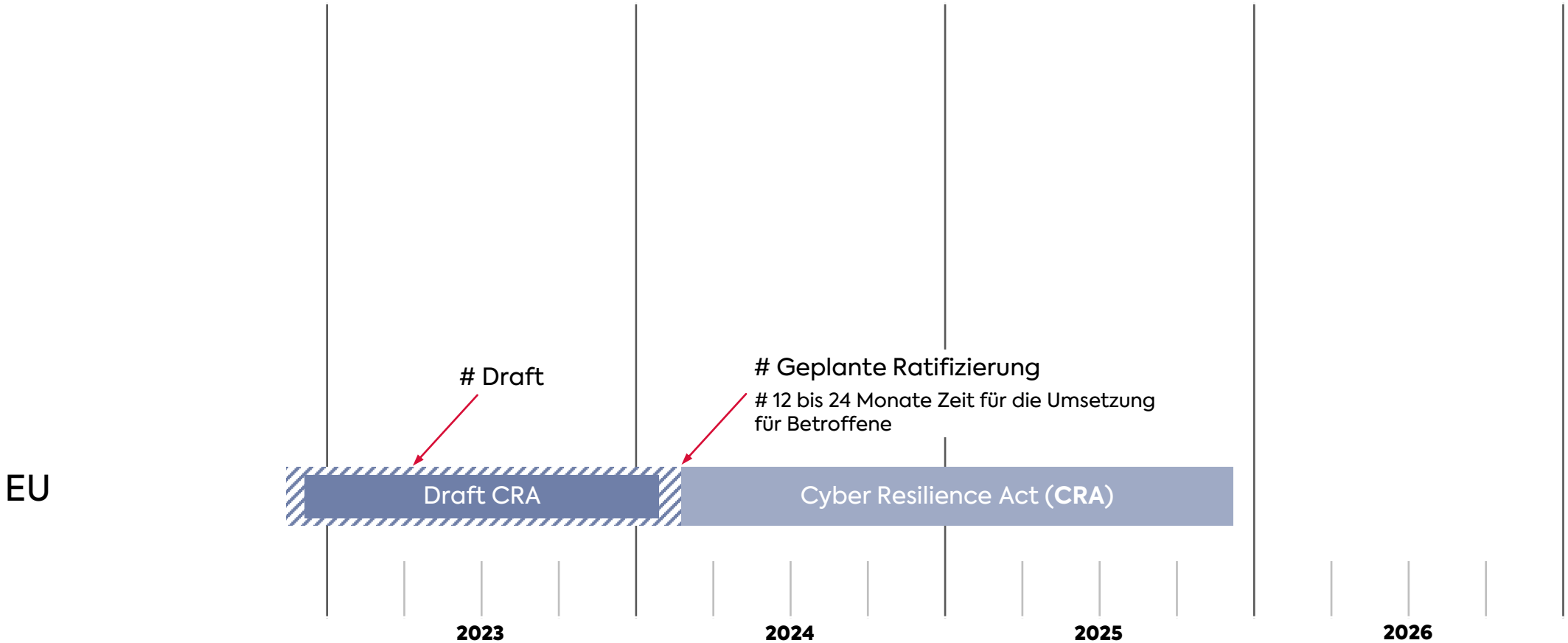
Klassifikation von kritischen Produkten (Annex III)

Class II

- Operating systems for servers, desktops, and mobile devices
- Hypervisors and container runtime systems that support virtualised execution of operating systems and similar environments
- Public key infrastructure and digital certificate issuers;
- Firewalls, intrusion detection and/or prevention systems intended for industrial use;
- General purpose microprocessors
- Microprocessors intended for integration in programmable logic controllers and secure elements
- Routers, modems intended for the connection to the internet, and switches, intended for industrial use
- Secure elements
- Hardware Security Modules (HSMs)
- Secure cryptoprocessors
- Smartcards, smartcard readers and tokens
- Industrial Automation & Control Systems (IACS) intended for the use by essential entities of the type referred to in [Annex I to the Directive XXX/XXXX (NIS2)], such as programmable logic controllers (PLC), distributed control systems (DCS), computerised numeric controllers for machine tools (CNC) and supervisory control and data acquisition systems (SCADA)
- Industrial Internet of Things devices intended for the use by essential entities of the type referred to in [Annex I to the Directive XXX/XXXX (NIS2)]
- Robot sensing and actuator components and robot controllers
- Smart meters

EU CRA

Zeitlicher Ablauf und Fristen



EU CRA

Wesentliche Inhalte (Überblick)

- Anforderungen werden nach Kriterien hinsichtlich der Relevanz der Auswirkungen unterschieden
- Für Produkte, die größere wirtschaftliche Bereiche betreffen werden strengere Vorschriften erwartet
- Solche Produkte sollen die Cybersicherheit bereits im Produktionsprozess bzw. bei der Konfiguration berücksichtigen
- Hersteller werden verpflichtet, ausführliche Dokumentation zu führen
- Folgen für Unternehmen sind weitreichend, und betreffen gesamten Produktlebenszyklus
- Bereitstellen von Softwarepatches und aktive Kommunikation zu Sicherheitslücken und deren Fehlerbehebung ist wesentlicher Baustein der Regulierung
- Zu betroffenen Produkten müssen klare und verständliche Bedienungs- bzw. Betriebsanleitungen zur Verfügung gestellt werden
- Bußgelder: 15 Millionen Euro bzw. 2,5% Jahresumsatz weltweit

04

Überblick EU RCE

EU Directive on the Resilience of Critical Entities

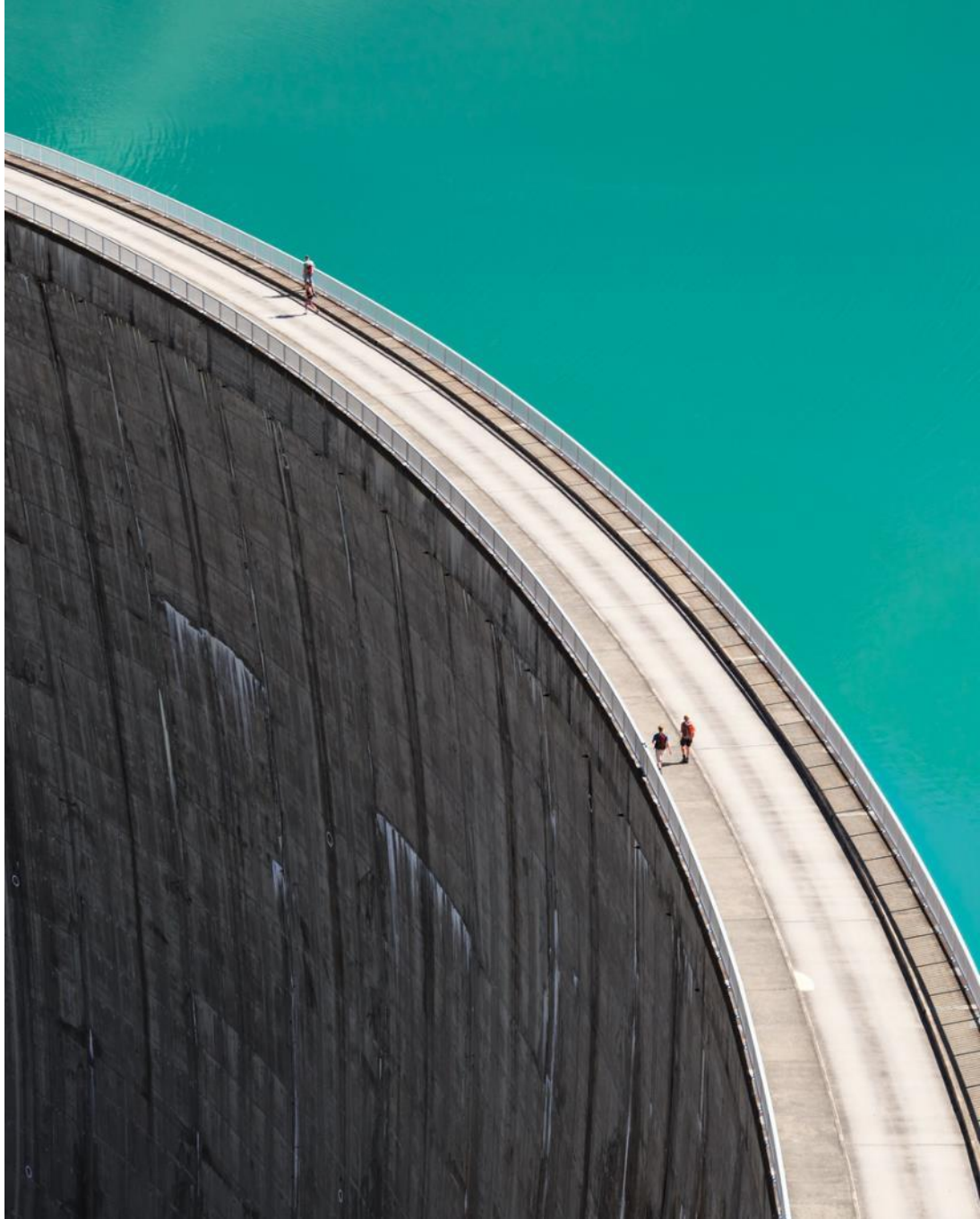
EU RCE
Überblick über das Gesetz

- **Directive** on the **R**esilience of **C**ritical **E**ntities (Directive (EU) 2022/2557)
- Am 16.01.2023 in Kraft getreten, Umsetzung in nationales Recht bis 17.10.2024 („KRITIS-Dachgesetz“)
- Richtlinie über die Resilienz kritischer Einrichtungen
- Ziel: **physische Widerstandsfähigkeit** kritischer Einrichtungen stärken; **hybriden Bedrohungen** / Lagen begegnen
- Betroffene Wirtschaftszweige in Kategorien wesentlich und wichtig unterteilt (große thematische Überschneidung mit EU NIS-2)
- Aber: starker Fokus auf materiellen/physischen Schutz

EU RCE

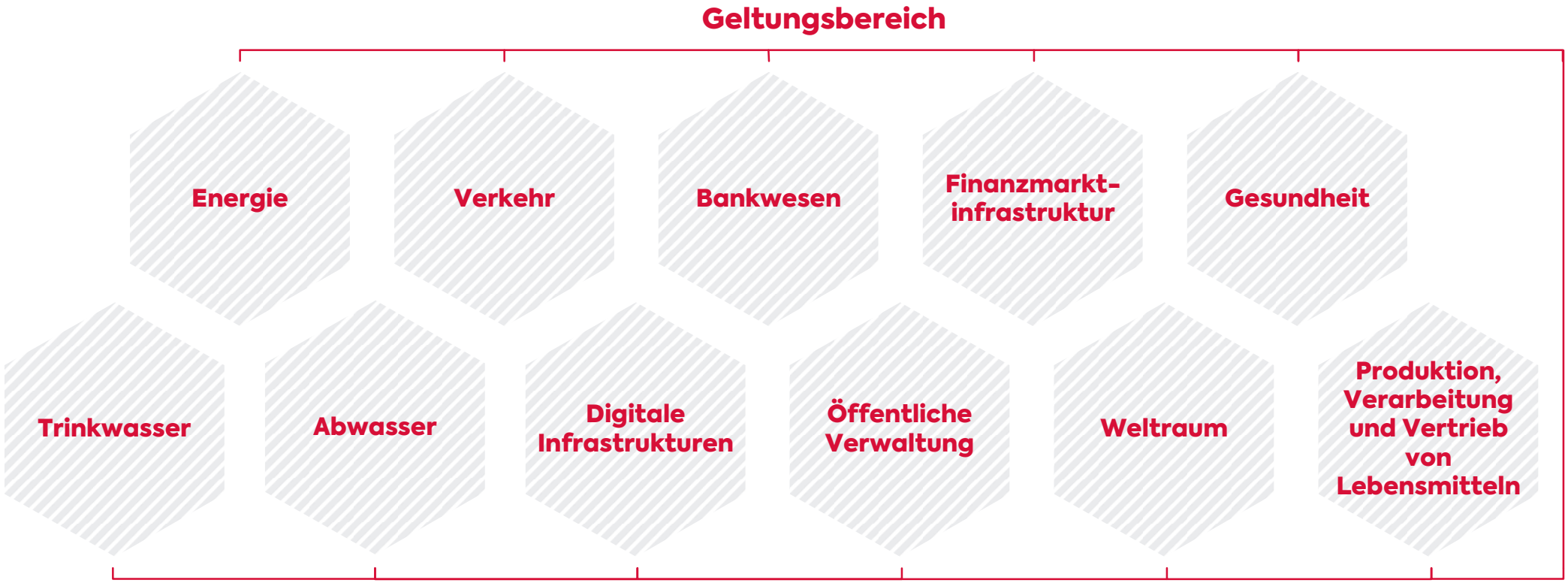
Ziele des Gesetzes

- Integration des Blickwinkels „physischer Schutz“ in die Betrachtung von Sicherheit
- Verpflichtung zur Erstellung nationaler Strategien
- Verpflichtung der Mitgliedstaaten zur Identifikation von kritischen Einrichtungen
- Verpflichtung kritischer Einrichtungen diese angemessen und wirksam zu schützen
- Vorbereitung auf den Krisenfall (BCM)
- Regelung von Verantwortlichkeiten („wer ist zuständig?“ Landespolizei, Bundespolizei, Bundeswehr, Betreiber usw.)



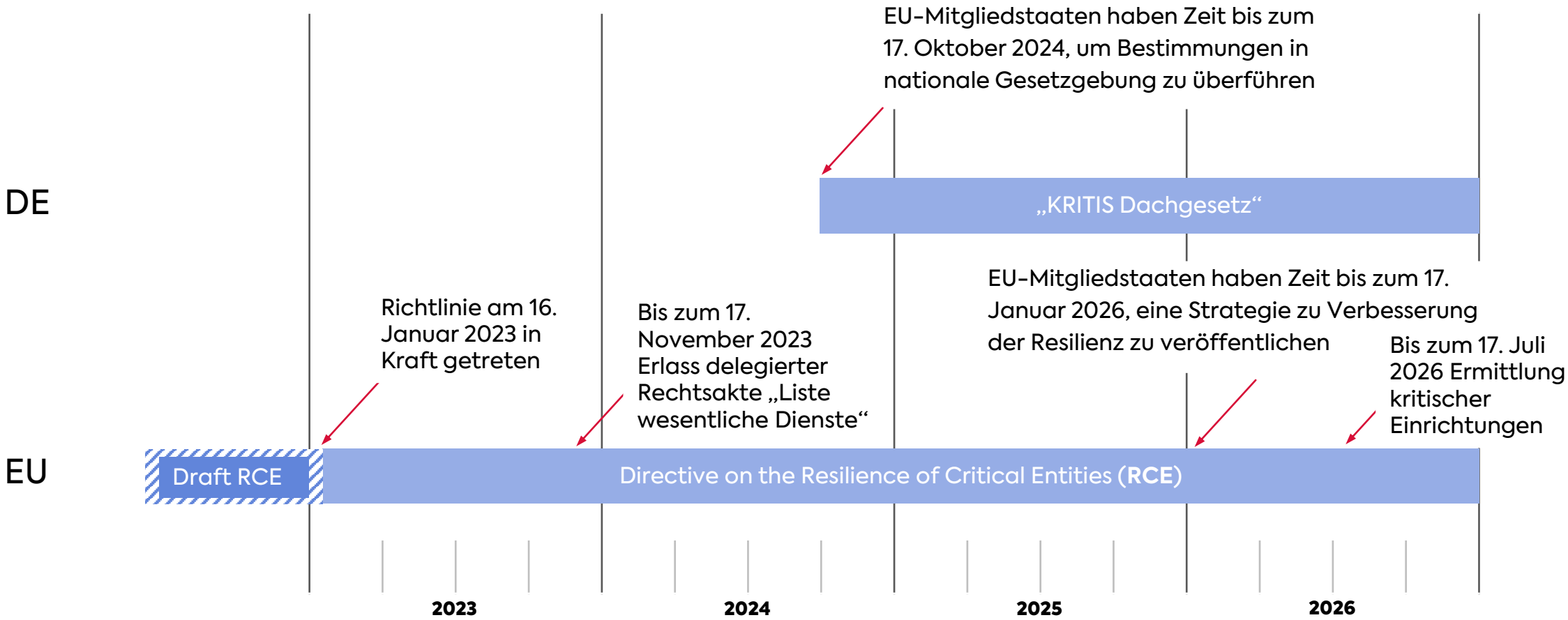
EU RCE

Zielgruppen des Gesetzes



EU RCE

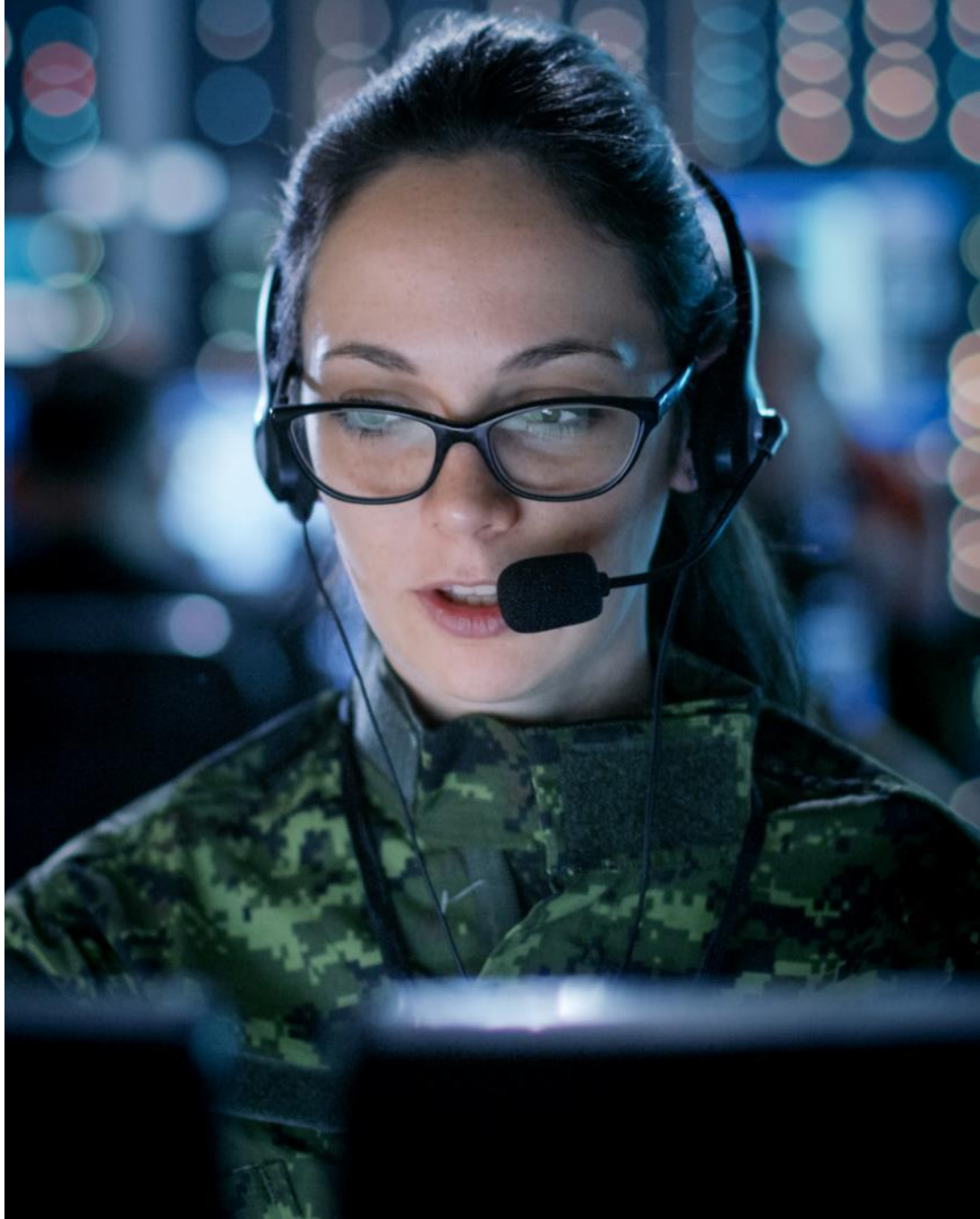
Zeitlicher Ablauf und Fristen



EU RCE

Wesentliche Inhalte

- Funktionsfähiges **Risikomanagement** muss aufgebaut werden
- **Technische**, **sicherheitsbezogene** und **organisatorische Maßnahmen** zur Resilienz
  - Katastrophenvorsorge, Physischer Schutz von Einrichtungen
  - Risiko- und Krisenmanagementverfahren, Wiederherstellung u. alternative Lieferketten
  - Sicherheitsmanagement, Zuverlässigkeitsprüfungen, Schulungen
  - Resilienzpläne, Ansprechpartner für Behörden
- Sicherheitsvorfälle behandeln, **Vorfallbehandlung** planen
- Sicherheitsvorfälle sollen gemeldet werden (**Meldewesen**)
- Aufsichtsbehörden können eigene Inspektionen und Audits durchführen und die Implementierung von angemessenen Maßnahmen durchsetzen
- Bußgelder sollen wirksam und abschreckend sein



Was sollten Betroffene jetzt tun?

- **Prüfung** der **Betroffenheit**
- **Prüfung** der neuen **Anforderungen**, die umzusetzen sind; Lieferketten, kritische Komponenten, Dienstleister, Unternehmenszuordnung und Mindestanforderungen beachten
- **Meldeprozesse vorbereiten** bzw. vorhandene anpassen (für relevante Incidents, also Vorfälle / Bedrohungen / Risiken); neues Melderegime
- **Risikomanagement aufsetzen**

Wie kann secunet helfen?

- Workshop „Betroffenheitsprüfung“
- Workshop „Scoping“ – Identifikation der betroffenen Prozesse und Produkte
- Reifegradanalysen und Vor-Audits
- Konzeption zur Umsetzung der gesetzlichen Anforderungen
- Beratung und Implementierung zu Managementsystemen, Risikomanagementsystemen, Mindestsicherheitsmaßnahmen u. w.
- Aufbau von Meldestrukturen
- Vorbereitung zur Nachweiserbringung
- Begleitende Penetrationstests u. Beratung
- Produkte im Rahmen der Erfüllung von Anforderungen (z. B. secunet edge und secunet monitor KRITIS)


secunet