FRAUSCHER CONSULTING

Reliable and Energy Efficient Data Center Design & Services

ASSA ABLOY
Opening Solutions

Opening Solutions Day

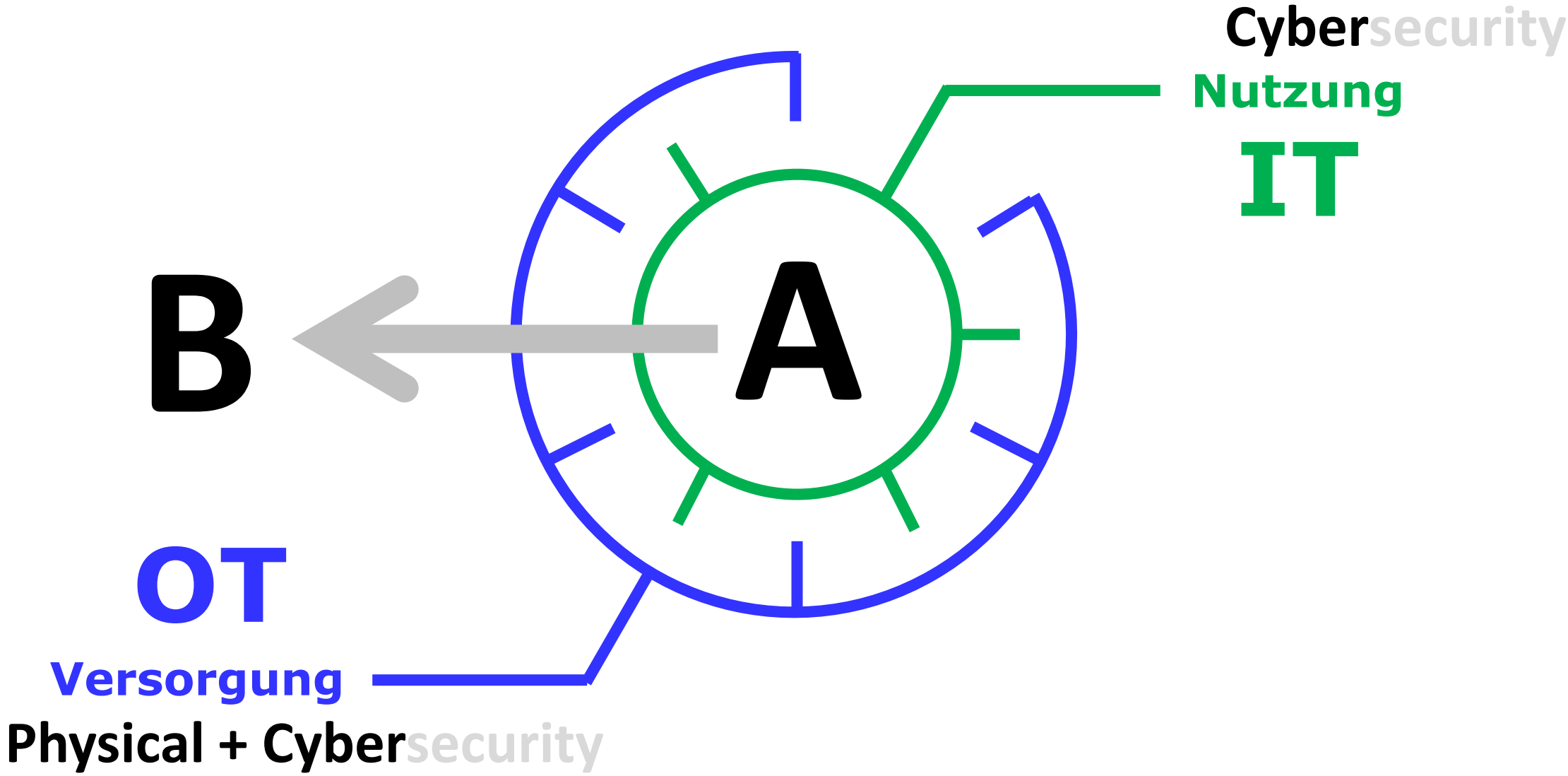
Experience a safer
and more open world

NIS, RKE, CRA, IOT – Cybersicherheit am Weg von A nach B

Dipl.-Ing. Georg Meixner, MBA

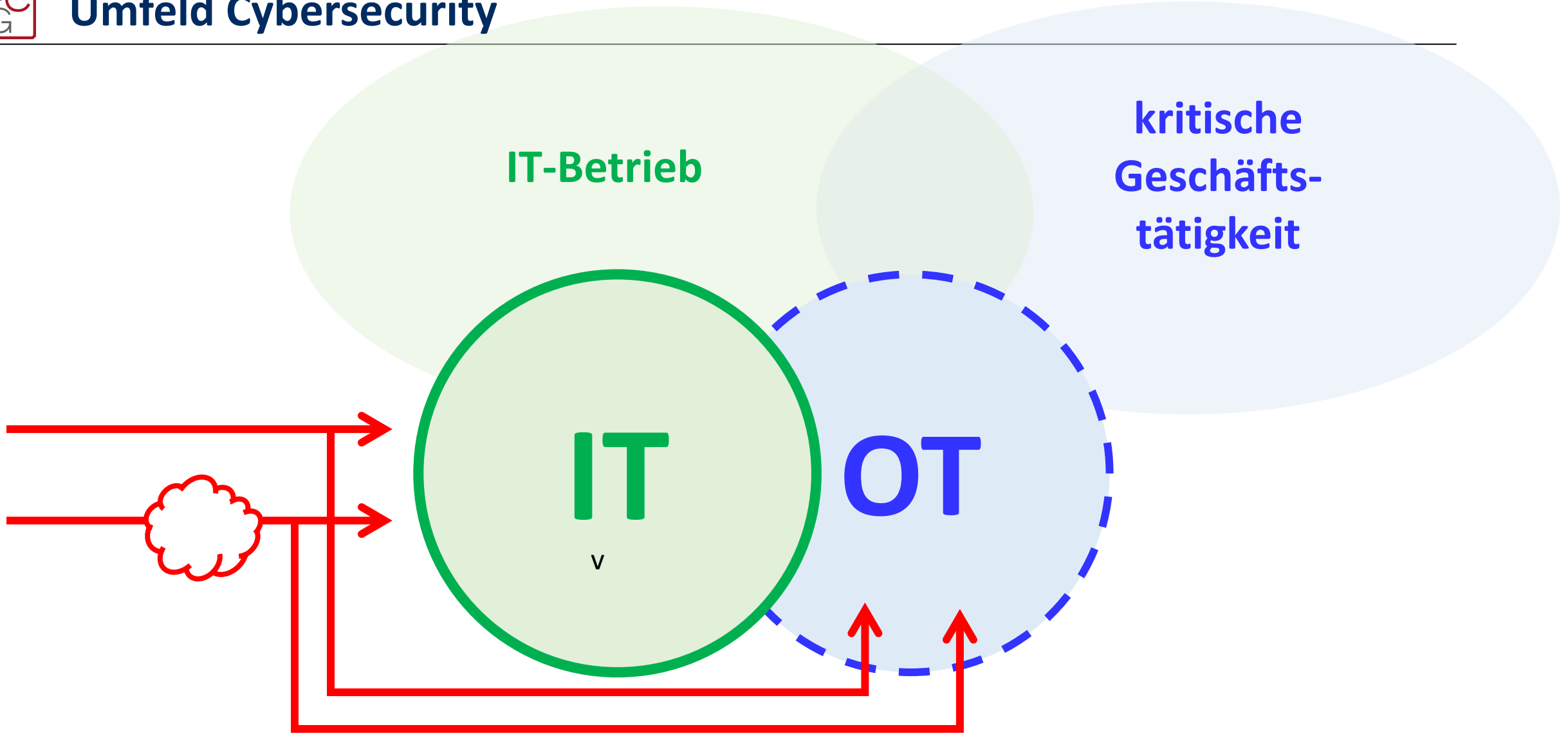
15.05.2024

© 2024 FRAUSCHER CONSULTING GmbH



© 2024 FRAUSCHER CONSULTING GmbH

Umfeld Cybersecurity



„IT-OT-Konvergenz“

© 2024 FRAUSCHER CONSULTING GmbH

Definition kritische Infrastruktur

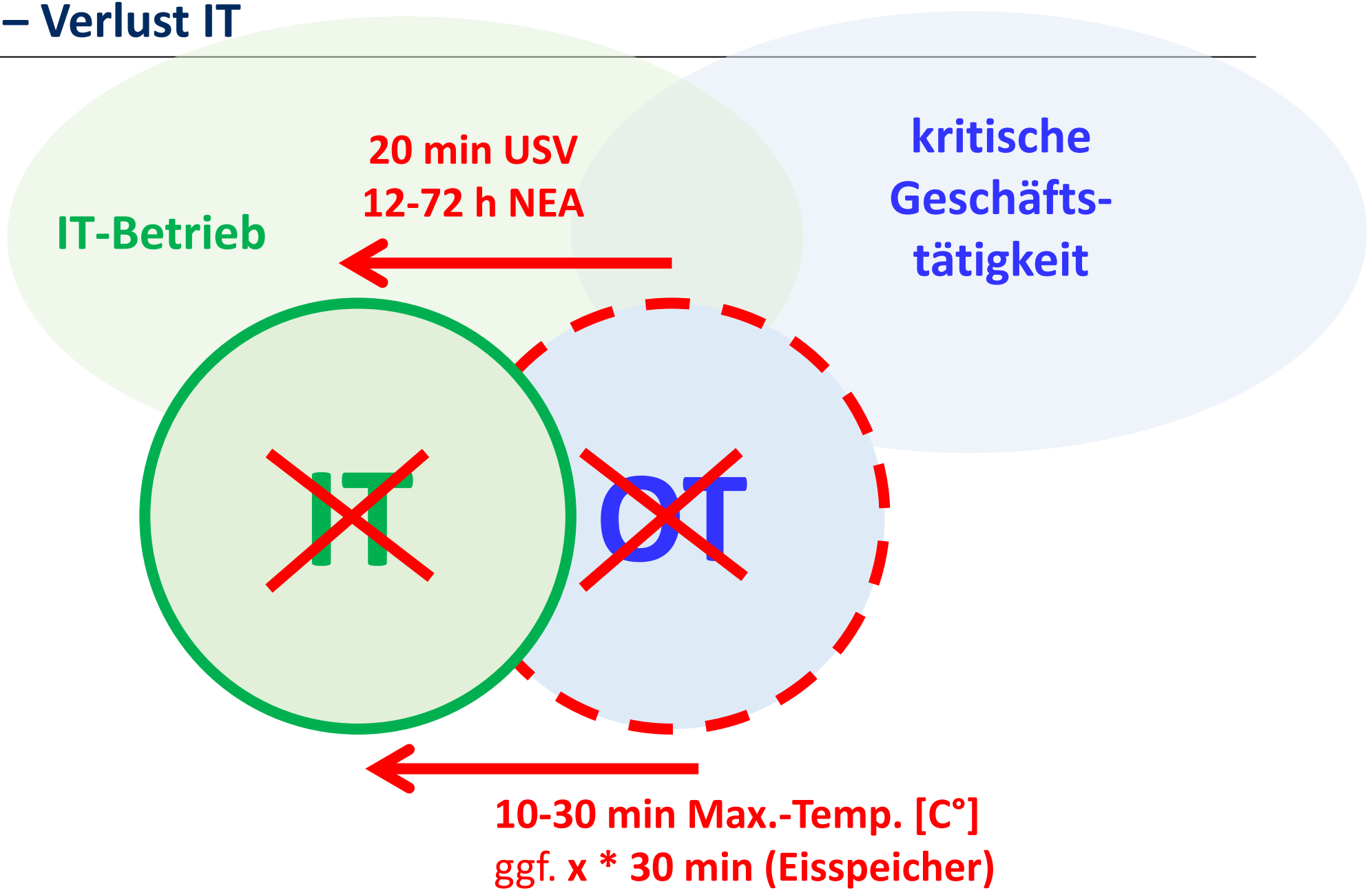
Kritische Infrastrukturen sind von hoher Bedeutung für das Funktionieren des Gemeinwesens.

Durch ihren Ausfall oder ihre Beeinträchtigung würden erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten

(BSI-Gesetz, 2021, §2, Abs.10)

© 2024 FRAUSCHER CONSULTING GmbH

Verlust OT – Verlust IT



© 2024 FRAUSCHER CONSULTING GmbH

Europäischer Cybersecurity Act *)

4 Richtlinien & Verordnungen:

Fokus: Europäische Cybersicherheits-Strategie

DSGVO

NIS2
Network & Information Security

Fokus: spezifische Verordnung für Finanzsektor

DORA
Digital Operational Resiliency Act

RKE/RCE
EU 2022/2557

Fokus: Resilienz von Betreibern kritischer Infrastrukturen

CRA
Cyber Resiliency Act
(noch Entwurf)

Fokus: Sicherheit von Produkten mit digitalen Elementen

IT-SiG
(seit 2015; V3.0)

IOT

KRITIS
Entsorgung

*) Act/Verordnung: verbindlicher Rechtsakt, von allen EU-Mitgliedsstaaten vollumfänglich umzusetzen in nationales Recht

**) Richtlinie: Rechtsakt mit einem zu erreichenden Ziel, zu deren Verwirklichung die EU-Mitgliedsstaaten eigene Rechtsvorschriften erlassen.

© 2024 FRAUSCHER CONSULTING GmbH

NIS2 vs. RKE

NIS2		RKE
Mindestniveau für Cyber Security & Risikomanagement bei Betreibern	**Baseline**	Resilienz & Physische Sicherheit, Risiko
▪ 10 wesentliche + 6 wichtige Sektoren ▪ mittel-groß (NIS2 size-cap)	Unternehmen die kritische Dienste & Infrastrukturen in der EU betreiben	▪ 10 wesentliche Sektoren (equivalent zu NIS2; Ausnahmen: IT, Finanzwesen) ▪ national-spezifisch: Festlegung nat. Behörden
Regulierung & Governance durch Mitgliedstaaten / Risiko & Umsetzung unter EU-Aufsicht		

▪ Umsetzung ersetzt NIS1	vorgestellt 12/2020, in Kraft seit 01/2023
	Umsetzung in nationales Recht bis 10/2024
		▪ Umsetzung ersetzt
		  ▪ EPCIP / (EU) RL 2008/114
		  ▪ Komplementiert APCIP

▪ Nationale Cyber Security Strategie ▪ Betreiber identifiziert sich selbst	**nationale Governance**	▪ Nationale Resilienz Strategie ▪ Staat identifiziert krit. Einrichtungen

© 2024 FRAUSCHER CONSULTING GmbH

NIS-G 2024

Netz- und
Informationssystem-
Sicherheits-
Gesetz

© 2024 FRAUSCHER CONSULTING GmbH

Netz- & Informationssystem Sicherheitsgesetz

NISG

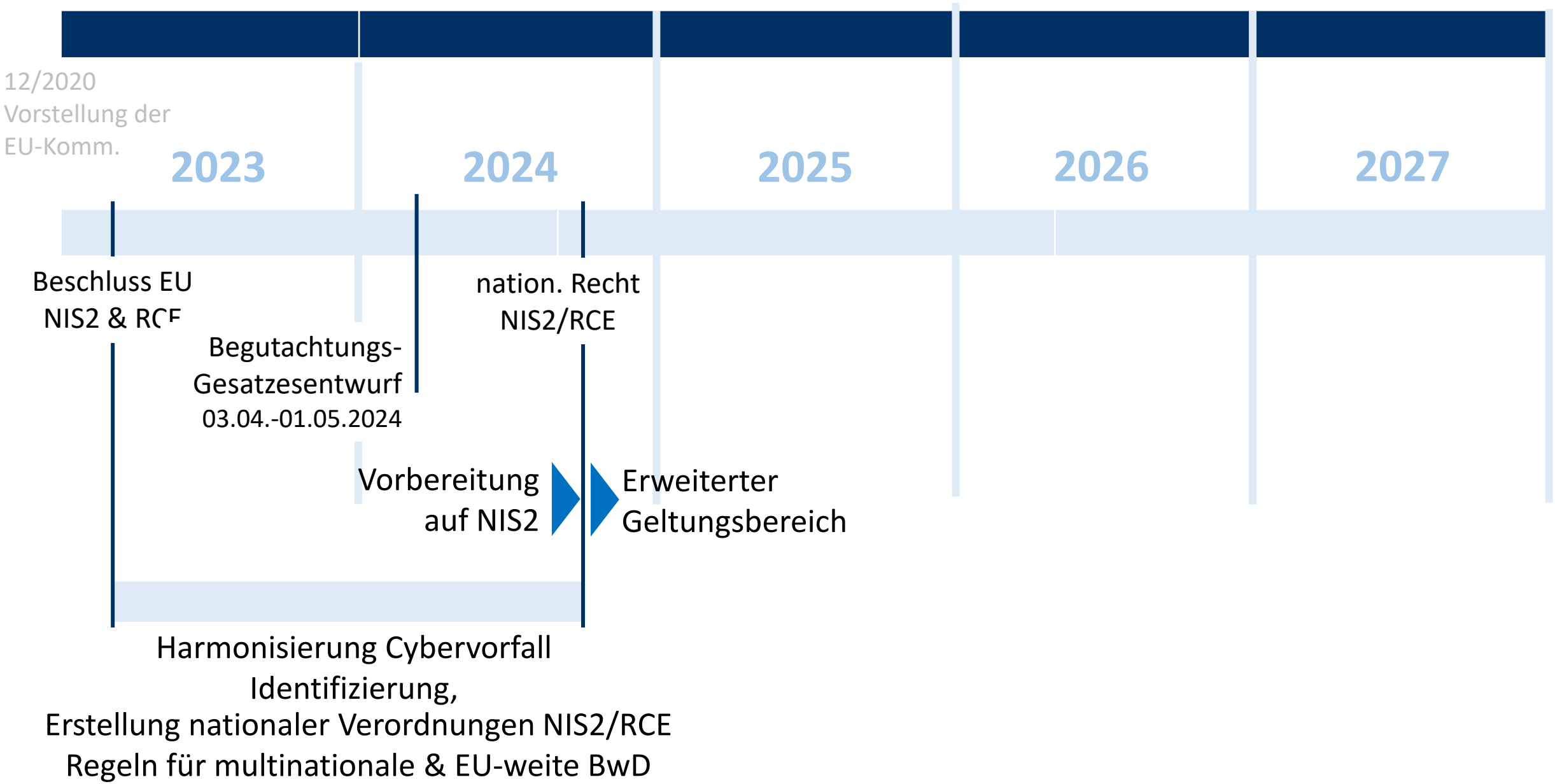
- **IT-Systeme haben zentrale Rolle in Gesellschaft**
  - IT / OT, Betrieb & Dienste
- **Verlässlichkeit & Sicherheit entscheidend**
  - Wirtschaft
    - Funktionieren des Binnenmarktes
  - Gesellschaft
- **EU-Rechtsakt über Cybersicherheit**
  - gemeinsames Sicherheitsniveau von NIS
  - Maßnahmen dorthin

- Zusammenarbeit - nicht versperren davor
- Eigenverantwortung - nicht darauf setzen, dass jemand ein Problem für uns löst

- **Wo IT eingesetzt wird – muss IT-Sicherheit mitgedacht & mitgelebt werden**

© 2024 FRAUSCHER CONSULTING GmbH

Chronologie NIS2



© 2024 FRAUSCHER CONSULTING GmbH

Ziele seitens des Gesetzgebers & Wie sieht Erfolg aus?

- **Ziel 1:** optimale Rahmenbedingungen für ein hohes Cybersicherheitsniveau in AT
  - Erfolg: Ausweitung von **7 auf 18 Sektoren**

Umsetzung durch:
Maßnahme 1: Errichtung eines nationalen Cybersicherheitszentrums (NCSZ) zur Bündelung der Kompetenzen
Maßnahme 2: Umsetzung und Durchführung von Unionsrechtsakten im Bereich der Cybersicherheit
Maßnahme 3: Weiterentwicklung und Koordination einer neuen nationalen Cybersicherheitsstrategie
Maßnahme 4: Benennung einer zentralen Anlaufstelle für Cybersicherheit (SPOC)
Maßnahme 5: Benennung einer nationalen Behörde für das Management von Cybersicherheitsvorfällen großen Ausmaßes
Maßnahme 6: Benennung von Computer-Notfallteams (CSIRTs) zur Unterstützung der wesentlichen und wichtigen Einrichtungen
Maßnahme 7: Vorschriften zum Austausch von Cybersicherheitsinformationen
Maßnahme 8: Pflicht zur Setzung geeigneter Aufsichts- und Durchsetzungsmaßnahmen
Maßnahme 9: Pflicht zur Setzung geeigneter Risikomanagementmaßnahmen und Berichtspflichten
Maßnahme 10: Pflicht zur Führung eines Registers der wesentlichen und wichtigen Einrichtungen

© 2024 FRAUSCHER CONSULTING GmbH

Ziele seitens des Gesetzgebers & Wie sieht Erfolg aus?

- Ziel 2: Synergieeffekte innerhalb der zivilen staatlichen Cybersicherheits-Strukturen in AT
  - Erfolg: **Cybersicherheitsbehörde im BMI** als einheitlicher Ansprechpartner

Umsetzung durch:
Maßnahme 1: Errichtung eines nationalen Cybersicherheitszentrums (NCSZ) zur Bündelung der Kompetenzen
Maßnahme 2: Umsetzung und Durchführung von Unionsrechtsakten im Bereich der Cybersicherheit

- Ziel 3: Schutz & Prävention gegenüber Netz- & Informationssysteme in AT
  - Erfolg: Pool an geeigneten **Fachkräften: von 12 auf 63**

© 2024 FRAUSCHER CONSULTING GmbH

Ziele seitens des Gesetzgebers & Wie sieht Erfolg aus?

Maßnahme 5: Benennung einer nationalen Behörde für das Management von Cybersicherheitsvorfällen großen Ausmaßes

Verschiedene präventive Maßnahmen:

- Ermitteln von Kapazitäten, Mittel und Verfahren zur Abwehr

- Verabschiedung eines **nationalen Planes für die Reaktion:**
  - Ziele der nationalen Vorsorgemaßnahmen und –tätigkeiten
  - Aufgaben und Zuständigkeiten der Behörden für das Management von Cybersich.vorfällen großen Ausmaßes
  - Die Verfahren für das Management von C.s.Vorfällen gr. A., einschließlich deren Integration
    - In den nationalen Rahmen für das allgemeine Krisenmanagement
    - Die Kanäle für den Informationsaustausch
  - Nationale Vorsorgemaßnahmen, einschließlich Übungen und Ausbildungsmaßnahmen
  - Die einschlägigen öffentlichen & privaten Interessensträger und die betroffene Infrastruktur
  - Die zwischen den einschlägigen nationalen Behörden und Stellen vereinbarten nationalen Verfahren und Regelungen die gewährleisten sollen, dass sich
    - Die Republik Österreich wirksam am koord. Management von C.s.vorfällen gr. A. auf Unionsebene beteiligen und dieses unterstützen kann

© 2024 FRAUSCHER CONSULTING GmbH

NIS2 – Unterstützungsmaßnahmen / Prävention

Selbstverpflichtung des BMI:

- Vermittlung von Vorsichtsmaßnahmen und konkreten Handlungsempfehlungen
- Schulungskonzepte und Vorträge
- Workshops für MitarbeiterInnen von Einrichtungen
- Abstimmung mit Sicherheitsverantwortlichen im Rahmen von Vorträgen
- Publikationen, Schriftenreihen, Broschüren zu Cybersicherheit
- etc.

© 2024 FRAUSCHER CONSULTING GmbH

Nachweis der Cybersecurity-Maßnahmen

- Quasten (qualifizierte Stellen) im wesentlichen dieselben wie bei NIS1:
  unabhängige Stellen:
  - Aufgaben & Befugnisse an Anforderungen der NIS2-RL angepaßt
  - Jurist. Personen & eingetrag. Personengesellschaften
  - Zugelassen zur Prüfung der Risikomanagement-Maßnahmen wesentlicher & wichtiger Einrichtungen durch Cybersicherheitsbehörde
  - min. ein „befähigter sicherheitsüberprüfter Prüfer“ als natürliche Person
  - Prüfung der Nachweise einer wes./wich. Einrichtung

- **Unabhängige Prüfer:**
  - positive Sicherheitsüberprüfung (durch unabh. Stelle oder nach SPG)
  - Eignung zur Beurteilung durch Absolvierung einer Fachprüfung
  - Ausreichend theoretische Fachkenntnisse über Risikomanagement-Maßnahmen
  - Ausreichend praktische Fähigkeiten zur Beurteilung deren pflichtgem. organis. od. technischen Umsetzung

© 2024 FRAUSCHER CONSULTING GmbH

Risikomanagementmaßnahmen

© 2024 FRAUSCHER CONSULTING GmbH

Anwendung / Sektoren

Anhang I (= Sektoren mit hoher Kritikalität)	Anhang II (= sonstige kritische Sektoren)
Energie (Elektrizität, Fernwärme/Kälte, Öl, Gas und Wasserstoff)	Post- und Kurierdienste
Verkehr (Luft, Schiene, Schifffahrt, Straße)	Abfallbewirtschaftung
Bankwesen	Chemie (Herstellung und Handel)
Finanzmarktinfrastrukturen	Lebensmittel (Produktion, Verarbeitung, Vertrieb)
Gesundheitswesen (Gesundheitsdienstleister, EU-Referenzlaboratorien, Forschung und Herstellung von pharmazeutischen und medizinischen Produken und Geräte)	Verarbeitendes / Herstellendes Gewerbe (Medizinprodukten; Datenverarbeitungs-, elektronische und optische Geräte und elektronische Ausrüstungen; Maschinenbau; Kraftwagen und Kraftwagenteile und sonstiger Fahrzeugbau)
Trinkwasser	Anbieter digitaler Dienste (Suchmaschinen, Online-Marktplätze und soziale Netzwerke)
Abwasser	Forschung
Digitale Infrastruktur (IXP, DNS, TLD, Cloud-Computing, Rechenzentren, CDN, TSP und Anbieter öffentlicher elektronischer Kommunikationsnetze- und dienste)	
Verwaltung von IKT-Diensten (B2B) Managed Svs Prov,/ Managed Security Svs Prov.	
Öffentliche Verwaltung	
Weltraum	Rot = Neuerungen gegenüber NIS1

16

Quelle:
NIS2 Die neue Cybersicherheits-Richtlinie WKÖ Live-Webinar Mag. Vinzenz Heußler, LL.M. Bundeskanzleramt, Abteilung I/8 (Cyber Security, GovCERT, NIS-Büro und ZAS) Leiter NIS-Büro Wien, 21. Februar 2023

© 2024 FRAUSCHER CONSULTING GmbH

Ausnahmen zur Anwendung

Ausnahmen durch Sektor (unabh. Größe):

- KU-Ausnahme: insbes.
  - im Sektor digitale Infrastruktur
  - + mit hoher Kritikalität
  - von Lieferkette betroffen

- Digitale Dienste:
  - Qualifizierter Vertrauensdienstanbieter
  - öffentl. elektronische Kommunikationsnetze oder –dienste
  - TLD-Namensregister, DNS-Diensteanbieter

- nationale Monopole, essenziell für Aufrechterhaltung kritischer gesellschaftlicher oder wirtschaftlicher Aktivitäten, grenzüberschreitend, systemisches Risiko

- Ausgenommen: gew. öffentliche Verwaltungen (Parlament, LV, Bildungssektor, …)

Ausnahmen durch Lieferkette:

- Dienstleister und Lieferanten von betroffenen Unternehmen

© 2024 FRAUSCHER CONSULTING GmbH

All-Gefahren-Ansatz / risikobasierter Ansatz

Angemessene & verhältnismäßige Maßnahmen:

- technisch
- operativ
- Organisatorisch

Berücksichtigung:

- Stand der Technik
- Kosten der Umsetzung

- Ausmaß der Risikoexposition
- Größe des Unternehmens

- Wahrscheinlichkeit des Eintretens von Sicherheitsvorfällen &
- deren Schwere, inkl. gesellschaftlichen & wirtschaftlichen Auswirkungen

© 2024 FRAUSCHER CONSULTING GmbH

Meldepflicht eines erheblichen Sicherheitsvorfalles

erheblicher Sicherheitsvorfalles:

Hat verursacht / kann verursachen:

- schwerwiegende Betriebsstörungen der Dienste
- Finanzielle Verluste für die Einrichtung

Hat beeinträchtigt / kann beeinträchtigen:

- andere natürliche / juristische Personen durch
- Erhebliche materielle / immaterielle Schäden

	Wesentliche Einrichtungen	Wichtige Einrichtungen	Einrichtungen außerhalb des AWB
Erheblicher Sicherheitsvorfall § 35 NISG 2024	Pflichtmeldung		
(Near Miss) Beinahe-Cybersicherheitsvorfall § 3 Z 29 NISG 2024	Freiwillige Meldung		
Cyberbedrohung § 3 Z 27 NISG 2024			
Cybersicherheitsvorfall § 3 Z 30 NISG 2024			

Quelle: bmi.gv.at, KSÖ-Rechts- & Technologiedialog, April 2024

© 2024 FRAUSCHER CONSULTING GmbH

Meldepflicht eines erheblichen Sicherheitsvorfalles

Erstmeldung / Frühwarnung

unverzüglich bis max.

24h nach Kenntnis

Verdacht, ob

- rechtswidrig, od.
- Grenzüberschreitend
- Betroffene Nutzer
- Dauer (bisher, vorauss.)
- Geograf. Gebiet
- Art, Ursache, Folgen

Meldung

unverzüglich bis max.

72h nach Kenntnis

erste Bewertung

- Bestätigung / Aktualisierung / Negierung
- Schweregrad
- Auswirkungen, ggf.
- Komprom.indikatoren

Zwischen-Meld./Ber.

- Auf Ersuchen
- Relevante Aktualisierungen

Folgemeldung

1 Mo nach Kenntnis

ausführl. Beschreib.

- Art der Bedrohung
- Ursachen; vermutet & tatsächlich
- Folgen
- Ergriffene Maßnahmen
- Betroffene kritische Infrastruktur

Nach-Meldung

- Später bekannt gewordene Umstände
- Beendigung (unverzüglich)

Unverzüglich:

→ **Dienstempfänger:** über erheblichen Sicherheitsvorfall

erhebliche Cyberbedrohung:

→ **pot. betroffene Dienstempfänger:** über

- Abhilfemaßnahmen ihrerseits
- erhebliche Cyberbedrohung

andauernder Vorfall

- Fortschrittsbericht

Abschluss-bericht

- grundsätzlich unverzüglich
- längstens **2 Mo** nach Beendigung

© 2024 FRAUSCHER CONSULTING GmbH

Meldepflicht eines erheblichen Sicherheitsvorfalles:

Meldepflichtigkeit

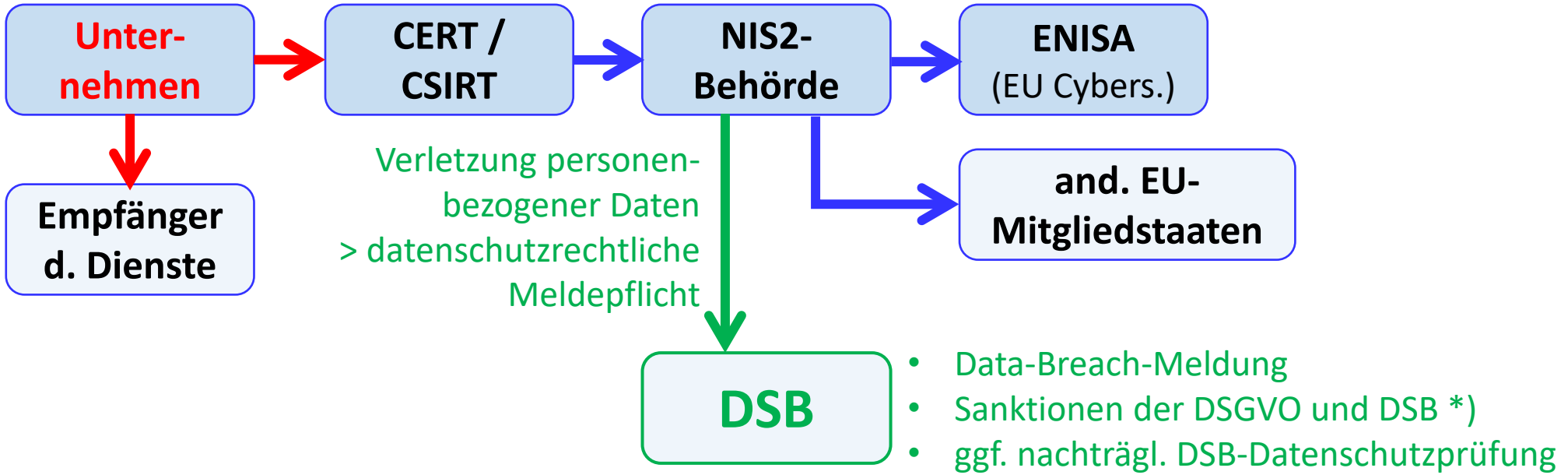
Konkretisierung in Verordnung des BMI:

- Anzahl der betroffenen Nutzer
- Dauer der Störung
- betroffenes geografisches Gebiet

DSGVO:

Datenschutzrechtliche Handlungspflichten:

- Anpassung der Verzeichnisse der Verarbeitungstätigkeiten & Datenschutzinformationen
- TOMs zu dokumentieren (Technisch Organisatorische Maßnahmen)
- Datenschutz-Folgenabschätzung



*) max. Strafrahmen in € Mio oder % ww Jahresumsatz: DSGVO 10/2% bzw. DSB 20/4%

© 2024 FRAUSCHER CONSULTING GmbH

Anwendung / betroffene Sektoren – Size-Cap-Rule

- Empfehlung 2003/361/EG der EU-Kommission
- Benutzerleitfaden der EU-Kommission zur Def. „KMU“

- **Großunternehmen**
  - min. 250 Pers. beschäftigt
  - **alt.**: - J.umsatz > € 50 Mio **und**
    - Jahresbilanzsumme > € 43 Mio

- **mittleres Unternehmen**
  - min. 50 / < 250 Pers. beschäftigt
  - **alt.**: - J.umsatz > 10 **und**
    - Jahresbilanzsumme > € 10 Mio
    - nicht schon Großunternehmen

- **Kleinunternehmen**
  - < 50 Pers. beschäftigt
  - **alt.**: - Jahresumsatz < € 10 Mio, **oder**
    - Jahresbilanzsumme < € 10 Mio

Größen-Schwellwert
(Size-Cap-Rule)

Prüfschema:
1) DL oder Tätigkeit in der EU ausgeübt?
2) wesentliche oder wichtige Einrichtung (gem. RL-Anhang I/II)
3) Size-Cap-Rule, s- links

© 2024 FRAUSCHER CONSULTING GmbH

NIS2 - Aufsicht & Durchsetzung der nat. Behörden

Prüfregime

- Aktuelles NISG-Prüfregime nicht auf NIS2 übertragbar, deutlich mehr Unterworfene
- NISG 2 / 2024:
- Selbstdeklaration als Basis
- Prüfung durch unabhängige Stellen/Prüfer

Aufsicht

- Durchsetzung & Aufsicht
- Überblick von Umsetzung und Compliance
- Eingriff & Monitoring
  - **wesentliche:** ex ante (& ex post)
  - **wichtige:** ex post

Bußgelder bei non-Compliance

Risikomanagement-Maßnahmen oder Meldepflicht:

- **wesentliche** Einrichtungen
  - (€ 100k) bis max. **€ 10 Mio**, oder
  - **2% ww** Jahresumsatz (vorige G.-Jahr)
- **wichtige** Einrichtungen
  - (€ 100k) bis max. **€ 7 Mio**, oder
  - **1,4% ww** Jahresumsatz (vorige G.-Jahr)
- Allgemeine Tatbestände
  - (€ 100k bis **€ 2 Mio**)
- Haftbarkeit leitender Angestellter (Top-Mgmt)
  - Können für Pflichtverletzungen haftbar gemacht werden

© 2024 FRAUSCHER CONSULTING GmbH

NIS2 - Aufsicht & Durchsetzung der nat. Behörden

Durchsetzung (Verwaltungsrecht)

- Mindestliste an **Verwaltungssanktionen**, jedenfalls vorzusehen, z.B.
  - verbindliche Anweisungen
  - bescheidliche Anordnungen
  - Verwaltungsstrafen, nur ultima ratio

Verhängung von Geldstrafen

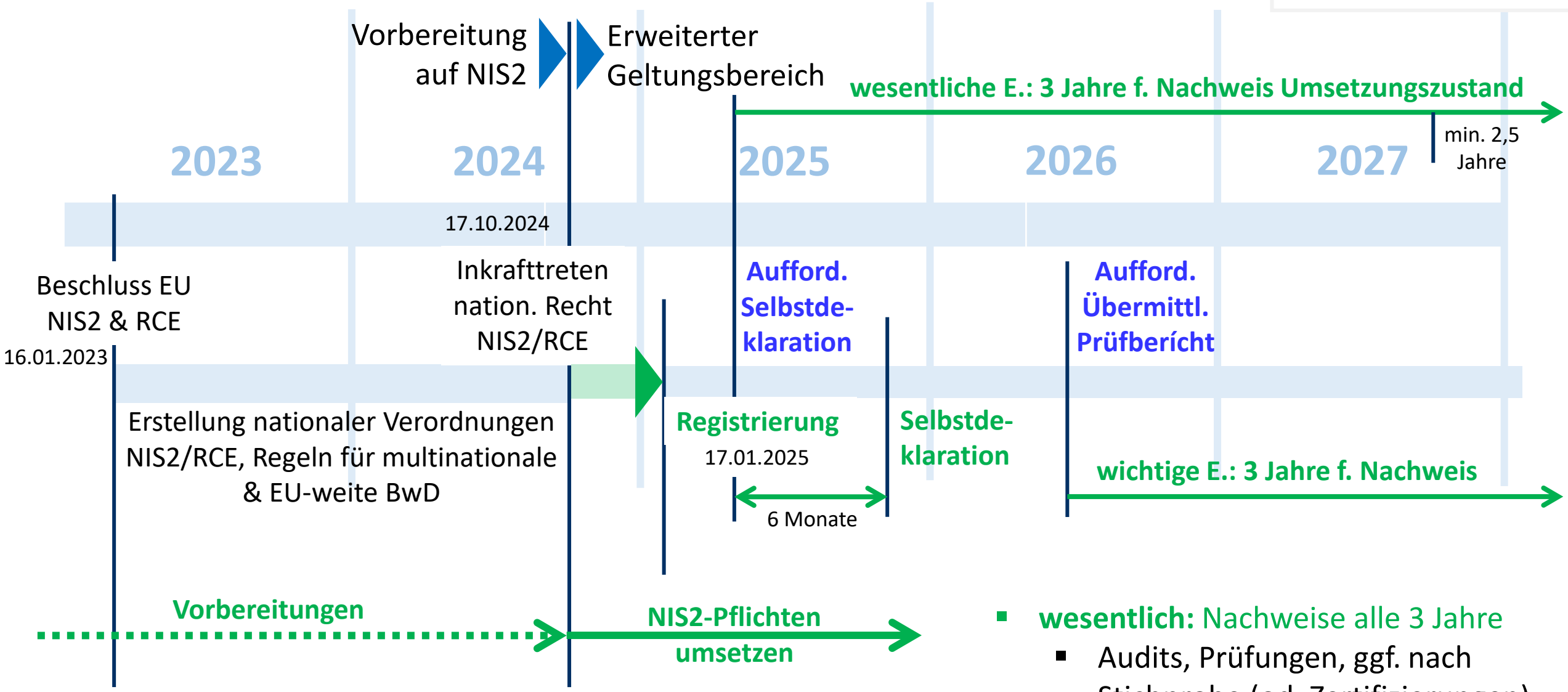
- Verstöße gegen die Verpflichtungen aus dem Bundesgesetz ergeben sich Verwaltungsstrafen
  - Bezirksverwaltungsbehörde zuständig
  - Hinsichtl. Erforderlicher Expertise > sprengelübergreifende Zusammenarbeit in „Kompetenzzentren“

- Orientierung am Bankwesengesetz
- Berücksichtigung des Doppelstrafverbotes aus demselben Verhalten (z.B. NISG 2024 & DSGVO)

© 2024 FRAUSCHER CONSULTING GmbH

Chronologie NIS2

NIS2 Behörde
NIS2 Unternehmen



- **wesentlich:** Nachweise alle 3 Jahre
  - Audits, Prüfungen, ggf. nach Stichprobe (od. Zertifizierungen)
- **wichtig:** Prüfung nach Anlass

© 2024 FRAUSCHER CONSULTING GmbH

RKE/CER

RL über die Resilienz kritischer Einrichtungen

Critical Entities Resilience Directive

© 2024 FRAUSCHER CONSULTING GmbH

Von APCIP zu RKE

APCIP		RKE
Ministerratsbeschluss	Rechtliche Basis	RKE-G als nationale Umsetzung der EU RKE-RL
Freiwilligkeit in Zusammenarbeit Unternehmen / Behörden	Verbind-lichkeit	Verpflichtung inkl. Strafbestimmungen
physischer Schutz, traditionell Objektschutz	Fokus	+ Risikobewertung + BCM + organisatorische Maßnahmen

© 2024 FRAUSCHER CONSULTING GmbH

Anwendung / Sektoren: 18 NIS2 – 11 RKE/APCIP

Anhang I (= Sektoren mit hoher Kritikalität)	Anhang II (= sonstige kritische Sektoren)
Energie (Elektrizität, Fernwärme/Kälte, Öl, Gas und Wasserstoff)	Post- und Kurierdienste
Verkehr (Luft, Schiene, Schifffahrt, Straße)	Abfallbewirtschaftung
Bankwesen	Chemie (Herstellung und Handel)
Finanzmarkt	Lebensmittel (Produktion, Verarbeitung, Vertrieb)
Gesundheits (Gesundheits Herstellung und Geräte)	Verarbeitendes / Herstellendes Gewerbe (Medizinprodukten; Datenverarbeitungs-, elektronische und optische Geräte und elektronische Ausrüstungen; Maschinenbau; Kraftwagen und Kraftwagenteile und sonstiger Fahrzeugbau)
Trinkwasser	Anbieter digitaler Dienste (Suchmaschinen, Online-Marktplätze und soziale Netzwerke)
Abwasser	Forschung
Digitale Infra (IXP, DNS, TL Anbieter öffe dienste)	Hilfs- & Einsatzkräfte
Verwaltung v	Sozial- & Verteilungssysteme
Öffentliche Verwaltung	
Weltraum	

- Viele Unternehmen gem. APCIP kritische Infrastruktur, aber nicht gem. RKE-RL
- künftige Zusammenarbeit mit Sicherheitsbehörden:
  - freiwillige Einbindung in RKE
  - Neben RKE Weiterführung APCIP

Rot = Neuerungen gegenüber NIS1

Quelle:
NIS2 Die neue Cybersicherheits-Richtlinie WKÖ Live-Webinar Mag. Vinzenz Heußler, LL.M. Bundeskanzleramt, Abteilung I/8 (Cyber Security, GovCERT, NIS-Büro und ZAS) Leiter NIS-Büro Wien, 21. Februar 2023

© 2024 FRAUSCHER CONSULTING GmbH

RKE - Pflichten kritischer Einrichtungen

Pflichten der kritischen Einrichtungen:

- Risikobewertung & -management
- Erstellung Resilienzplan
  (od. gleichwertige Dokumente)
- Umsetzung geeigneter & verhältmässiger technischer, sicherheitsbezog. und organisatorischer Maßnahmen
- Meldepflicht, Krisen & erhebliche Sicherheitsvorfälle (nat. + EU), ev. gleiche Portal wie etablierte NIS2
- Vor-Ort-Kontrollen oder Audits der krit. Infrastruktur & der Räumlichkeiten
- alternative Lieferketten, um wesentl. Dienste ggf. wiederaufzunehmen
- Kooperationspflicht
- Benennung Ansprechpartner
- Antrag auf Zuverlässigkeitsprüfungen möglich

maßgebende Ziele:

- EU: Mindeststandards (ggü. Land & krit. Einrichtungen)
- Verfügbarkeit & Unterbrechung von DL
- Normative Resilienz Vorgaben auf nat. Ebene
- BCM verbessern
- Physische Sicherheit

© 2024 FRAUSCHER CONSULTING GmbH

RKE - Sanktionen

Sanktionen:

- von Mitgliedstaaten erlassen
- müssen wirksam, verhältnismäßig & abschreckend sein

Bei Nichterfüllung der Verpflichtungen:

- Maxime: Dialog statt Strafen
- Anordnung durch Bescheid > Herstellung des rechtmäßigen Zustands
- letzte Konsequenz: Verwaltungsstrafe:
  - bis € 7 Mio
  - bis 1,4 % ww Gesamtnetto-Jahresumsatz des Vorjahres
  - je nachdem welcher Betrag höher

Prüfregime – Aufsicht & Durchsetzung:

- müssen **proaktiv übersendet** werden
- BMI kann innerhalb angemessener Frist einen **Nachweis für Erfüllung** der Verpflichtungen verlangen
- **Anordnung von Audits** durch „Qualifizierte Stellen“ / vor-Ort-Kontrollen (nach vorheriger Ankündigung)

© 2024 FRAUSCHER CONSULTING GmbH

RKE - Anwendungsbereich

bescheidmäßige Feststellung

4 kumulative Voraussetzung:

1) KE im Inland tätig **+** 2) krit. Infrastruktur der KE im Inland **+** 3) min. 1 wesentlicher Dienst erbracht **+** 4) potenz. Sicherheits-vorfall *)

Schwellenwerte

Analog NIS1 in Branchengesprächen mit Interessensvertretungen erarbeitet

- Für wesentliche Dienste & Sicherheitsvorfälle
- 7 Sektoren (NIS-G/-VO) zu adaptieren, 4 neu zu erarbeiten
- per Verordnung des BM kundgemacht

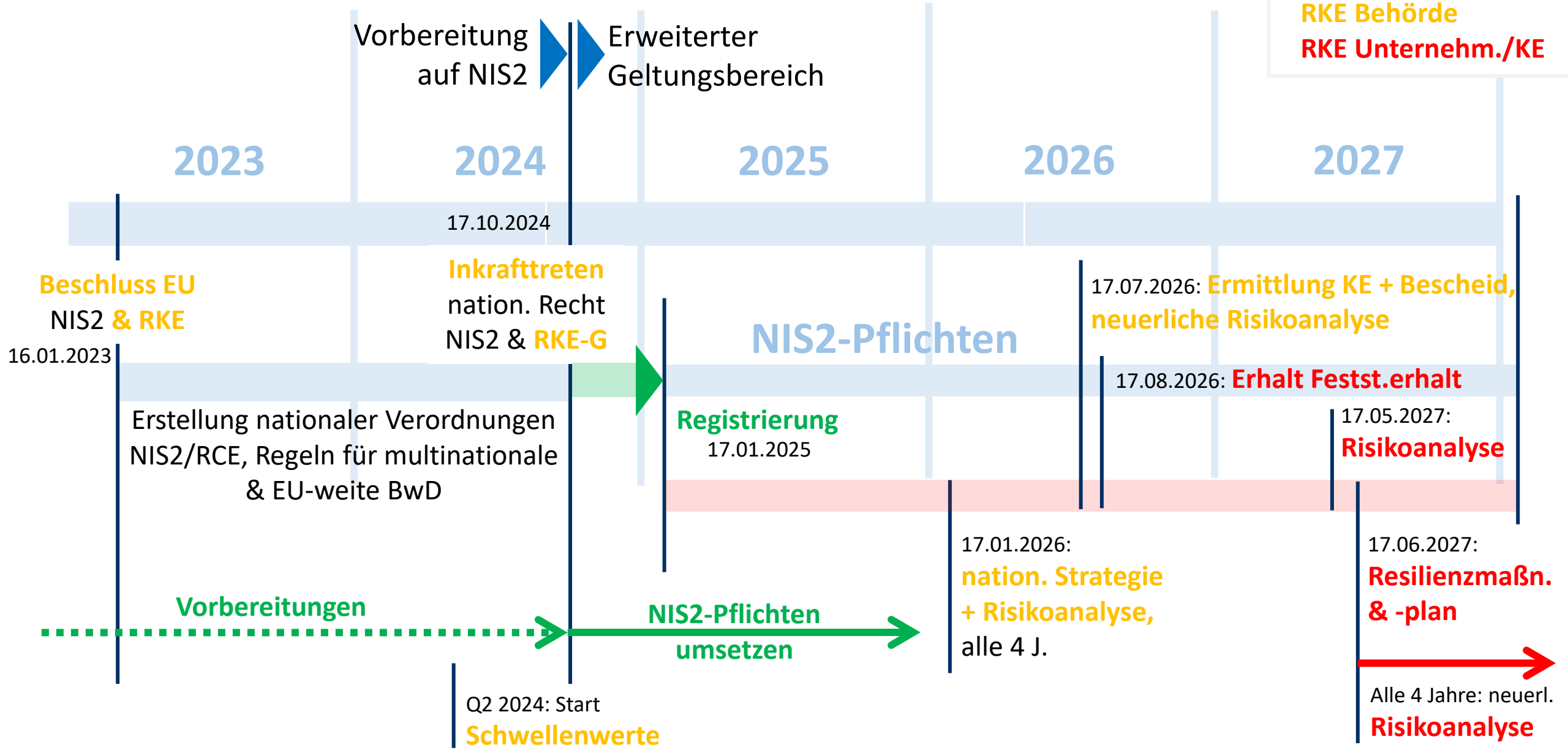
*) ein Sicherheitsvorfall könnte eine erhebliche Störung **) bei dem wesentlichen Dienst oder bei anderen wesentlichen Diensten, die von der Einrichtung abhängig sein, bewirken

**) wann eine Störung erheblich ist wird vom BMI mittels Verordnung für jeden (Teil-)Sektor konkretisiert

© 2024 FRAUSCHER CONSULTING GmbH

Chronologie NIS2 & RKE

NIS2 Behörde
NIS2 Unternehm./KE
RKE Behörde
RKE Unternehm./KE

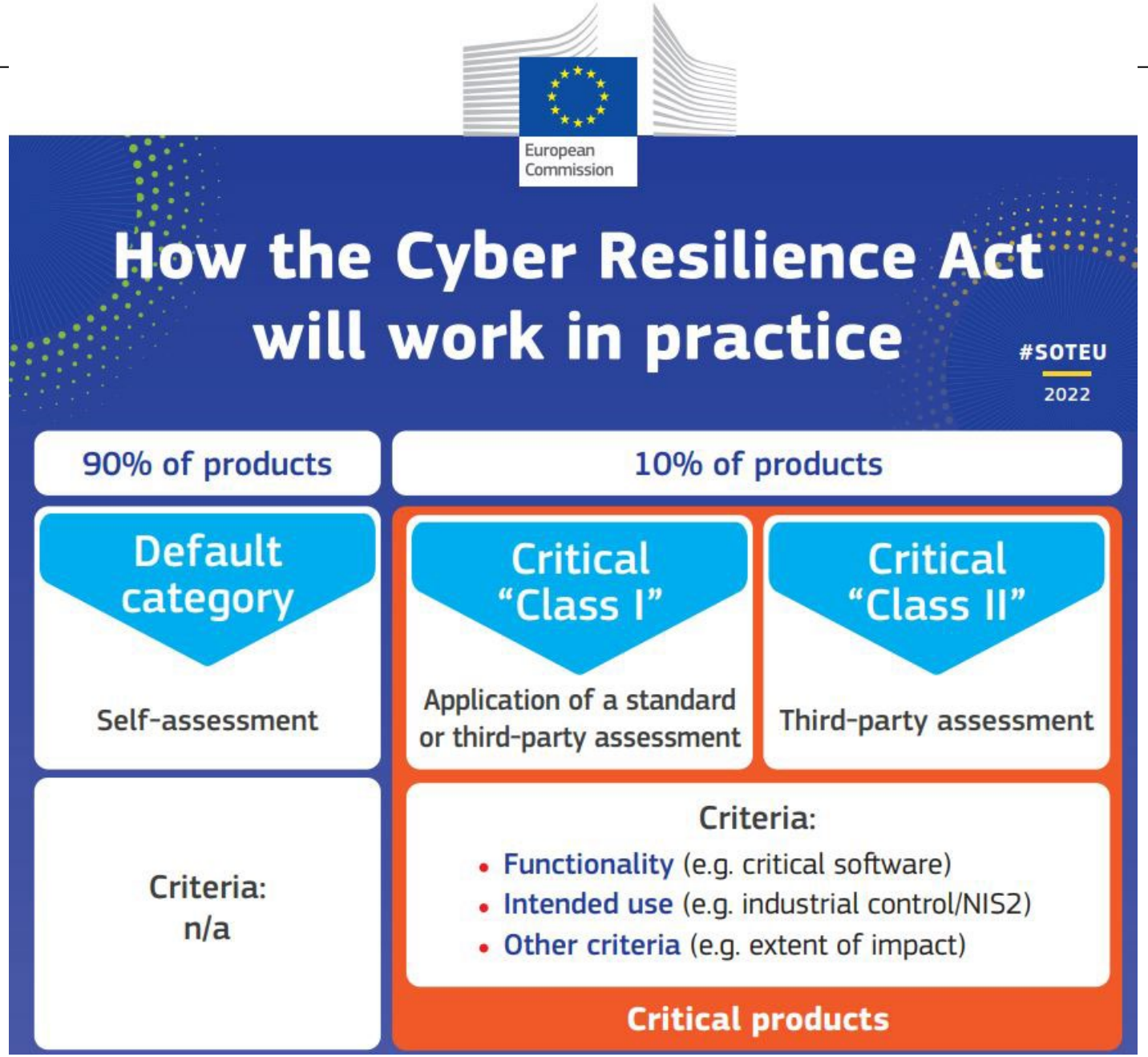


© 2024 FRAUSCHER CONSULTING GmbH

CRA

Cyber Resiliency Act

© 2024 FRAUSCHER CONSULTING GmbH



© 2024 FRAUSCHER CONSULTING GmbH

Womit ist zu rechnen?

© 2024 FRAUSCHER CONSULTING GmbH

CRA: Beschluss EU-Rat noch Q2 2024.

Umsetzung RKE-RL Mitte Mai 2024 möglich.

NIS-G 2024 & ggf. NIS-VO bis Ende 2024.

Beschluss des NISG 2024 nach bereits erfolgter Begutachtung.

Konkretisierung der Umsetzungsanforderungen
in der NIS2 VO bis Jahresende / Anfang 2025?

Bis dahin ist der §32 des Gesetzesentwurfes NISG 2024 eine Orientierung für die kommenden Risikomanagement-Maßnahmen.

© 2024 FRAUSCHER CONSULTING GmbH

NIS2 RL 2024, Interpretation der zu erwartenden Inhalte - beispielhaft

- Angaben zur Durchführung von Risikomanagementmaßnahmen
  > weitgehend anwendbar auf Konvergenz IT/OT
- Nähere Angaben zu einer Risikoanalyse > Grundlage eines ausgewogenen Sicherheitskonzeptes
- Richtlinien zur Sicherheit von Lieferketten, Anforderungen an das Unternehmen & an Lieferanten
  > selben Anforderungen wie bei IT-Betrieb für OT
- Details zum Umgang mit Cybersicherheitsvorfällen > z.B. Inselbetrieb, Wiederaufnahme Regelbetrieb
- Nähere Angaben zur Überwachung von Systemen und Netzwerken > Security Operations
- Spezifizierung von Physischer Zutrittskontrolle > RA-abhängig Ausprägung der Maßnahmen
- Anforderungen an Protokollierungen, Analyse und Dokumentation > Zutrittskontrolle + SMS
- Prävention der Auswirkungen von Cybersicherheitsvorfällen: Angaben zu
  - Incident Response
  - Business Continuity & Recovery (Backup-Wiederherstellung) > Wiederanlauf der OT für KRITIS
- Kommunikation, Meldungen nach innen & außen > 7/24h-Analyse & -Response der GLT/MSR/SMS
- Schulungsmaßnahmen, Cybersecurity-Bewußtseinsbildung & -kompetenz > Sicherheitstestläufe
- Netzwerksicherheit > z.B. OT-Netzwerke-Segmentierung + Pentests
- Überprüfung der Wirksamkeit der Sicherheitsmaßnahmen > Audits, Zertifizierungen, Compliance

© 2024 FRAUSCHER CONSULTING GmbH

Physische Sicherheit?

© 2024 FRAUSCHER CONSULTING GmbH

NIS2 & Physische Sicherheit

NIS1

NIS Fact Sheet 9/2022:
Pkt. 7.1 Phys.Sicherheit:
Der **Physische Schutz vor unbefugtem Zutritt** & Zugang ist zu gewährleisten.
Betreiber erstellt ein **Phys. Sicherheitskonzept inkl. Sicherheitszonen** und definiert Verfahren für den **sicheren Umgang** mit versch. Personengruppen.

NIS2 Ankündigungen

Orientierung an den Kategorien der Sicherheitsmaßnahmen der NISV;
sinngemäß angewandt für IT & OT

NIS2 Gesetzesentwurf

(ausgeg. 03.04.2024, Begutachtung bis 01.05.2024)

§32 (2) 2. NISG 2024, Begutachtungsentwurf:
Risikomanagement-Maßnahmen im Bereich der Cybersecurity: … diese haben auf einem **gefahrenübergreifenden Ansatz** zu beruhen, der auf den Schutz von Netz- & Informations-Systemen **und deren physischer Umwelt** vor Cyber-sicherheitsvorfällen abzielt.

NIS2 Verordnung (Interpretation)

Spezifizierungen der Anforderungen aus dem NISG 2024 werden erwartet.

Aber auch:

1. Ein dem besteh. Risiko angemessenes Cyber-sicherheitsniveau ist zu gewährleisten auf dem Stand der Technik

3. Die Sicherheit der Lieferketten ist gebührend zu berücksichtigen.

© 2024 FRAUSCHER CONSULTING GmbH

CRA & Physische Sicherheit

Erhebliche Auswirkungen auf Produkte der Sicherheitstechnik:
> ZuKo, EMA, Video, SMS, Detektoren, Sensoren, …

- So gut wie alle Endprodukte und Software-Komponenten
- Pflichten für Hersteller, wie initiales Risiko-Assessment
- Für die Lebensdauer
  - ist Cybersicherheit zu gewährleisten
  - Kostenlose Updates zur Verfügung zu stellen
- Nachweise der Konformität
- Bei sicherheitsrelevanten Vorfällen > Meldepflicht binnen 24h an Cyber Security Incident Response Team
- Sanktionen: € 15 Mio oder 2,5% ww Umsatz + ggf. Produkte-Rückholung
- Gilt für Produkte des Binnenmarktes und von aussen

© 2024 FRAUSCHER CONSULTING GmbH

RKE & Physische Sicherheit

RKE-RL, Artikel 13:
Mitgliedstaaten stellen sicher, dass krit. Einrichtungen … geeignete & verhältnismässige technische, sicherheitsbezogene & organis. Maßnahmen zur Gewährleistung ihrer Resilienz ergreifen, u.a.:

- Verhinderung Auftreten von Sicherheitsvorfällen, gebührende Katastrophenvorsorge, Maßnahmen zur Anpassung an den Klimawandel
- Angemessener physischer Schutz der Räumlichkeiten & krit. Infrastrukturen
- Sicherheitsvorfälle: reagieren / abwehren / Folgen begrenzen
- Nach Sicherheitsvorfällen Wiederherstellung der wesentlichen Dienste
- Angemessenes Sicherheits-Management hinsichtlich der Mitarbeiter: Festlegung von (Kategorien von Personal mit kritischen Funktionen, Zugangsrechte, Qualifikation,…)
- entsprechendes Personal für die genannten Maßnahmen zu sensibilisieren

© 2024 FRAUSCHER CONSULTING GmbH

Next Steps

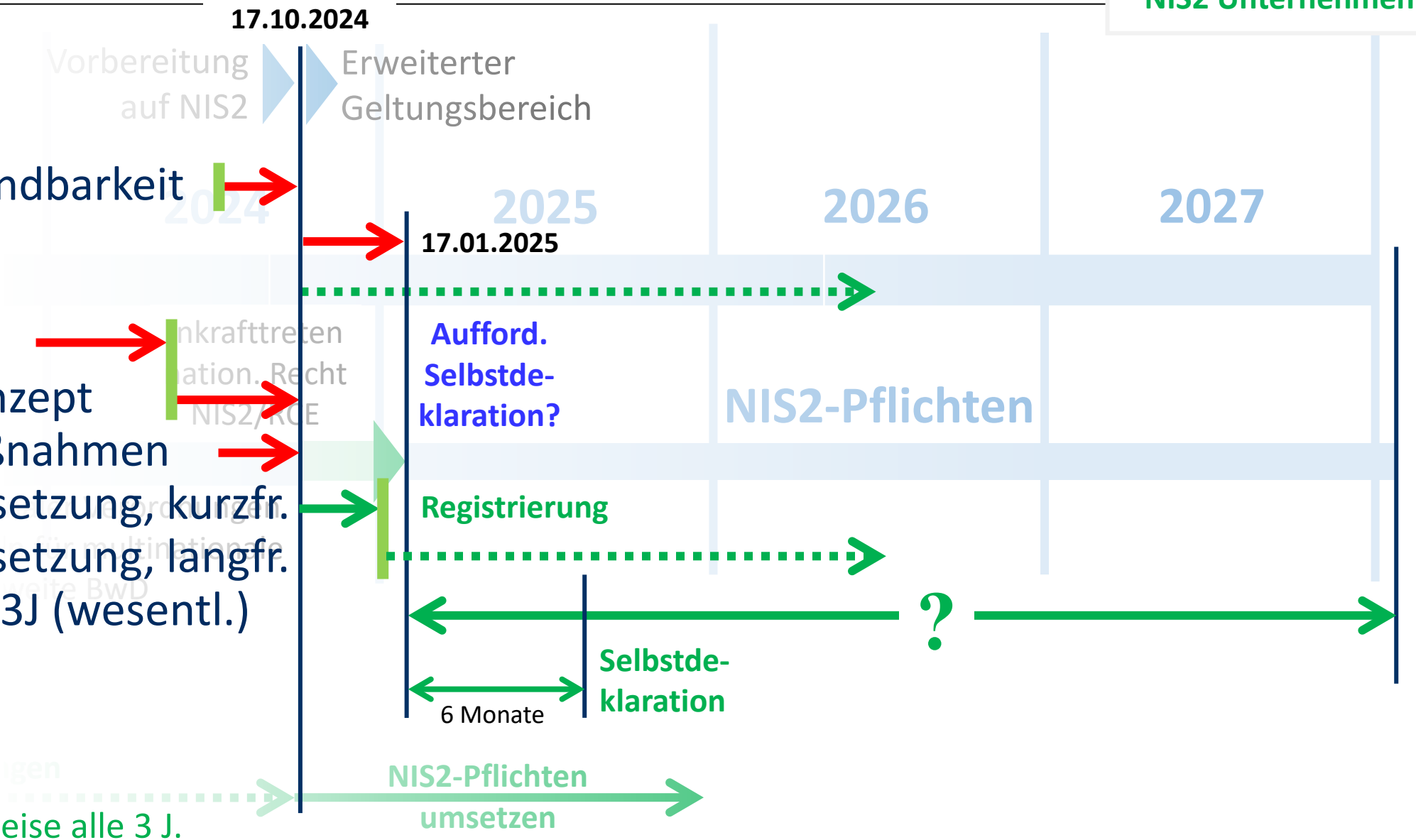
to NIS2-Compliance

© 2024 FRAUSCHER CONSULTING GmbH

Next Steps - Chronologie NIS2

NIS2 Behörde
NIS2 Unternehmen

- Klärung Anwendbarkeit
- Registrierung
- Meldepflicht
- Risikoanalyse
- Sicherheitskonzept
- Schulungsmaßnahmen
- Planung / Umsetzung, kurzfr.
- Planung / Umsetzung, langfr.
- Nachweis alle 3J (wesentl.)



- **wesentlich:** Nachweise alle 3 J.
- **wichtig:** Prüfung nach Anlass

© 2024 FRAUSCHER CONSULTING GmbH

Next Steps

Selbstverantwortlichkeit:

- Anwendbarkeit
- Registrierung
- risikobasierter Ansatz (Allgefahrenansatz), via Risikoanalyse:
- NIS2-RA voraussichtlich für RKE weiter verwendbar

risikobasierter Ansatz:

- Cybersicherheit – bisher definiert: IT betroffen
- Künftig: risikobasiert alle Einflüsse mit Auswirkung auf IT

IT-OT-Konvergenz:

- Überprüfen auf Cyber-Anfälligkeit

Meldepflicht:

- Jedenfalls auch bezogen auf Breach der OT / Physischen Sicherheit
- Einmelden binnen 24h
- Folge: etabliertes 24/7h-Monitoring

zusätzliche Aufwände:

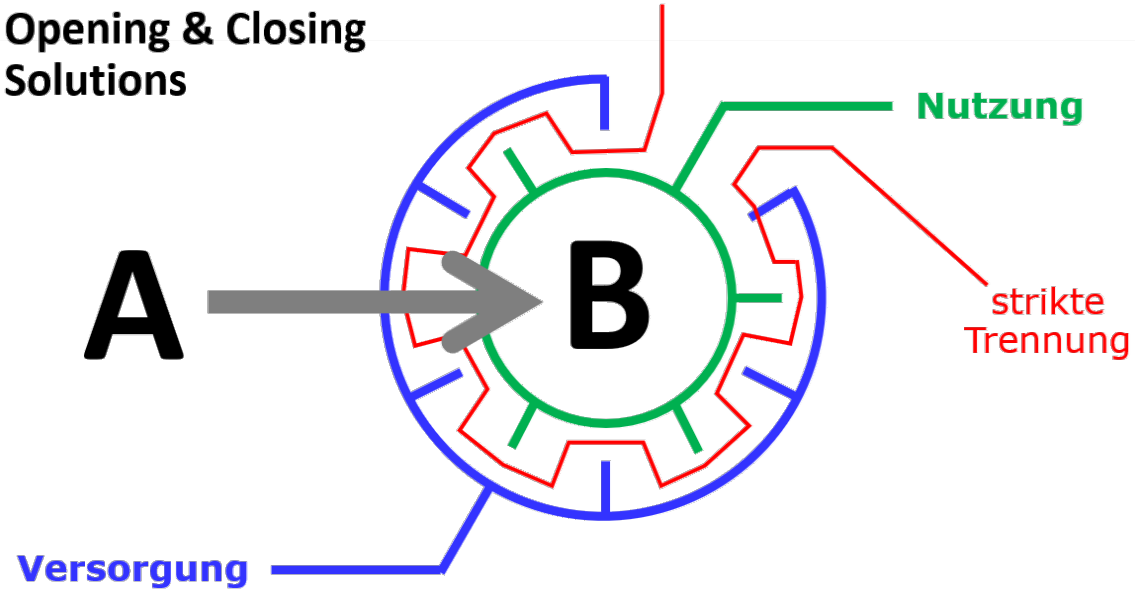
- Anpassung an den Stand der Technik, Meldepflicht, Compliance-Aufwände

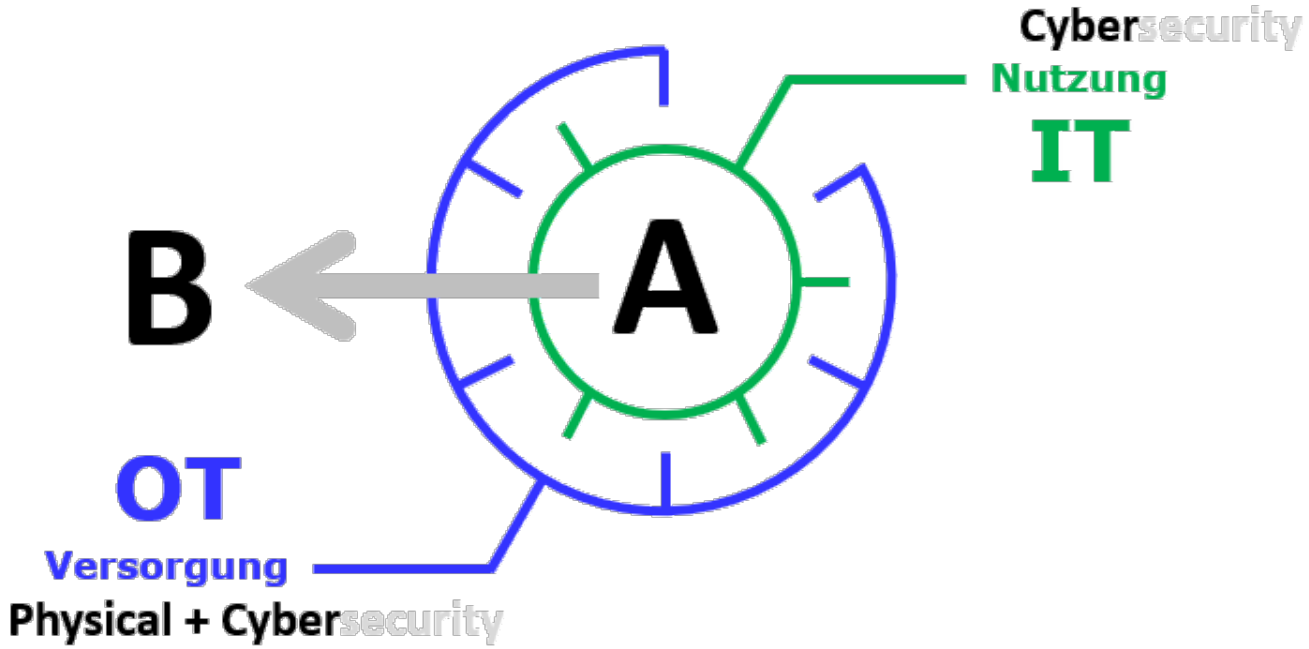
Umsetzung:

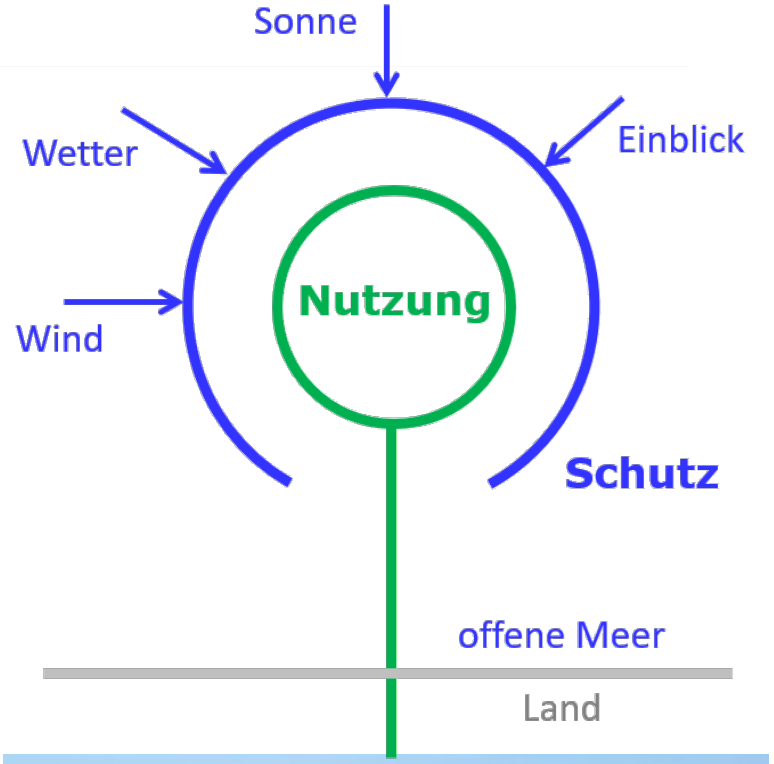
- straffen rechtlichen Zeitpläne vs. Fachkräftemangel insbesondere bei Cybersecurity

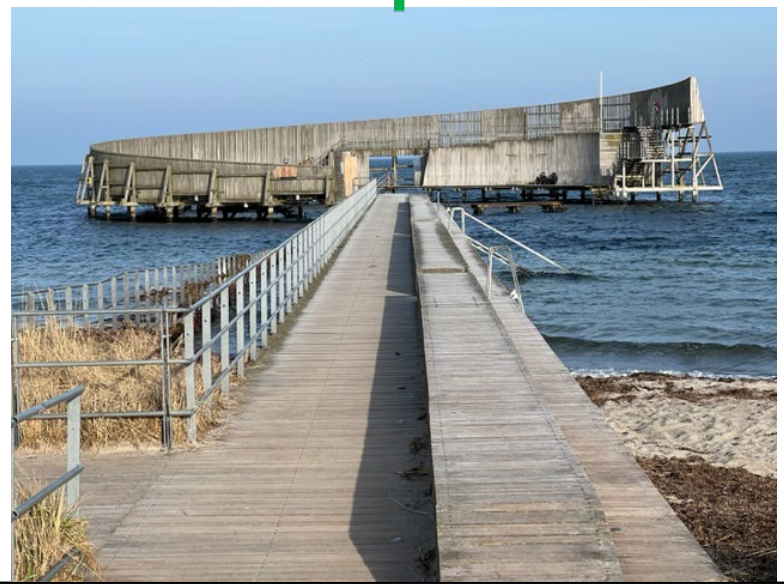
© 2024 FRAUSCHER CONSULTING GmbH

Opening & Closing Solutions









© 2024 FRAUSCHER CONSULTING GmbH

Reliable and Energy Efficient Data Center Design & Services

Rechenzentrum?
Data Center?

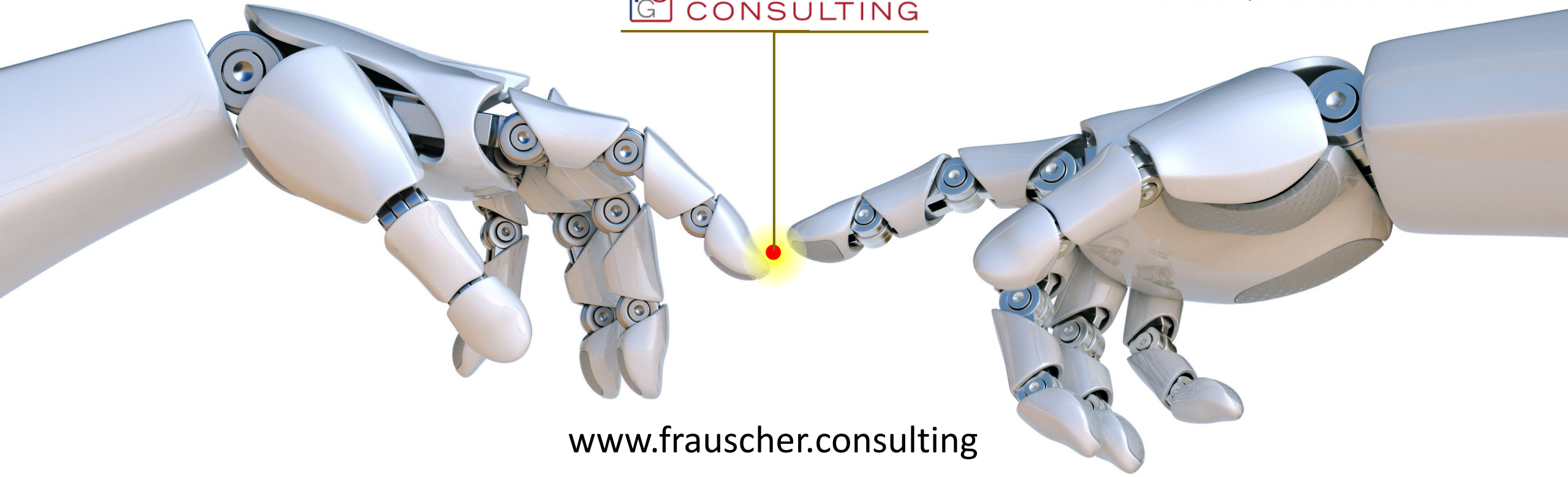
Cyber

IT

Physical

RZ Architektur
TGA, Services

FRAUSCHER CONSULTING



www.frauscher.consulting

© 2024 FRAUSCHER CONSULTING GmbH

ASSA ABLOY
Opening Solutions

Opening Solutions Day

Experience a safer
and more open world

Danke.

FRAUSCHER CONSULTING

Dipl.-Ing. Georg Meixner, MBA

georg.meixner@frauscher.consulting

+43 676 884855 210

© 2024 FRAUSCHER CONSULTING GmbH