NIS-2-Richtlinie

Umsetzung in Deutschland und anderen Mitgliedstaaten der Europäischen Union

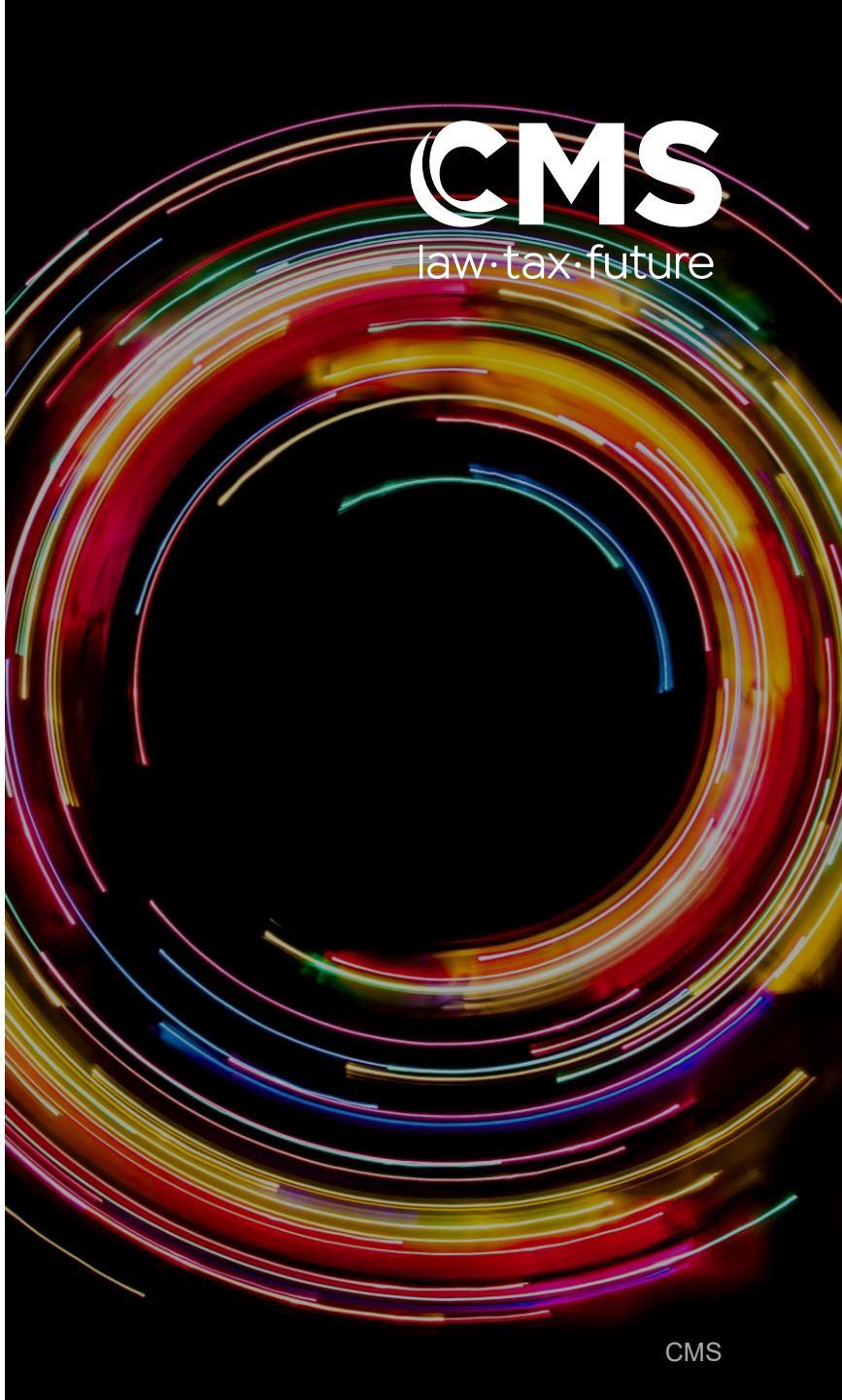
Dr. Michael Biendl, M.A.

Dr. Michael Biendl, M.A.

Counsel

IT-Grundschutz-Praktiker nach BSI-Curriculum

T +49 89 23807 0
E michael.biendl@cms-hs.com



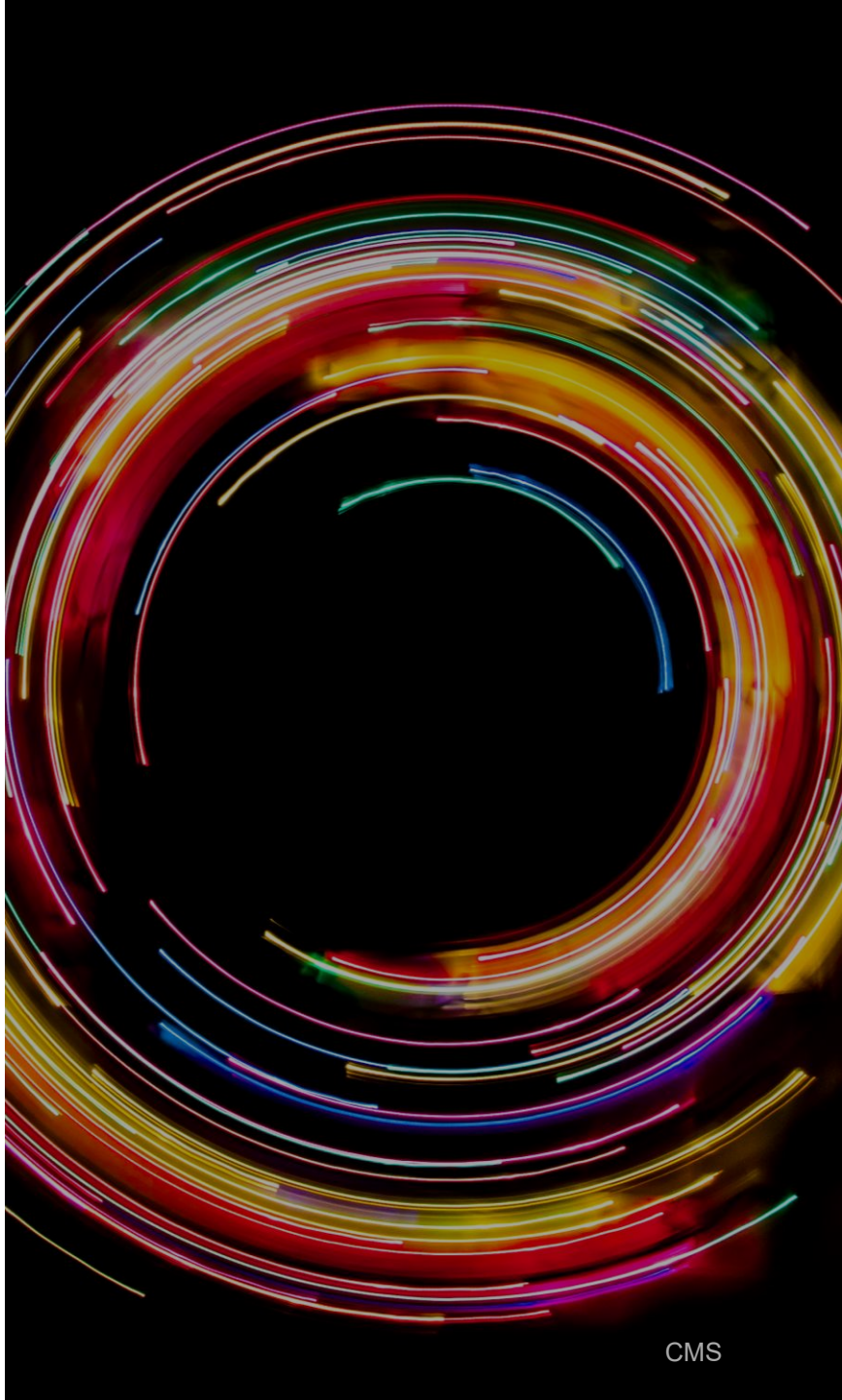
Agenda

I. Umsetzungsstand

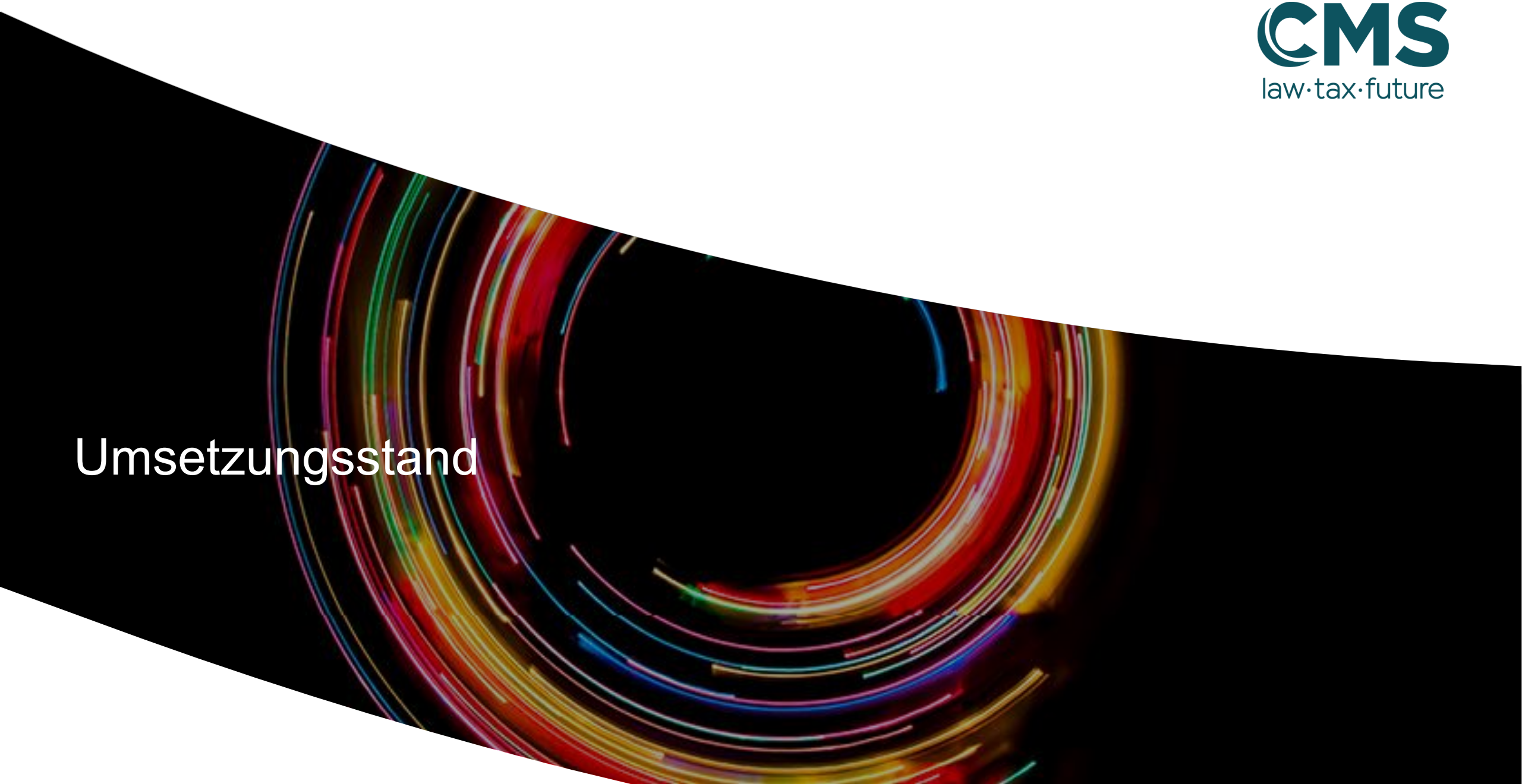
II. Anwendbarkeitsprüfung

III. Pflichtenkanon

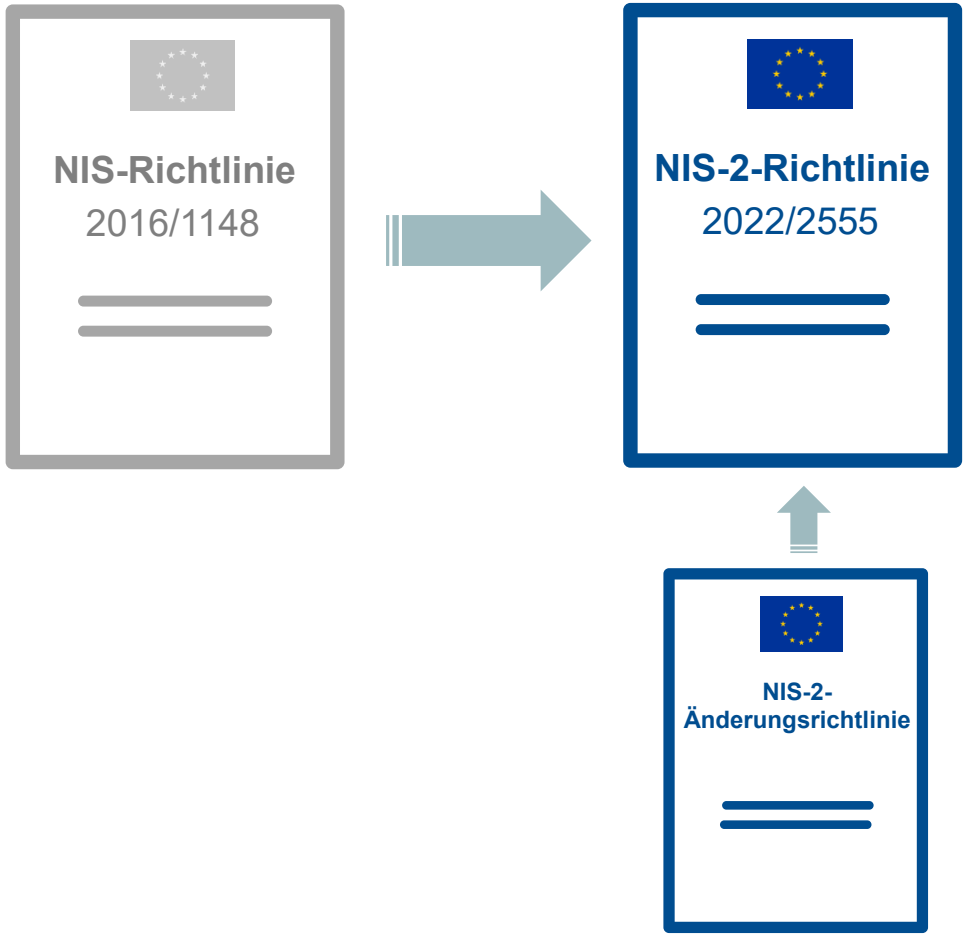
IV. Q&A

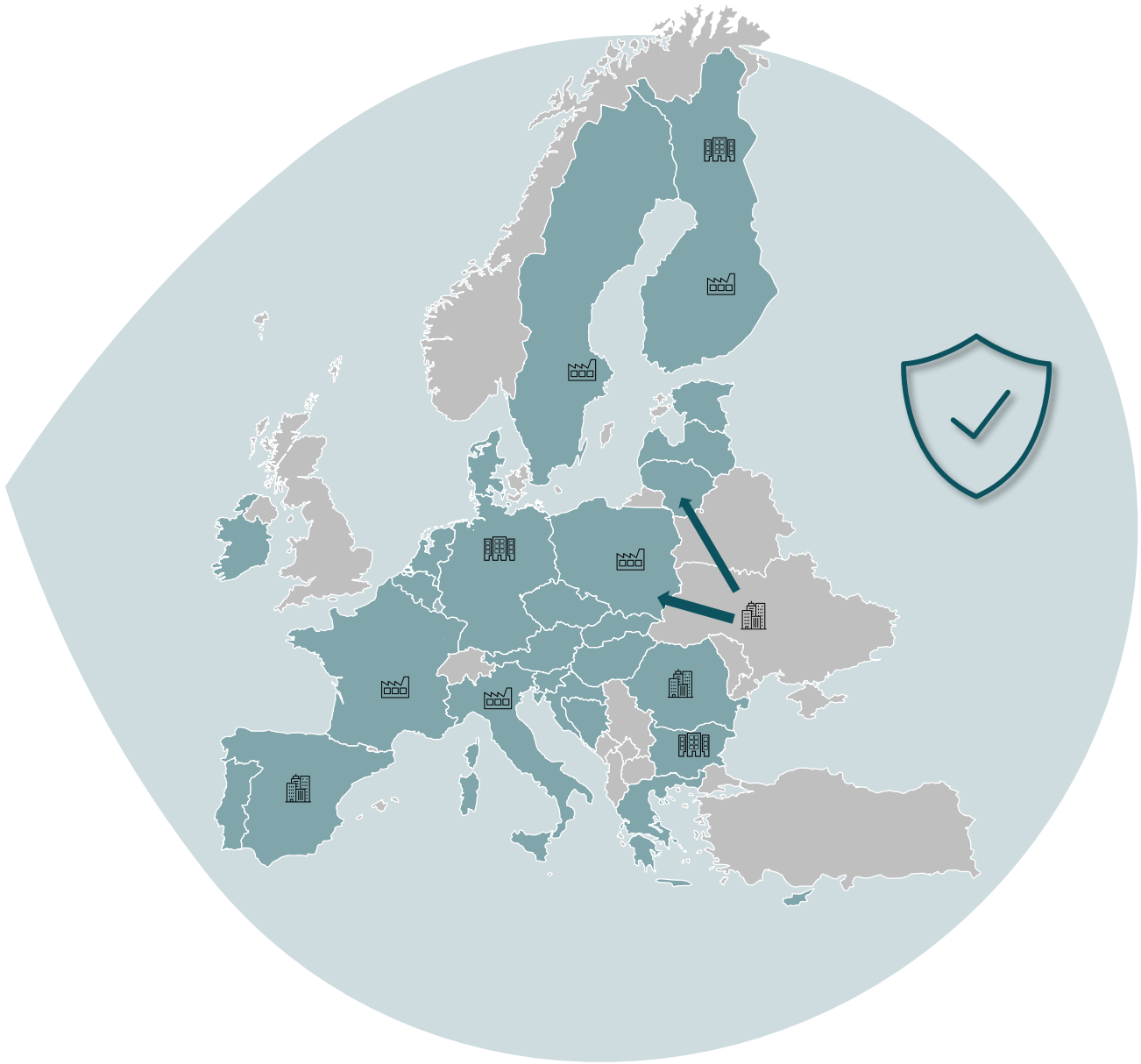


Umsetzungsstand



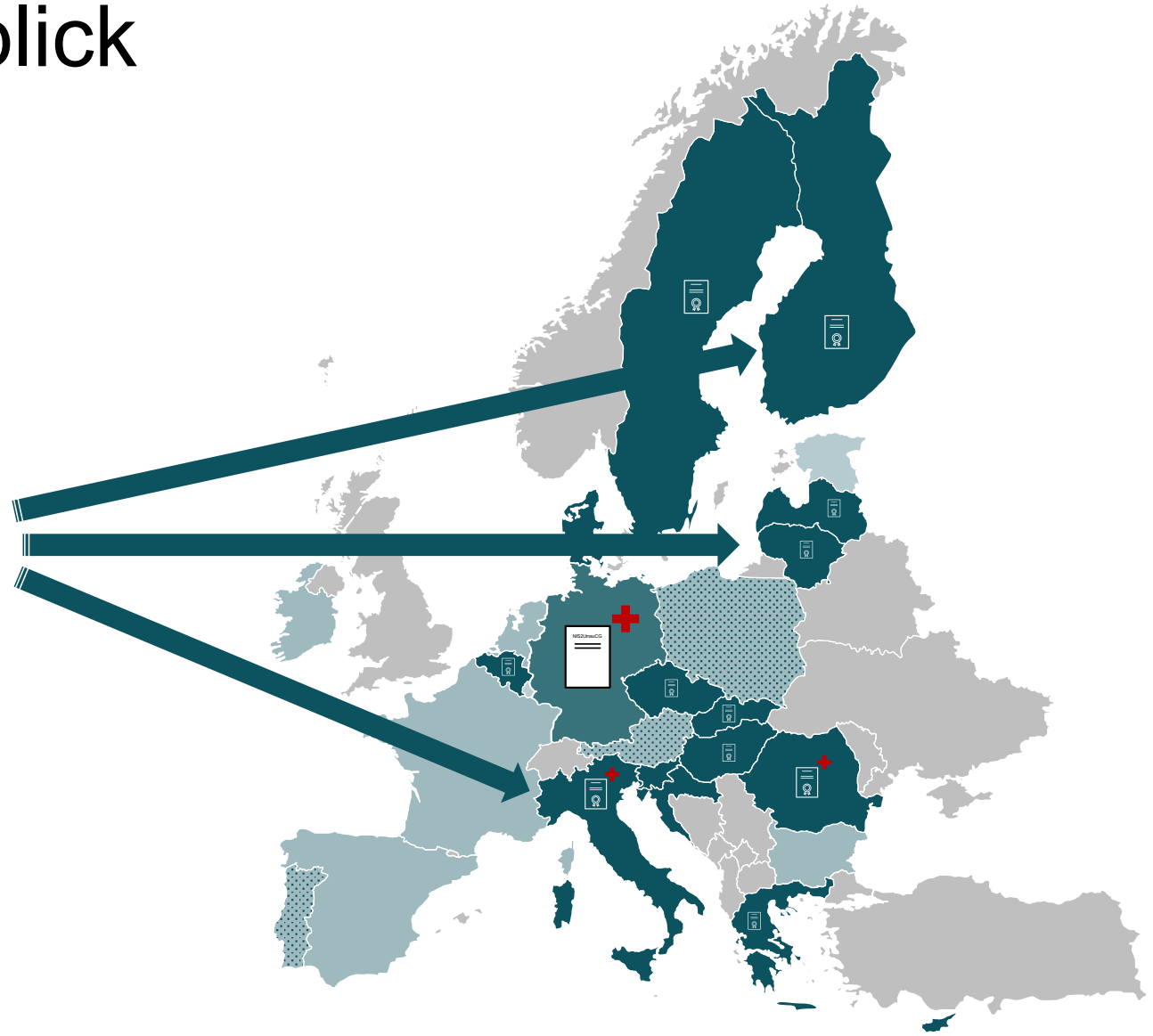
NIS-2 im Überblick





NIS-2 im Überblick

NIS-2-Richtlinie
2022/2555

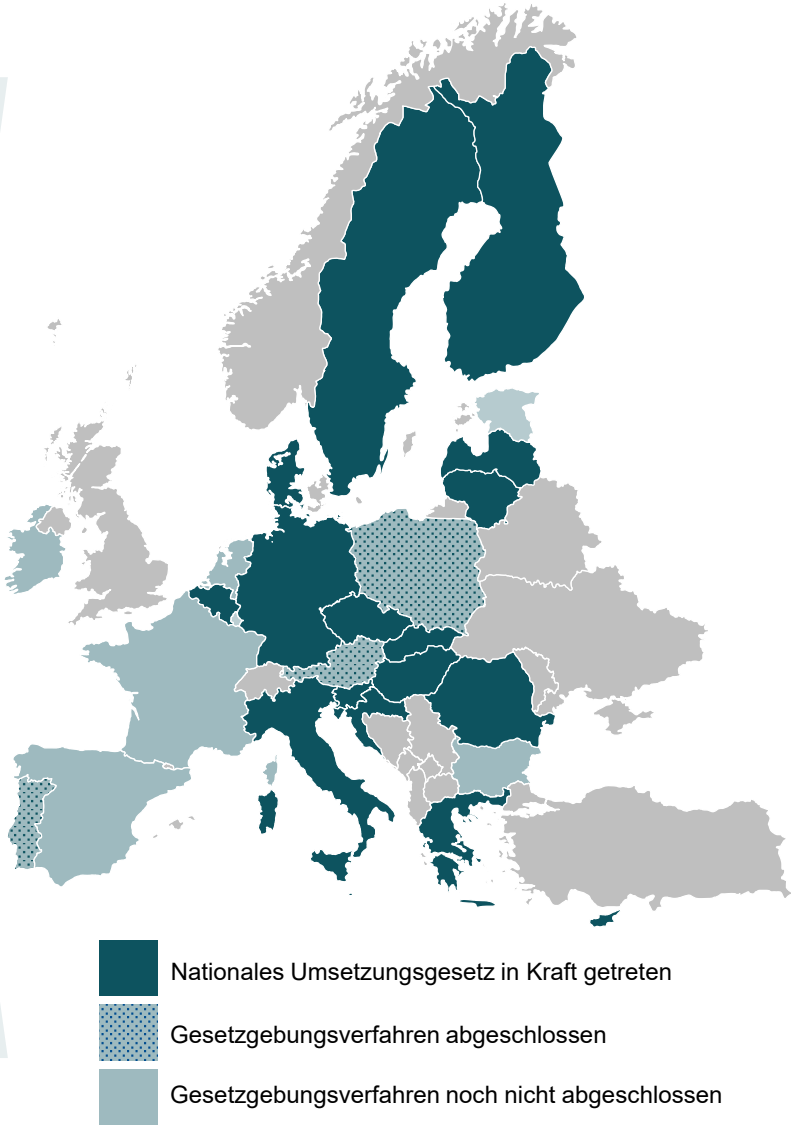


Umsetzungsstand in der Europäischen Union

Umsetzungsgesetz in Kraft getreten	
Land	**In-Kraft-Treten**
Belgien	18. Oktober 2024
Dänemark	1. Juli 2025
Deutschland	6. Dezember 2025
Finnland	8. April 2025
Griechenland	27. November 2024
Ungarn	3. Januar 2025
Italien	16. Oktober 2024
Kroatien	15. Februar 2024
Lettland	1. September 2024
Litauen	18. Oktober 2024
Rumänien	30. December 2024
Slowakei	1. Januar 2025
Slowenien	19. Juni 2025
Schweden	15. Januar 2026
Tschechien	1. November 2025
Zypern	25. April 2025

Gesetzgebungsverfahren abgeschlossen	
Land	**In-Kraft-Treten**
Österreich	1. Oktober 2026
Polen	Ende März
Portugal	3. April 2026

Gesetzgebungsverfahren noch nicht abgeschlossen	
Land	**Geplantes In-Kraft-Treten**
Bulgarien	Q1 2026
Frankreich	Q1 2026
Irland	Q1/Q2 2026
Luxemburg	Q1 2026
Estland	Q1/Q2 2026
Malta	n/a
Niederlande	Q2 2026
Spanien	Q1/Q2 2026



Welches nationale Gesetz findet Anwendung?

Tätigkeiten, die vor Ort ausgeübt werden

Niederlassungsprinzip

Art. 26 Abs. 1

*"Einrichtungen, die in den Anwendungsbereich dieser Richtlinie fallen, gelten als der Zuständigkeit des Mitgliedstaats unterliegend, **in dem sie niedergelassen sind**, außer in folgenden Fällen […]"*

Digitale Dienste (nicht: Telekommunikation)

One-Stop-Shop-Prinzip

Art. 26 Abs. 1 lit. b) i.V.m. Abs. 2

*"DNS-Diensteanbieter, TLD-Namenregister, Einrichtungen, die Domänennamen-Registrierungsdienste erbringen, **Anbieter von Cloud-Computing-Diensten**, **Anbieter von Rechenzentrumsdiensten**, Betreiber von Inhaltszustellnetzen, **Anbieter von verwalteten Diensten**, **Anbieter von verwalteten Sicherheitsdiensten** sowie Anbieter von Online- Marktplätzen, Online-Suchmaschinen oder Plattformen für Dienste sozialer Netzwerke, die als der Zuständigkeit des Mitgliedstaats unterliegend betrachtet werden, in dem sie gemäß Absatz 2 **ihre Hauptniederlassung in der Union** haben"*

Die Bestimmung der Hauptniederlassung unter dem One-Stop-Shop-Prinzip

Als Hauptniederlassung gilt gemäß Art. 26 Abs. 2

1) die Niederlassung in demjenigen Mitgliedstaat betrachtet wird, in dem die **Entscheidungen im Zusammenhang mit den Maßnahmen zum Cybersicherheitsrisikomanagement vorwiegend getroffen werden**
2) Kann ein solcher Mitgliedstaat nicht bestimmt werden oder werden solche Entscheidungen nicht in der Union getroffen, so gilt als Hauptniederlassung der Mitgliedstaat, in dem die **Cybersicherheitsmaßnahmen durchgeführt werden**.
3) Kann ein solcher Mitgliedstaat nicht bestimmt werden, so gilt als Hauptniederlassung der Mitgliedstaat, in dem die betreffende Einrichtung die Niederlassung mit der **höchsten Beschäftigtenzahl in der Union** hat.

[weitere Spezifizierungen in Erwägungsgrund 114 der NIS2-Richtlinie]

Achtung:

Hat eine dem One-Stop-Shop-Prinzip unterfallende Einrichtung **keine Niederlassung in der Union**, bietet aber Dienste innerhalb der Union an, muss sie einen **Vertreter in der Union benennen**. Der Vertreter muss in einem der Mitgliedstaaten niedergelassen sein, in denen die Dienste angeboten werden. Es wird davon ausgegangen, dass eine solche Einrichtung der **Zuständigkeit des Mitgliedstaats** unterliegt, in dem der **Vertreter niedergelassen** ist.

Wurde in der Union kein Vertreter benannt, kann ***jeder Mitgliedstaat***, in dem die Einrichtung Dienste erbringt, gegen die Einrichtung rechtliche Schritte wegen des Verstoßes gegen diese Richtlinie einleiten.

NIS-2 vs. CER

	NIS-2	CER
	Sicherheit von Netz- und Informationssystemen	(Physische) Resilienz kritischer Infrastrukturen
	Einrichtungen aus mind. 13 verschiedenen Sektoren	Betreiber kritischer Anlagen aus mind. 10 Sektoren
	Cybersicherheitsbezogenes Risikomanagement	Risikoanalyse + Maßnahmen zur Gewährleistung der Resilienz
	BSIG 2025 u.a.	Kritis-Dachgesetz

Umsetzung in Deutschland

	NIS-2	CER
Referentententwurf	24. Juni 2025	29. August 2025
Regierungsentwurf	30. Juli 2025	10. September 2025
Zuleitung BR	15. August 2025	10. Oktober 2025
1. Durchgang BR	26. September 2025 (TOP 32; Ausschussempfehlung)	21. November (TOP 38; Ausschussempfehlung)
1. Lesung BT	11. September 2025	6. November 2025
Ausschüsse und SV-Anhörungen	13. Oktober 2025	1. Dezember 2025
2./3. Lesung BT	13. November 2025 (DIP)	29. Januar 2026
2. Durchgang BR	21. November 2025 (DIP)	**Vermittlungsausschuss!**
Inkrafttreten	6. Dezember 2025	

Anwendbarkeitsprüfung

Anwendungsvoraussetzungen – schematisch

	§ 28 BSIG	Kritis-DachG-E
1 Einrichtungsart	§ 28 Abs. 1, 2 und 3, Anhang 1, Anhang 2	(neue) BSI-Kritis-V (Delegierte Verordnung 2023/2450)
2 Schwellenwerte	§ 28 Abs. 1, 2 und 4	(neue) BSI-Kritis-V

Wichtig:
Prüfung grundsätzlich auf Ebene der einzelnen Gesellschaften/juristischen Personen

Erfasste

Hersteller und Importeure nach Artikel 3 Nummern 9 und 11 der Verordnung (EG) Nr. 1907/2006 von chemischen Stoffen und Gemischen im Sinne des Artikels 3 Nummer 1 und 2 der genannten Verordnung, sofern diese in Kategorie 20 der Statistischen Systematik der Wirtschaftszweige in der Europäischen Gemeinschaft (NACE Rev. 2) fallen und der Registrierungspflicht nach Artikel 6 der genannten Verordnung unterliegen

Energie

sorgung & eseitigung

Digitale Infrastruktur

Herstellung von Datenverarbeitungs-geräten

Produktion, Herstellung und Handel mit chemischen Stoffen

Gesundheit

Produktion, Verarbeitung und Vertrieb von Lebens-mitteln

Verarbeitendes Gewerbe/Herstellung von Waren

Finanzwesen

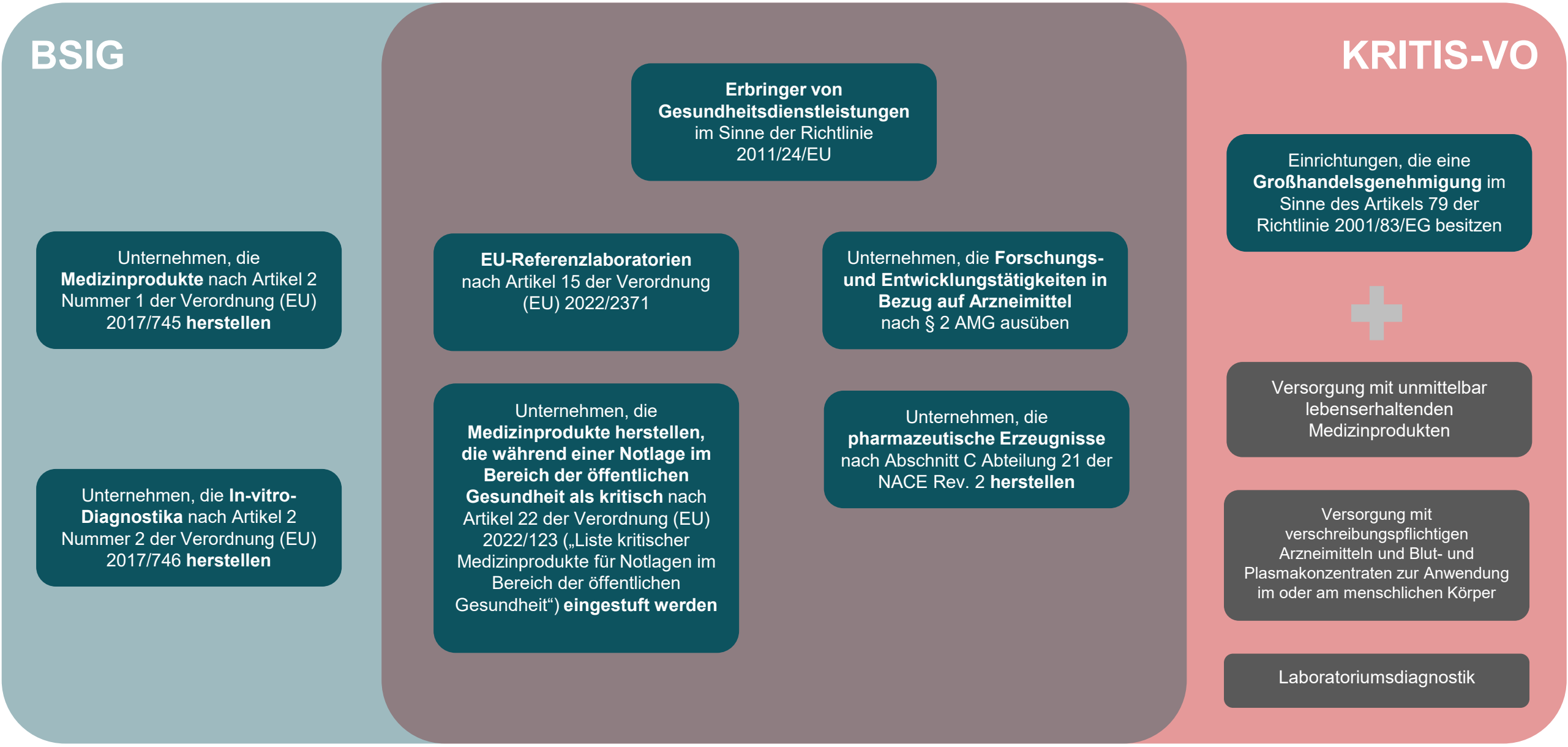
Anbieter digitaler Dienste

Weltraum

Post- & Kurierdienste

Abfall-bewirtschaftung

Forschung


BSIG
KRITIS-VO
Erbringer von Gesundheitsdienstleistungen im Sinne der Richtlinie 2011/24/EU
Unternehmen, die Medizinprodukte nach Artikel 2 Nummer 1 der Verordnung (EU) 2017/745 herstellen
EU-Referenzlaboratorien nach Artikel 15 der Verordnung (EU) 2022/2371
Unternehmen, die Forschungs- und Entwicklungstätigkeiten in Bezug auf Arzneimittel nach § 2 AMG ausüben
Unternehmen, die In-vitro-Diagnostika nach Artikel 2 Nummer 2 der Verordnung (EU) 2017/746 herstellen
Unternehmen, die Medizinprodukte herstellen, die während einer Notlage im Bereich der öffentlichen Gesundheit als kritisch nach Artikel 22 der Verordnung (EU) 2022/123 („Liste kritischer Medizinprodukte für Notlagen im Bereich der öffentlichen Gesundheit“) eingestuft werden
Unternehmen, die pharmazeutische Erzeugnisse nach Abschnitt C Abteilung 21 der NACE Rev. 2 herstellen
Einrichtungen, die eine Großhandelsgenehmigung im Sinne des Artikels 79 der Richtlinie 2001/83/EG besitzen
+
Versorgung mit unmittelbar lebenserhaltenden Medizinprodukten
Versorgung mit verschreibungspflichtigen Arzneimitteln und Blut- und Plasmakonzentraten zur Anwendung im oder am menschlichen Körper
Laboratoriumsdiagnostik

Erbringer von Gesundheitsdienstleistungen

Richtlinie 2011/24/EU

„**Gesundheitsversorgung**“ Gesundheitsdienstleistungen, die von Angehörigen der Gesundheitsberufe gegenüber Patienten erbracht werden, um deren Gesundheitszustand zu beurteilen, zu erhalten oder wiederherzustellen, einschließlich der Verschreibung, Abgabe und Bereitstellung von Arzneimitteln und Medizinprodukten;

„**Angehöriger der Gesundheitsberufe**“ ein[…] Arzt, eine Krankenschwester oder einen Krankenpfleger für allgemeine Pflege, ein[…] Zahnarzt, eine Hebamme oder einen Apotheker im Sinne der Richtlinie 2005/36/EG oder eine andere Fachkraft, die im Gesundheitsbereich Tätigkeiten ausübt, die einem reglementierten Beruf im Sinne von Artikel 3 Absatz 1 Buchstabe a der Richtlinie 2005/36/EG vorbehalten sind, oder eine Person, die nach den Rechtsvorschriften des Behandlungsmitgliedstaats als Angehöriger der Gesundheitsberufe gilt;

Richtlinie 2005/36/EG

a) „**reglementierter Beruf**“ ist eine berufliche Tätigkeit oder eine Gruppe beruflicher Tätigkeiten, bei der die Aufnahme oder Ausübung oder eine der Arten der Ausübung **direkt oder indirekt durch Rechts- und Verwaltungsvorschriften an den Besitz bestimmter Berufsqualifikationen gebunden ist**;

eine Art der Ausübung ist insbesondere die Führung einer Berufsbezeichnung, die durch Rechts- oder Verwaltungsvorschriften auf Personen beschränkt ist, die über eine bestimmte Berufsqualifikation verfügen.

Trifft Satz 1 dieser Begriffsbestimmung nicht zu, so wird ein unter Absatz 2 fallender Beruf als reglementierter Beruf behandelt;

(2) Einem reglementierten Beruf gleichgestellt ist ein Beruf, der von Mitgliedern von Verbänden oder Organisationen im Sinne des Anhangs I ausgeübt wird.

Die in Unterabsatz 1 genannten Verbände oder Organisationen verfolgen insbesondere das Ziel der Wahrung und Förderung eines hohen Niveaus in dem betreffenden Beruf. Zur Erreichung dieses Ziels werden sie von einem Mitgliedstaat in besonderer Form anerkannt; sie stellen ihren Mitgliedern einen Ausbildungsnachweis aus, gewähren, dass ihre Mitglieder die von ihnen vorgeschriebenen berufsständischen Regeln beachten und verleihen ihnen das Recht, einen Titel zu führen, eine bestimmte Kurzbezeichnung zu verwenden oder einen diesem Ausbildungsnachweis entsprechenden Status in Anspruch zu nehmen.

Erbringer von Gesundheitsdienstleistungen

2. Umfasst die Einrichtungsart "Erbringer von Gesundheitsdienstleistungen" auch den Vertrieb oder die Versorgung mit Medizinprodukten?

Anlage 1 Nr. 4.1.1 BSIG stellt ausdrücklich auf Gesundheitsdienstleister im Sinne des Artikel 3 Buchstabe g) der Richtlinie (EU) 2011/24 und damit auf Erbringer von Gesundheitsleistungen gegenüber Patienten ab. Die o.g. Richtlinie erfasst u.a. Gesundheitsdienstleistungen nach Artikel 3 Buchstabe a) der Richtlinie (EU) 2011/24, welche die Verschreibung, Abgabe und Bereitstellung von Medizinprodukten beinhalten, soweit diese Tätigkeiten von Angehörigen der Gesundheitsberufe im Rahmen der Patientenversorgung erfolgen.
Medizintechnikunternehmen i.S.d. o.g. Richtline erbringen i.d.R. keine Gesundheitsdienstleistungen gegenüber Patienten. Eine NIS-2-Betroffenheit von Medizintechnikunternehmen, welche Medizinprodukte in Deutschland vertreiben, könnte sich jedoch aus Anlage 1 Nr. 4.1.2. bis 4.1.5. BSIG oder aus Anlage 2 Nr. 5.1.1. BSIG ergeben.

Digitale Dienste

Managed (Security) Service Provider

Managed Service Provider = *"Anbieter von Diensten im Zusammenhang mit der Installation, der Verwaltung, dem Betrieb oder der Wartung von IKT-Produkten, -Netzen, -Infrastruktur, -Anwendungen oder jeglicher anderer Netz- und Informationssysteme durch Unterstützung oder aktive Verwaltung in den Räumlichkeiten der Kunden oder aus der Ferne"*

Das BSI fordert "*einen **gewissen Grad an tatsächlichem Zugriff** auf die betreffenden IKT-Produkte, -Netzwerke oder –Infrastrukturen*" (siehe FAQ 17 zum Anwendungsbereich)

Negativ abzugrenzen von

- bloßen Beratungstätigkeiten und
- bloßer geschäftlicher Verantwortung für Serviceerbringung.

Anbieter von Cloud-Computing-Diensten

Cloud-Computing-Dienst = "*digitaler Dienst, der auf Abruf die Verwaltung eines skalierbaren und elastischen Pools gemeinsam nutzbarer Rechenressourcen sowie den umfassenden Fernzugang zu diesem Pool ermöglicht, auch wenn die Rechenressourcen auf mehrere Standorte verteilt sind*"

Erfasst werden sämtliche Bereitstellungsmodelle (SaaS, IaaS, PaaS und NaaS, siehe Erwägungsgrund 33 der NIS2-Richtlinie)

Das BSI hält Auto-Skalierbarkeit (das Cloud-Kriterium nach NIST SP 800) nicht für eine konstitutive Voraussetzung für das Vorliegen eines Cloud-Computing-Dienstes unter NIS2 (siehe FAQ 6 zu digitaler Infrastruktur).

Reine Webhosting-Dienste qualifiziert das BSI nicht als Cloud-Computing-Dienste.

Anbieter von Rechenzentrumsdiensten

Rechenzentrumsdienst = "*Dienst, der Strukturen umfasst, die dem vorrangigen Zweck der zentralen Unterbringung, der Zusammenschaltung und dem Betrieb von IT- oder Netzwerkausrüstungen dienen, und die Datenverarbeitungsdienste erbringen, mitsamt allen benötigten Anlagen und Infrastrukturen, insbesondere für die Stromverteilung und die Umgebungskontrolle*"

Fungiert als Auffangtatbestand, sofern Cloud-Computing-Dienste-Begriff nicht greift (siehe Erwägungsgrund 35 der NIS2-Richtlinie)

Regelung zu vernachlässigbaren Geschäftstätigkeiten, § 28 Abs. 3 BSIG

Vernachlässigbare Geschäftstätigkeiten

(3) Bei der Zuordnung zu einer der Einrichtungsarten nach den Anlagen 1 und 2 können solche Geschäftstätigkeiten unberücksichtigt bleiben, die im Hinblick auf die gesamte Geschäftstätigkeit der Einrichtung vernachlässigbar sind.

Entscheidend:

Gesamtbild der betreffenden Geschäftstätigkeit im Lichte der Gesamtgeschäftstätigkeit der Einrichtung

Indizien

Anzahl der in diesem Bereich tätigen **Mitarbeiter**	Durch die Geschäftstätigkeit erwirtschafteter **Umsatz**
Bilanzsumme für diesen Bereich	Keine Nennung in **Gesellschaftervertrag, Satzung**, etc.

Schwellenwerte

Ausnahme in § 28 Abs. 4 Satz 2 BSIG

Die Daten von Partner- oder verbundenen Unternehmen im Sinne der Empfehlung der Kommission 2003/361/EG sind nicht hinzuzurechnen, wenn das Unternehmen unter Berücksichtigung der rechtlichen, wirtschaftlichen und tatsächlichen Umstände mit Blick auf die Beschaffenheit und den Betrieb der informationstechnischen Systeme, Komponenten und Prozesse unabhängig von seinen Partner- oder verbundenen Unternehmen ist.

Grundsatz: **Zurechnung** der Daten von Partner- und verbundenen Unternehmen

Wichtige Einrichtungen

- ≥ 50 Mitarbeiter

ODER

- > 10 Mio. EUR Jahresumsatz UND > 10 Mio. EUR Jahresbilanz

Besonders wichtige Einrichtungen

- ≥ 250 Mitarbeiter

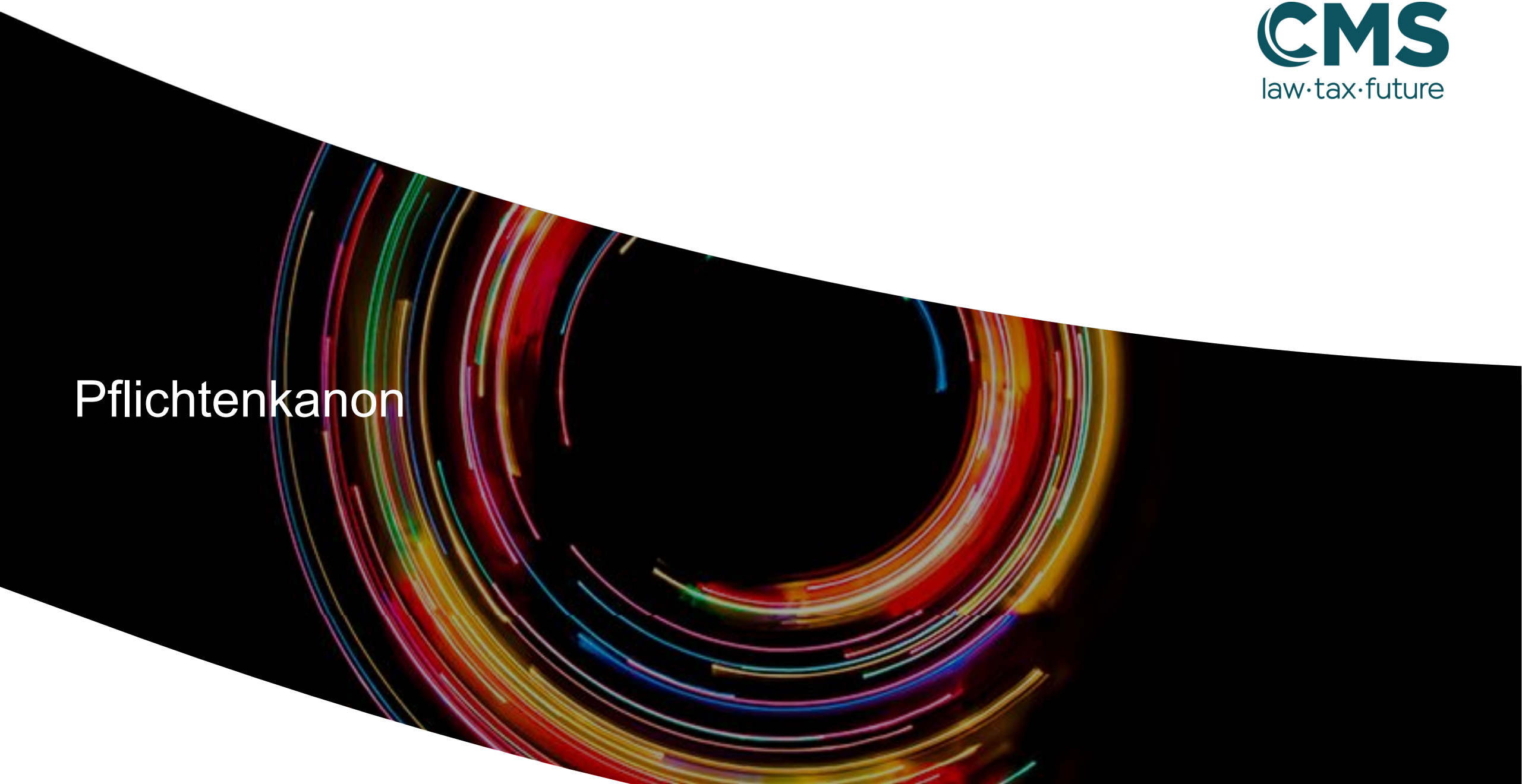
ODER

- > 50 Mio. EUR Jahresumsatz UND > 43 Mio. EUR Jahresbilanz

Betreiber kritischer Anlagen

- Versorgungsrelevanz → anlagenspezifische Schwellenwerte

Pflichtenkanon



Pflichtenkanon

Wichtig:

Die regulatorischen Pflichten greifen jeweils auf Entity-Ebene, gelten also für jede juristische Person, die in den Anwendungsbereich fällt, gesondert!

Geschäftsleitung

Umsetzung

Überwachung

Schadensersatzhaftung der Geschäftsleitung!

Schulung

Registrierung

Jede juristische Person, die in den Anwendungsbereich des BSIG-E fällt, muss sich bei der vom BSI und dem BBK eingerichteten Plattform registrieren

Cybersicherheits-bezogenes Risikomanagement

Geeignete, wirskame und verhältnismäßige
technische und organisatorische Maßnahmen
zur

- Vermeidung von Störungen der Verfügbarkeit, Integrität und Vertraulichkeit der informationstechnischen Systeme, Komponenten und Prozesse &
- Geringhaltung der Auswirkungen von Sicherheitsvorfällen

Meldung erheblicher Sicherheitsvorfälle

gegenüber

- Behörden
- Kunden/Nutzer

Erhöhte Bußgeldrisiken!

Pflichtenkanon

Pflichten (nicht abschließend)	**Wichtige Einrichtungen**	**Besonders wichtige Einrichtungen**	**Betreiber kritischer Anlagen**
Registrierung	X	X	X
Risikomanagement	X	X	X
Governance	X	X	X
Nachweise	(X)	(X)	X
Meldepflichten	X	X	X

Registrierung

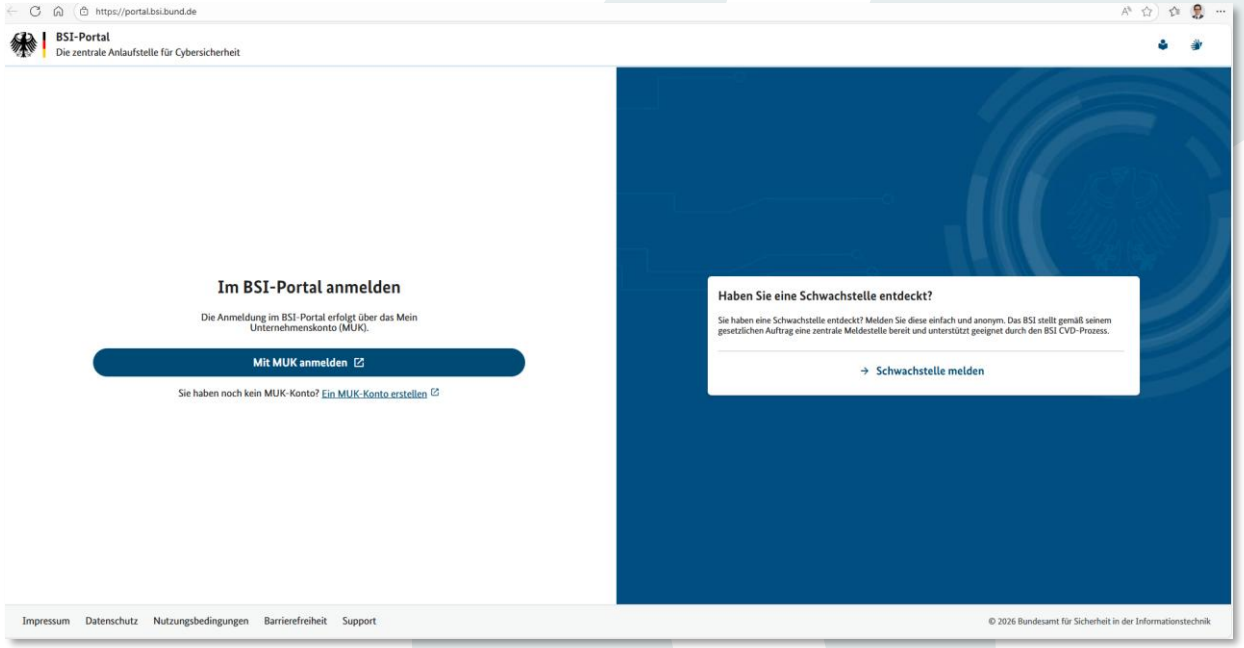
	Allgemeine Registrierungspflicht *§ 33 BSIG*	**Besondere Registrierungspflicht** *§ 34 BSIG*
Verpflichtungs-adressat	Wichtige Einrichtungen Besonders wichtige Einrichtungen Domain-Name-Registry-Diensteanbieter	Anbieter/Betreiber digitaler Infrastruktur *(mit wenigen Ausnahmen)* Anbieter digitaler Dienste Domain-Name-Registry-Diensteanbieter
Frist	**Drei Monate** ab Qualifikation als entsprechende Einrichtung	
Inhalt	– Name, Rechtsform und Handelsregisternummer – Anschrift – aktuelle Kontaktdaten (inkl. öffentl. IP-Adressbereiche) – Sektor und Branche – Mitgliedstaaten, in denen Dienste erbracht werden – Zuständige Aufsichtsbehörden **Zusätzliche Angaben von Betreibern kritischer Anlagen** ***(insb. 24/7-Kontaktstelle)***	– Name – Anschrift der Niederlassungen in der EU (bzw. des benannten Vertreters) – Aktuelle Kontaktdaten (inkl. öffentl. IP-Adressbereiche) – Sektor, Branche und Einrichtungsart – Mitgliedstaaten, in denen Dienste erbracht werden
Eingangs-tor	Bundesamt für Sicherheit in der Informationstechnik Gemeinsam eingerichtetes **Registrierungsportal** Bundesamt für Bevölkerungsschutz und Katastrophenhilfe	Bundesamt für Sicherheit in der Informationstechnik → enisa

Registrierung über das BSI-Portal

Schritt-für-Schritt-Anleitung unter
BSI - Anleitung zur Registrierung im BSI-Portal

Zweistufiges Registrierungsverfahren:

1) "Mein Unternehmenskonto"-Registrierung
2) Registrierung im BSI-Portal



Wichtig:

Die Registrierungsfrist endet

am **6. März 2026**!

Risikomanagement – gesetzliche Leitplanken

Technische und organisatorische Maßnahmen

zur

- Beherrschung von Risiken für die Sicherheit der Netz- und Informationssysteme, die für ihren Betrieb oder für die Erbringung der Dienste genutzt werden
- Minimierung der Auswirkungen von Sicherheitsvorfällen auf Dienste-Empfänger, andere Dienste zu verhindern oder möglichst gering zu halten

Gewährleistung eines Sicherheitsniveaus, das dem bestehenden Risiko angemessen ist

Einhaltung von
("soll")

- Stand der Technik
- einschlägige europäische und internationale Normen

Verhältnismäßigkeit

- Ausmaß der Risikoexposition
- Einrichtungstyp
- Größe der Einrichtung
- Eintrittswahrscheinlichkeit und Schwere von Sicherheitsvorfällen (einschl. gesellschaftlicher und wirtschaftlicher Auswirkungen)
- Kosten der Umsetzung

Erhöhte Anforderungen für **Betreiber kritischer Anlagen**

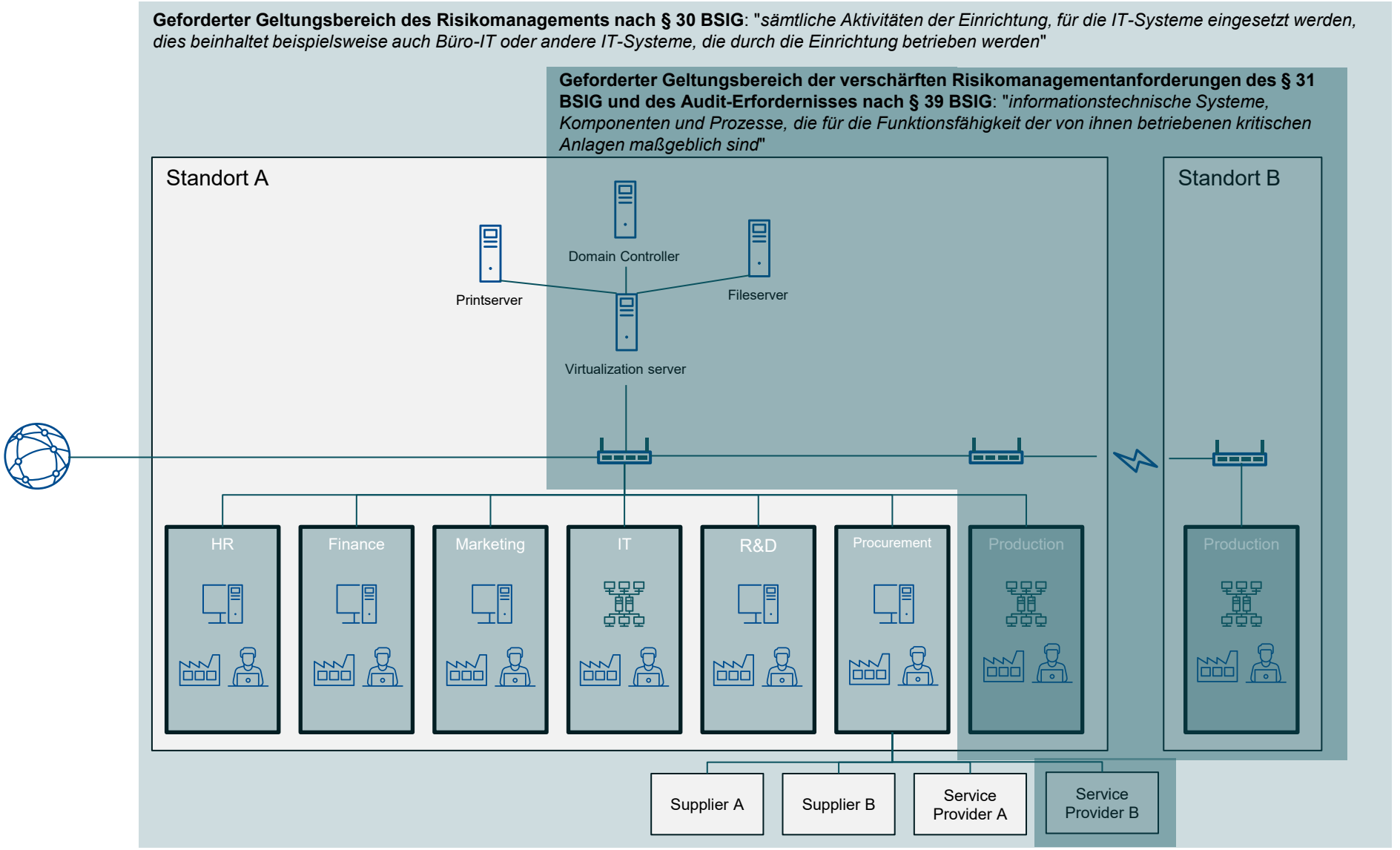
(insb. Pflicht zum Einsatz von Systemen zur Angriffs-erkennung)

Gefahrübergreifender Ansatz (auch genannt: All-Gefahren-Ansatz)
(Schutz der Netz- und Informationssysteme und der physischen Umwelt dieser Systeme vor Sicherheitsvorfällen)

Dokumentationspflicht!

Regelmäßige Nachweispflicht für **Betreiber kritischer Anlagen**

Geltungsbereich des geforderten Risikomanagements



#nis2know: NIS-2 Risikomanagementmaßnahmen

#nis2know

- Risikomanagementmaßnahmen – Warum?
- Was verlangt NIS-2?
- Was bedeutet „geeignet“, „wirksam“ und „verhältnismäßig“?
- Was bedeutet „Vertraulichkeit“, „Integrität“ und „Verfügbarkeit“?
- Was bedeutet „Auswirkungen von Sicherheitsvorfällen möglichst geringhalten“?
- Was ist sonst zu beachten?

Risikomanagement – Spezifizierung

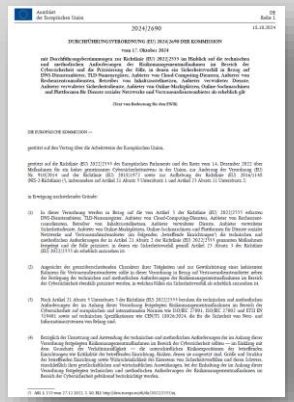
Umsetzung technischer und organisatorischer Maßnahmen

- Anbieter/Betreiber digitaler Infrastruktur (mit wenigen Ausnahmen)
- Anbieter digitaler Dienste
- Domain-Name-Registry-Diensteanbieter

- Wichtige Einrichtungen
- Besonders wichtige Einrichtungen

- Betreiber kritischer Anlagen

DurchführungsVO 2024/2690



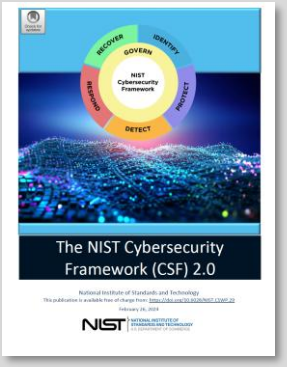
+

Mapping-Tabelle

ISO 27001:2022

IT-Grundschutz

NIST Cybersecurity Framework v2.0



B3S (Updates)

Geschäftsleitungspflichten und -haftung – Überblick

Geschäftsleitungen
müssen

Risikomanagementmaßnahmen "**umsetzen**"

Umsetzung der Risikomanagementmaßnahmen **überwachen**

Haftung der Geschäftsleitung
gegenüber der Einrichtung für schuldhafte Verletzung der Umsetzungs- und Überwachungspflichten

nach gesellschaftsrechtlichen Regeln

nach BSIG

Regelmäßige Teilnahme an Schulungen
um

Erkennung und Bewertung von Risiken und von **Risikomanagementpraktiken** im Bereich der Cybersicherheit

Beurteilung der Auswirkungen von Risiken sowie Risikomanagementpraktiken auf die von der Einrichtung erbrachten Dienste

Umsetzungsverantwortung der Geschäftsleitung

Übernahme der Gesamtverantwortung für das Thema Cybersicherheit

Initiierung, Steuerung und Kontrolle des Risikomanagementprozesses

1) Förmliche Genehmigung eines **Cybersicherheitskonzeptes**
2) Bereitstellung ausreichender **finanzieller und personeller Ressourcen**
3) Schaffung der erforderlichen **organisatorischen Rahmenbedingungen** einschl. Zuweisung und Kommunikation von Verantwortlichkeiten und Weisungsbefugnissen (mindestens eine Person muss gegenüber der Geschäftsleitung verantwortlich sein und regelmäßig über Cybersicherheitsstand berichten)
4) Sicherstellung der **Durchführung einer Risikoanalyse**
5) **Entscheidung über den Umgang mit identifizierten (Rest-)Risiken** (Letztverantwortung der Geschäftsleitung!)
6) **Überwachung der Umsetzung der Mitigierungsmaßnahmen**
7) Regelmäßige und anlassbezogene **Überprüfung, Bewertung und Aktualisierung** des Cybersicherheitskonzeptes und der Verantwortlichkeiten und Weisungsbefugnissen (anhand von Kennzahlen) und Korrektur von Schwachstellen

Schulung in Risikoanalyse und Risikomanagementpraktiken

Schulungspflicht der Geschäftsleitung

Adressaten: Geschäftsleitungen besonders wichtiger Einrichtungen und wichtiger Einrichtungen

Schulungszyklus: regelmäßig (risikoabhängig, nach Gesetzesbegründung: mindestens alle drei Jahre)

Schulungsinhalte

1) Grundlagen der NIS-2-Gesetzgebung
2) Risikoanalyse (Erkennung und Bewertung von Risiken)
3) Risikomanagementmaßnahmen
4) Auswirkungen von Risiken und Risikomanagementmaßnahmen
5) Ergänzende Inhalte (sektor- und einrichtungsspezifische Inhalte sowie Szenarien, Übungen und Case-Studies)

Risikomanagement – gesetzlicher Mindestkatalog

Mindestkomponenten

1. **Konzepte** in Bezug auf die **Risikoanalyse** und auf die **Sicherheit in der Informationstechnik**,
2. Bewältigung von **Sicherheitsvorfällen**,
3. **Aufrechterhaltung des Betriebs**, wie Backup-Management und Wiederherstellung nach einem Notfall, und Krisenmanagement,
4. **Sicherheit der Lieferkette** einschließlich sicherheitsbezogener Aspekte der Beziehungen zu unmittelbaren Anbietern oder Diensteanbietern,
5. Sicherheitsmaßnahmen bei **Erwerb, Entwicklung und Wartung von informationstechnischen Systemen**, Komponenten und Prozessen, einschließlich Management und Offenlegung von Schwachstellen,
6. Konzepte und Verfahren zur **Bewertung der Wirksamkeit von Risikomanagementmaßnahmen** im Bereich der Sicherheit in der Informationstechnik,
7. Grundlegende **Schulungen und Sensibilisierungsmaßnahmen** im Bereich der Sicherheit in der Informationstechnik,
8. Konzepte und Prozesse für den Einsatz von **kryptographischen Verfahren**,
9. Erstellung von Konzepten für die **Sicherheit des Personals**, die **Zugriffskontrolle** und für die Verwaltung von IKT-Systemen, -Produkten und -Prozessen,
10. Verwendung von Lösungen zur **Multi-Faktor-Authentifizierung** oder kontinuierlichen **Authentifizierung**, gesicherte Sprach-, Video- und Textkommunikation sowie gegebenenfalls gesicherte Notfallkommunikationssysteme innerhalb der Einrichtung.

Risikomanagementanforderungen "in a nutshell"

Holistischer und systematischer Ansatz

Die NIS-2-Richtlinie verpflichtet die betroffenen Unternehmen, **alle denkbaren Risiken zu beherrschen**, die für die Sicherheit **aller von ihnen genutzten Netz- und Informationssysteme** bestehen.

Dies erfordert eine umfassende und systematische **Identifizierung aller relevanter Assets**, eine **Bewertung aller denkbarer Risiken** in Bezug auf diese Assets sowie die **Umsetzung und Überwachung** angemessener **Risikominderungsmaßnahmen**.

Wirkbereich weit jenseits der IT-Abteilung

Die NIS-2-Richtlinie definiert einen Katalog von Mindestmaßnahmen zum Risikomanagement, die von den betroffenen Unternehmen zu ergreifen sind.

Dieser Katalog umfasst neben Risikoanalysekonzepten, Anforderungen an Incident Handling und Business Continuity Management auch die **Sicherheit der Lieferkette**, **physisches Anlagenmanagement** sowie **personalbezogene Sicherheitsaspekte**.

Die Wirksamkeit bestehender Maßnahmen muss **fortlaufend überprüft** und **erforderliche Anpassungen** vorgenommen werden (sog. PDCA-Zyklus).

1. Konzepte in Bezug auf die Risikoanalyse und auf die Sicherheit in der Informationstechnik

Übergreifendes Konzept für Sicherheit von Netz- und Informationssystemen

- Ausarbeitung eines übergreifenden Konzeptes einschließlich eines Risikomanagementrahmens
- Definition von Rollen und Verantwortlichkeiten (unterVermeidung von Interessenskonflikten)
- Förmliche Genehmigung durch Leitungsebene

Risikoanalyse

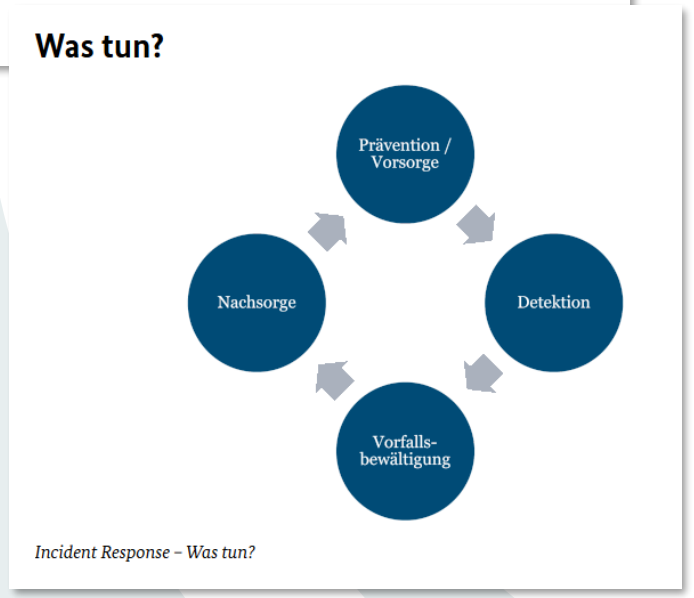
- Systematische Identifikation und Bewertung von Risiken
- Orientierung an bestehenden Standards (z.B. BSI-Standard 200-3) empfohlen

2. Bewältigung von Sicherheitsvorfällen

Konzept für Bewältigung von Sicherheitsvorfällen

- Kategorisierungssystem für Sicherheitsvorfälle
- Kommunikationspläne für Eskalation und Meldung
- Zuweisung von Rollen
- Erforderliche Dokumente und Vorlagen (Anleitungen, Eskalationsschemata, Kontaktlisten, etc.)
- Überprüfungen nach Sicherheitsvorfällen

Auch: Überwachungs- und Protokollierungsanforderungen



3. BCM, Backup-Management und Wiederherstellung nach einem Notfall sowie Krisenmanagement

- Notfallplan für Aufrechterhaltung und Wiederherstellung des Betriebs
- Backup-Sicherungs- und Redundanzmanagement
- Krisenmanagement

Auch: Physische Sicherheit!

4. Sicherheit der Lieferkette

Konzept für Sicherheit der Lieferkette

- Definition von Kriterien für Auswahl von Anbietern
- Risikobewertung von Anbietern/Zulieferern
- Vertragliche Vorsehung von Cybersicherheitsanforderungen

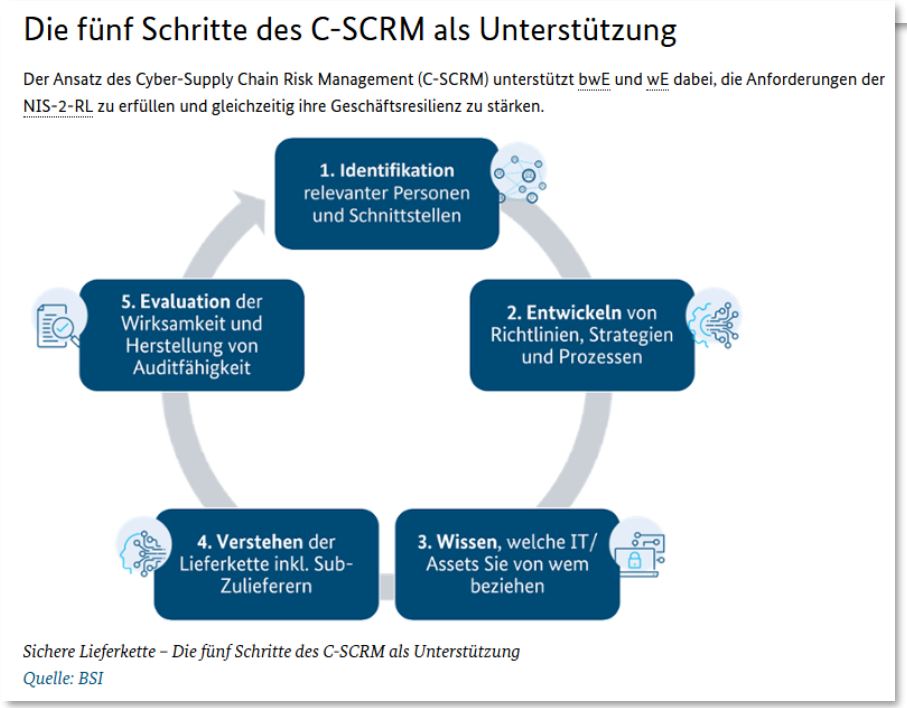
#nis2know
Sichere Lieferkette

Ein wesentliches Merkmal unserer weltweit digital vernetzten Wirtschaft ist die Abhängigkeit von Lieferketten.

#nis2know

Mit der zunehmenden Digitalisierung von Lieferketten steigt die Gefahr durch Cyberangriffe. Das BSI-Gesetz fordert daher von besonders wichtigen (bwE) und wichtigen Einrichtungen (wE), die Sicherheit ihrer Lieferkette zu gewährleisten.

- Sichere Lieferkette – Warum?
- Wer ist wie betroffen?
- Was ist zu beachten?
- Die fünf Schritte des C-SCRM als Unterstützung
- Was tun?
- Welche Standards gibt es bereits?
- Wie unterstützt das BSI?



Die fünf Schritte des C-SCRM als Unterstützung

Der Ansatz des Cyber-Supply Chain Risk Management (C-SCRM) unterstützt bwE und wE dabei, die Anforderungen der NIS-2-RL zu erfüllen und gleichzeitig ihre Geschäftsresilienz zu stärken.

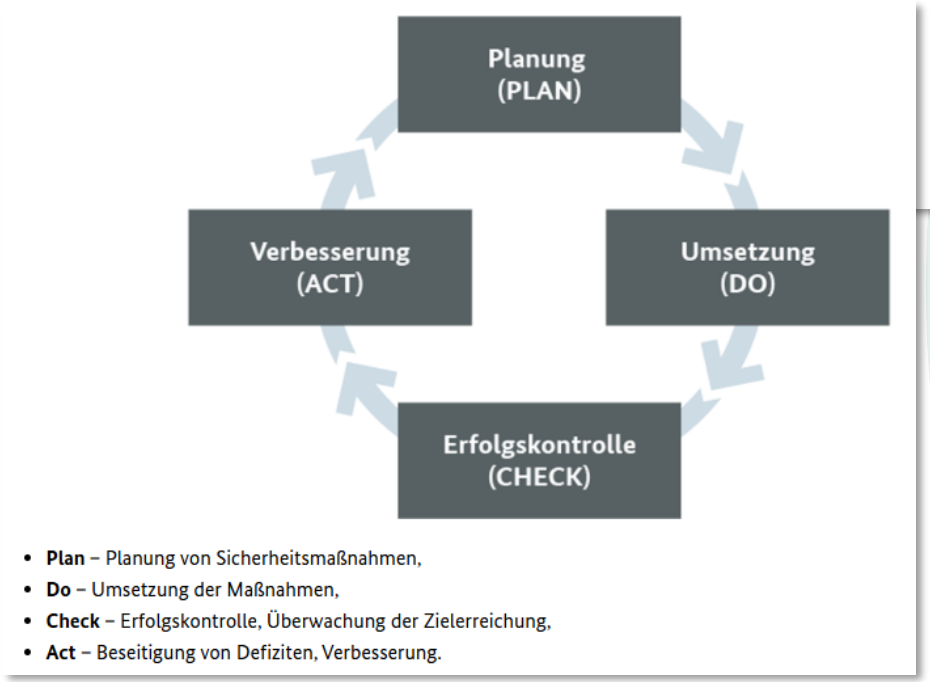
Sichere Lieferkette – Die fünf Schritte des C-SCRM als Unterstützung
Quelle: BSI

5. Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von informationstechnischen Systemen, Komponenten und Prozessen, einschließlich Management und Offenlegung von Schwachstellen

- Sicherheitsmaßnahmen beim Erwerb von IKT-Diensten oder IKT-Produkten
- Sicherer Entwicklungszyklus
- Konfigurationsmanagement
- Änderungsmanagement, Reparatur und Wartung
- Sicherheitsprüfung
- Sicherheitspatch-Management
- Netzsicherheit
- Netzsegmentierung
- Schutz gegen Schadsoftware und nicht genehmigte Software
- Behandlung und Offenlegung von Schwachstellen

6. Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen im Bereich der Sicherheit in der Informationstechnik

- Messbarkeit herstellen
- Regelmäßige Überprüfungen (Audits und Revisionen)
- Management-Berichte und Bewertungen
- Kontinuierlicher Verbesserungsprozess



7. Grundlegende Schulungen und Sensibilisierungsmaßnahmen im Bereich der Sicherheit in der Informationstechnik

- Sensibilisierungsmaßnahmen
- Sicherheitsschulungen

Dokumentationspflicht!

Anforderungskatalog – Delegierte Verordnung 2024/2690

Cyberhygiene und Schulungen (Ziffer 8)

Einrichtungen im Anwendungsbereich von NIS2 stellen sicher, dass Mitarbeitende (einschließlich der Mitglieder der Leitungsorgane, sowie direkte Anbieter und Diensteanbieter)

- sich der **Cybersicherheitsrisiken bewusst sind**,
- über die **Bedeutung der Cybersicherheit informiert werden** und
- **Verfahren im Bereich der Cyberhygiene anwenden**.

1 Sensibilisierungsmaßnahmen

- Zeitliche Planung dergestalt, dass die Maßnahmen **wiederholt** werden und neue Mitarbeitende erreichen
- **Einklang mit Sicherheitskonzept**, themenspezifischen Konzepten und einschlägigen Verfahren
- **Abdeckung einschlägiger Cyberbedrohungen**, bestehender Risikomanagementmaßnahmen im Bereich der Cybersicherheit, Kontaktstellen und Ressourcen für zusätzliche Informationen und Beratung zu Cybersicherheitsfragen sowie Verfahren im Bereich der Cyberhygiene für Nutzer
- **Regelmäßige Tests** des Sensibilisierungsprogramms auf seine **Wirksamkeit**
- **Regelmäßige Aktualisierung** des Sensibilisierungsprogramms (Anpassung an Bedrohungslage und Risiken)

2 Sicherheitsschulungen

- **Regelmäßige Schulung** von Mitarbeitenden, deren **Rollen** sicherheitsrelevante Fähigkeiten und Fachkenntnisse erfordern (auch bei Rollenwechsel!)
- **Festlegung des Schulungsbedarfs** für bestimmte Rollen und Positionen auf der Grundlage von klar definierten Kriterien
- Relevanz der Schulung für die Funktion des Mitarbeitenden
- Mindestinhalte:
  - Anweisungen für die **sichere Konfiguration** und den **sicheren Betrieb** der Netz- und Informationssysteme, einschließlich mobiler Geräte
  - Unterrichtung über **bekannte Cyberbedrohungen**
  - **Verhalten bei sicherheitsrelevanten Ereignissen**
- **Bewertung der Wirksamkeit** der Schulung
- **Regelmäßige Aktualisierung** des Programms, wobei geltende Konzepte und Vorschriften, zugewiesene Rollen und Verantwortlichkeiten sowie bekannte Cyberbedrohungen und technische Entwicklungen berücksichtigt werden.

ENISA-Guidance

Regelmäßiges Angebot und Update

Sensibilisierungsmaßnahmen und Cyberhygiene

Implementierungsleitlinien

- Implementierung eines **Programms zur Sensibilisierung für Cybersicherheit**
- Nutzung **verschiedener Formate** (wie Workshops, Webinare und E-Learning-Module) und **verschiedener Kommunikationskanäle** (E-Mails, Newsletter, Intranet), um Mitarbeiter über die aktuellen Entwicklungen im Bereich Cybersicherheit, Risiken und Cyberhygiene-Praktiken auf dem Laufenden zu halten

Cyberhygiene-Praktiken (indikativ)

- Clear-Desk-Policy
- Einsatz starker Authentifizierungsverfahren (inkl. Multi-Faktor)
- Vorfall-Reporting
- Sichere E-Mail-Nutzung und sicheres Surfen im Internet
- Schutz vor Phishing und Social Engineering
- Sichere Nutzung mobiler Geräte und vernetzter Fahrzeuge der Einrichtung
- Sichere Verbindungs-Praktiken (z.B. VPN)
- Backup-Maßnahmen
- Zero-Trust-Konzept
- Software-Updates
- Sichere Gerätekonfiguration
- Netzwerksegmentierung
- Sichere Telearbeits- und Home-Office-Praktiken

Inhalte des Sensibilisierungsprogramms (indikativ):

- Richtlinie zur Sicherheit von Netz- und Informationssystemen
- Erkennung von Social-Engineering-Angriffen wie Phishing, Pretexting und Tailgating
- Sensibilisierung für Ursachen unbeabsichtigter Datenoffenlegung
- Gefahren der Verbindung mit und der Übertragung von Daten über unsichere Netzwerke, einschließlich Vorgaben, um sicherzustellen, dass alle Benutzer ihre Heimnetzwerkinfrastruktur sicher konfigurieren.
- Umgang mit und Risiken von bösartiger und nicht autorisierter Software

+ Angebot von Anlaufstellen und Ressourcen für zusätzliche Beratung

+ Nutzung verfügbarer Guidance von nationaler und internationaler Cybersicherheitsorganisationen, (z.B. ENISA's **AR-in-a-Box** und Inhalte der **Cyber Skills Academy**)

Nachweise (exemplarisch)

- **Umfassende Übersicht über das Sensibilisierungsprogramm** mit detaillierten Angaben zu Zielen, Inhalten, Häufigkeit, Lehr- und Zeitplan
- **Kopien der an die Mitarbeiter verteilten Sensibilisierungsmaterialien**, einschließlich Handouts, E-Mails, Präsentationen und Online-Module
- **Protokolle, Anwesenheitslisten, Abschlusszertifikate oder Bestätigungen**, die den Mitarbeitern nach Abschluss des Programms ausgehändigt wurden und aus denen hervorgeht, welche Mitarbeiter an dem Sensibilisierungsprogramm eilgenommen haben.

ENISA-Guidance

Regelmäßige Durchführung und
mindestens jährliche Überprüfung und Aktualisierung

Sicherheitsschulungen

Implementierungsleitlinien

- Bewerten Sie, **welche Aufgaben** innerhalb der Einrichtung **sicherheitsrelevante Fähigkeiten und Fachkenntnisse** erfordern.
- Bieten Sie Schulungen an, die sich **auf die spezifischen Sicherheitsfähigkeiten konzentrieren**, die für die identifizierten Aufgaben erforderlich sind.
- Berücksichtigen Sie weltweit anerkannte Qualifikationen und Zertifizierungen sowie das European Cybersecurity Skills Framework (ECSF).
- Bieten Sie **rollenspezifische Schulungen zur Netz- und Informationssicherheit** an.
- Greifen Sie auf **verschiedene Formate**, wie Online-Kurse, Workshops, praktische Übungen und Simulationen zurück.
- Nutzen Sie **verschiedene Arten** von Schulungen, wie z. B. Kurse, Zertifizierungen oder die Teilnahme an Sicherheitskonferenzen oder Webinaren, sowie die Aufrechterhaltung von Zertifizierungen.
- **Beispiele für Schulungen** sind: Kurse zur sicheren Systemadministration für IT-Fachleute, Open Worldwide Application Security Project®-Schulungen zur Sensibilisierung und Prävention für Entwickler von Webanwendungen und fortgeschrittene Schulungen zur Sensibilisierung für Social Engineering für hochrangige Positionen.
- Das Schulungsprogramm kann unter anderem folgende **Themen** umfassen (indikative, nicht erschöpfende Liste):
  - Bewährte **Verfahren zur Authentifizierung**, wie z. B. MFA, Passwort-Erstellung und Verwaltung von Anmeldedaten
  - Identifikation und ordnungsgemäße Speicherung, Übertragung, Archivierung und Vernichtung **sensibler Daten**
  - Erkennung potenzieller Vorfälle wie ungewöhnlicher E-Mail-Anhänge, unerwartetes Systemverhalten und verdächtiger Netzwerkverkehr
  - Umgehende und genaue **Meldung von Ereignissen**, einschließlich der Nutzung dafür vorgesehener Kommunikationskanäle.
  - Überprüfung und Meldung veralteter Software oder Fehler in automatisierten Prozessen und Tools (inklusive Benachrichtigung des IT-Personals über Fehler in automatisierten Prozessen und Tools)
  - **Krisenmanagement** und Verfahren zur Aufrechterhaltung des Geschäftsbetriebs (einschließlich simulierter Krisensituationen).
  - Für Systemadministratoren und Softwareentwickler: **Sichere Konfiguration** und **sicherer Betrieb** des Netzwerks und der Informationssysteme
  - Regelmäßige Informationen über die **neuesten Cyber-Bedrohungen**
- **Regelmäßige Tests** der Sicherheitskenntnisse der Mitarbeiter, um sicherzustellen, dass diese ausreichend und auf dem neuesten Stand sind.
- Im Fall eines **Rollen-/Funktionswechsels**: Prüfen Sie, ob die neue Position oder Funktion eines Mitarbeiters eine rollenspezifische Schulung zur Netzwerk- und Informationssicherheit erfordert.

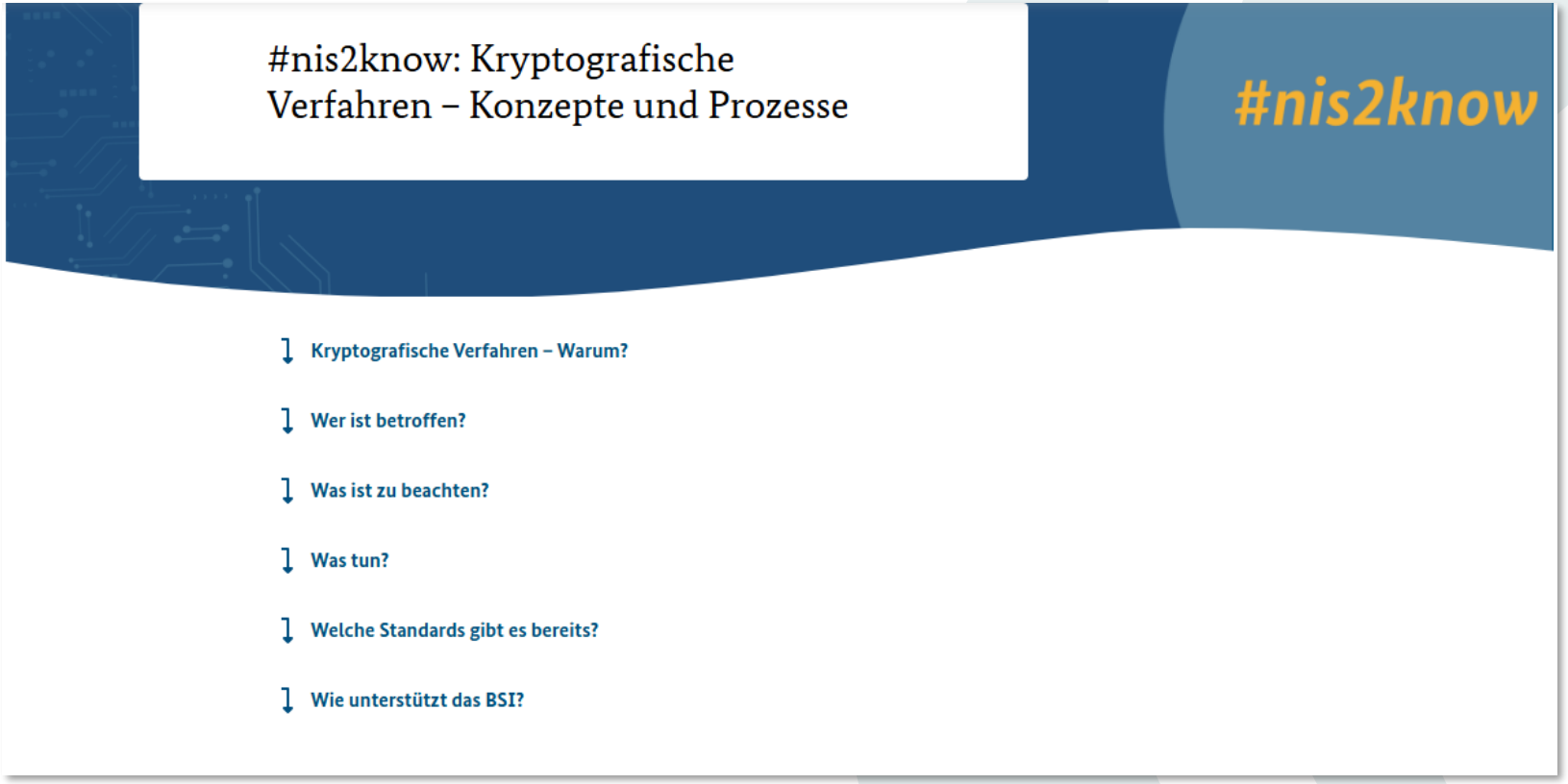
Nachweise (exemplarisch)

- Umfassende **Übersicht über das Schulungsprogramm** mit detaillierten Angaben zu den Zielen für verschiedene Funktionen/Rollen und deren Erreichung sowie zu den Inhalten und der Häufigkeit der Schulungen
- **Beurteilung der Wirkung** und Rückmeldungen zu den Schulungen
- **Ergebnisse von Tests oder Bewertungen**, die durchgeführt wurden, um das Verständnis der Mitarbeiter für die behandelten Themen zu messen
- Nachweis über die Aufrechterhaltung der erworbenen Zertifizierungen
- **Protokolle, Anwesenheitslisten, Abschlusszertifikate oder Bestätigungen**, die den Mitarbeitern nach Abschluss der Schulung ausgehändigt werden und aus denen hervorgeht, welche Mitarbeiter an den Schulungen teilgenommen haben
- An Mitarbeiter **verteilte Informationsmaterialien**, darunter Handouts, Präsentationen und Online-Module.
- **Aktualisierungen**, die zeigen, dass das Schulungsprogramm regelmäßig überprüft und aktualisiert wird, um mit den neuesten Cybersicherheitsbedrohungen und Best Practices Schritt zu halten
- **Feedback-Formulare** für Mitarbeiter zu den Schulungen, die Aufschluss über die Wirksamkeit der Schulungen und über Verbesserungsmöglichkeiten geben können

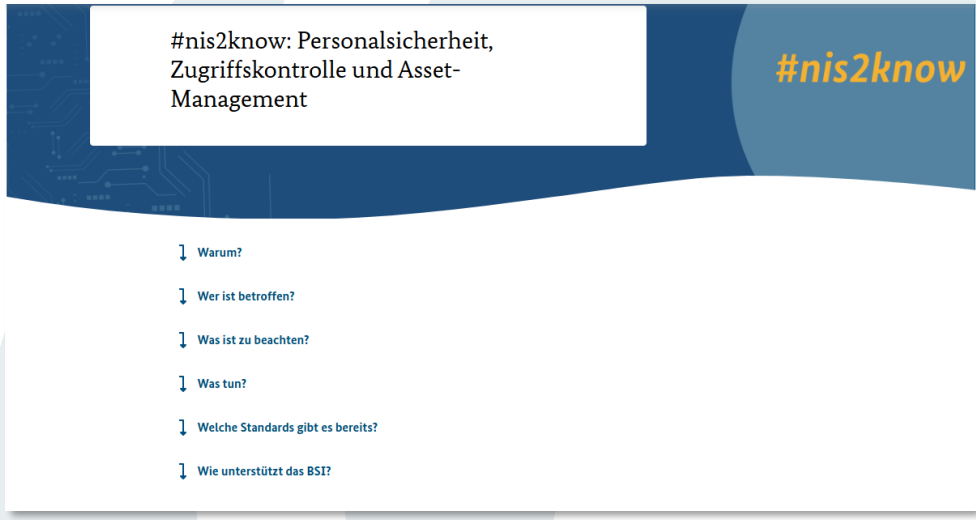
CMS

8. Konzepte und Prozesse für den Einsatz von kryptographischen Verfahren

- Inventarisieren
- Bewerten
- Verfahren umsetzen



9. Konzepte für die Sicherheit des Personals, die Zugriffskontrolle und für die Verwaltung von IKT-Systemen, -Produkten und -Prozessen

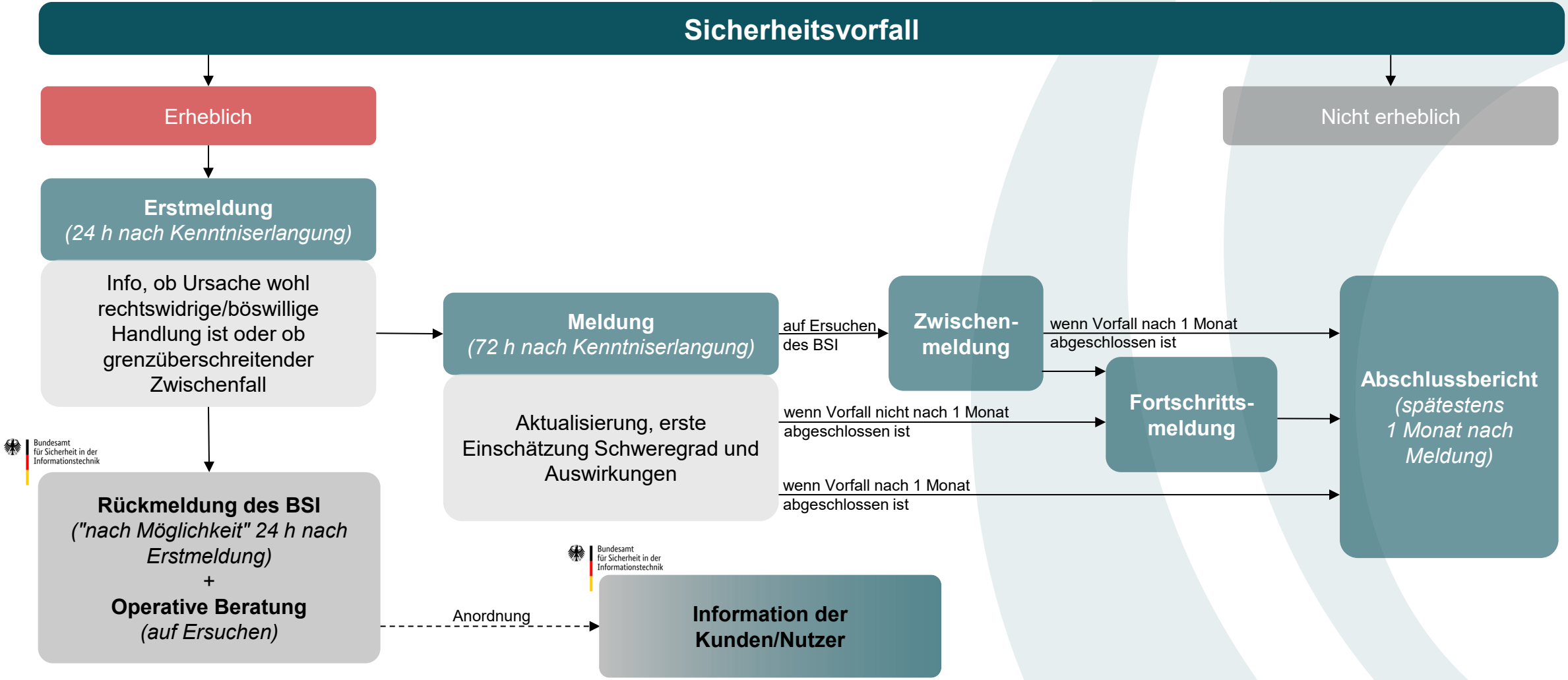


- Sicherheit des Personals
  - Zuverlässigkeitsüberprüfungen
  - Verfahren zur Beendigung oder Änderung des Beschäftigungsverhältnisses
  - Disziplinarverfahren
- Zugriffskontrolle
  - Konzepte für die Zugriffskontrolle
  - Management von Zugangs- und Zugriffsrechten
  - Privilegierte Konten und Systemverwaltungskonten
  - Systemverwaltungssysteme
  - Identifizierung
  - Authentifizierung (einschl. Multifaktor-Authentifizierung)

- Verwaltung von IKT-Systemen, -Produkten und –Prozessen
  - Anlagen- und Werteklassifizierung (inkl. Klassifizierungsstufen)
  - Behandlung von Anlagen und Werten
  - Konzept für Wechseldatenträger
  - Anlagen- und Werteinventar
  - Abgabe, Rückgabe oder Löschung von Anlagen und Werten bei Beendigung des Beschäftigungsverhältnisses

10. Lösungen zur Multi-Faktor-Authentifizierung oder kontinuierlichen Authentifizierung, gesicherte Sprach-, Video- und Textkommunikation sowie gegebenenfalls gesicherte Notfallkommunikationssysteme innerhalb der Einrichtung

Meldung erheblicher Sicherheitsvorfälle



Erheblichkeit nach DurchführungsVO 2024/2690

„erheblicher Sicherheitsvorfall“ ein Sicherheitsvorfall, der
- schwerwiegende Betriebsstörungen der Dienste oder finanzielle Verluste für die betreffende Einrichtung verursacht hat oder verursachen kann oder
- andere natürliche oder juristische Personen durch erhebliche materielle oder immaterielle Schäden beeinträchtigt hat oder beeinträchtigen kann,

sofern durch die Rechtsverordnung nach § 56 Absatz 5 keine konkretisierende Begriffsbestimmung erfolgt;

Erheblichkeitsschwellen

Eingetretener oder möglicher **direkter finanzieller Verlust i.H.v. mehr als EUR 500.000,- oder 5 % des Jahresumsatzes** im vorangegangenen Geschäftsjahr (je nachdem, welcher Wert niedriger ist)

Verursachung oder Möglichkeit der Verursachung eines **Abflusses von Geschäftsgeheimnissen**

Verursachung oder Möglichkeit der Verursachung des **Todes einer natürlichen Person**

Verursachung oder Möglichkeit der Verursachung einer **schweren Schädigung der Gesundheit einer natürlichen Person**

Erfolgreicher, mutmaßlich **böswilliger und unbefugter Zugriff auf Netz- und Informationssysteme**, der geeignet ist, **schwerwiegende Betriebsstörungen** zu verursachen

Planmäßige Betriebsunterbrechungen und **geplante Folgen planmäßiger Wartungsarbeiten**, die von oder im Auftrag der betreffenden Einrichtung durchgeführt werden

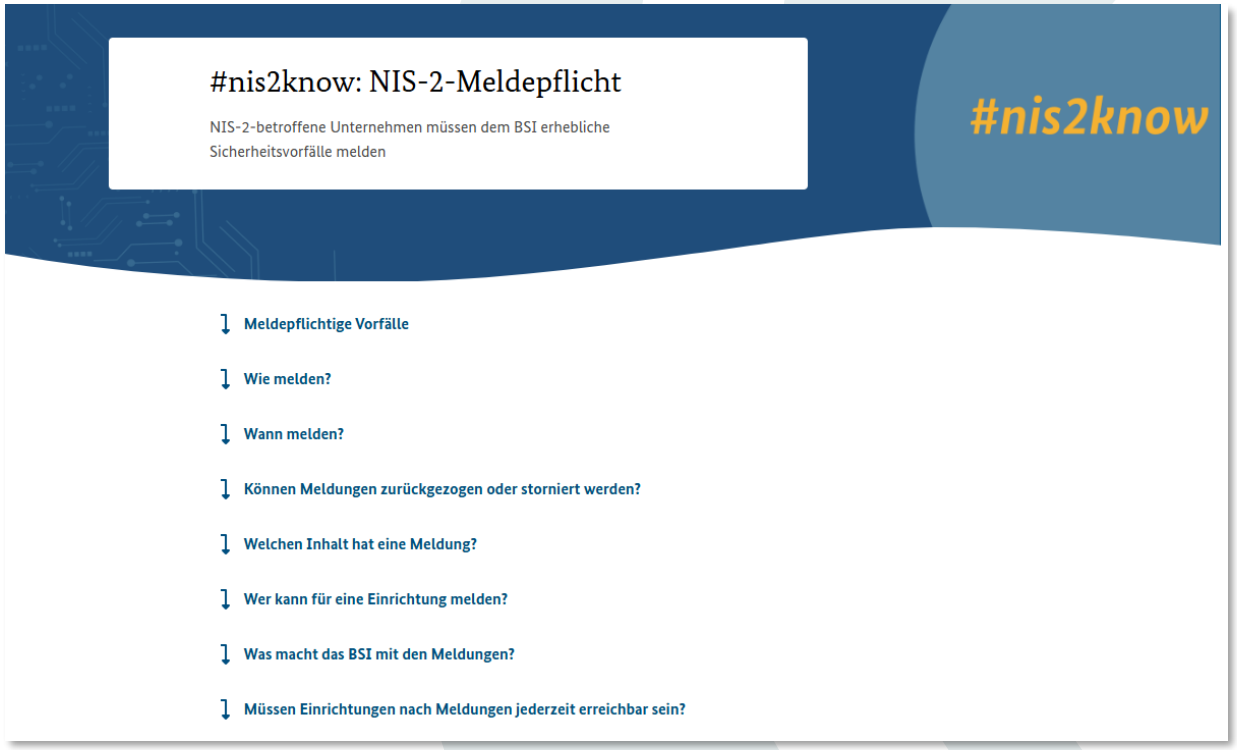
Wiederholte Sicherheitsvorfälle

Sicherheitsvorfälle, die einzeln betrachtet die links skizzierten Erheblichkeitsschwellen nicht überschreiten, gelten zusammen als ein erheblicher Sicherheitsvorfall, wenn sie **alle** folgenden Kriterien erfüllen:

1. Mind. zweimaliges Auftreten innerhalb von sechs Monaten
2. Dieselbe offensichtliche Ursache
3. Der eingetretene oder mögliche direkte finanzielle Verlust beträgt zusammengenommen mehr als EUR 500.000,- oder 5 % des Jahresumsatzes im vorangegangenen Geschäftsjahr (je nachdem, welcher Wert niedriger ist)

Meldekanäle und #nis2know des BSI

	BSI-Portal	Melde- und Informationsportal (MIP)
wE/ bwE, noch nicht registriert		X
wE/ bwE, bereits registriert	X	
KRITIS-Betreiber		X



Q&A