CONCEPTURE
GRUPPE | IHR ERFOLG. GESICHERT

VORTRAG

KRITIS-Dachgesetz, NIS2 und CRA
27.02.2025

AGENDA

1 VORSTELLUNG

2 GESETZLICHE RAHMENBEDINGUNGEN

3 KRITIS-DACHGESETZ

4 NIS 2

5 CYBER RESILIENCE ACT

AGENDA

1 VORSTELLUNG

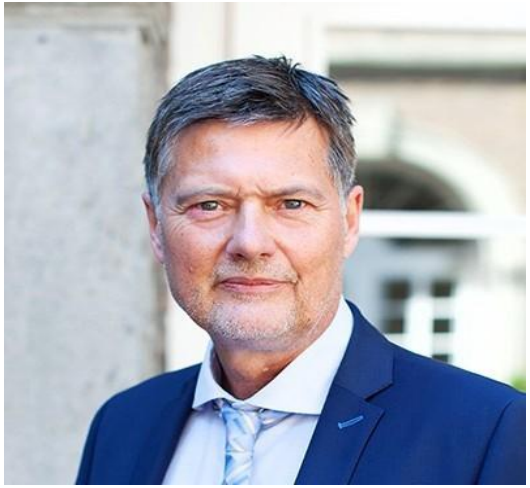
2 GESETZLICHE RAHMENBEDINGUNGEN

3 KRITIS-DACHGESETZ

4 NIS 2

5 CYBER RESILIENCE ACT

IHR REFERENT



Holger Berens

- 35 Jahre Erfahrung im Compliance und Sicherheitsmanagements
- Managing Partner bei Concepture
- Vorstandsvorsitzender des Bundesverbandes für den Schutz kritischer Infrastrukturen (BSKI)
- externer CISO von mehreren internationalen Konzernen für den EMEA-Bereich
- externer IKT-Beauftragter
- Autor von Fachbüchern sowie gefragter Experte der Medien im Bereich Compliance und Security.

BSKI
Bundesverband für den Schutz Kritischer Infrastrukturen e. V.

Satzungszweck

- Der Bundesverband für den Schutz Kritischer Infrastrukturen (BSKI) ist die zentrale Anlaufstelle für Entscheider aus Kritischen Infrastrukturen, um ganzheitliche Schutzkonzepte zu etablieren.
- Die Aufgabe des Bundesverbandes für den Schutz Kritischer Infrastrukturen ist es, Sicherheitsrisiken für kritische Infrastrukturen und deren Zulieferer frühzeitig zu er-kennen und durch gezielte Konzepte für Prävention, Reaktion und Postvention zu reduzieren. Dabei werden allerhöchste Schutzziele (technisch, organisatorisch, persönlich) für kritische Infrastrukturen verfolgt.

mehr Informationen unter:

AGENDA

1 VORSTELLUNG

2 GESETZLICHE RAHMENBEDINGUNGEN

3 KRITIS-DACHGESETZ

4 NIS 2

5 CYBER RESILIENCE ACT

IT-Sicherheitsgesetz 1.0 Änderungsgesetz zum BSIG, EnWG, TKG, AtG und TMG: Verpflichtet Betreiber Kritischer Infrastrukturen IT angemessen abzusichern und diese Sicherheit überprüfen zu lassen.

Neue Rechtssetzung durch die EU

NIS 2 & RCE (Resilience of Critical Entities) (Umsetzung bis 17. Oktober 2024)

Neue Sektoren: z. B. öffentliche Verwaltung, Weltraum, ForschungseinrichtungenEinführung „size-cap rule"

DORA (Digital Operational Resilience Act) VO und RL (Anwendung / Umsetzung bis 17.1.2025)

BSI-Kritisverordnung
Definition Sektoren:
Schwellenwerte (Bedeutung des Versorgungsgrads)

Umsetzungsfristen

2015

2016

2017

Umsetzungsgesetz NIS 1
Neu: Regelungen für Anbieter Digitaler Dienste

2021

2022/23

IT-Sicherheitsgesetz 2.0
Einsatz von Systemen zur Angriffserkennung (§ 8a Abs. 1a)
Neuer Sektor – Siedlungsabfallentsorgung, Selbsterklärung zur IT-Sicherheit Unternehmen im besonderen öffentlichen Interesse (§ 8f)

2024

2025

2025/26

jetzt

Inkrafttreten
BISG 3.0
KRITIS-Dachgesetz

Der Cyber Resilience Act („CRA")

wurde am 20.11.2024 im Amtsblatt veröffentlicht und tritt am 09.12.2024 in Kraft.

GESETZLICHE RAHMENBEDINGUNGEN

Es gibt zwei sogenannte EU-Richtlinien, die in nationales Recht umgesetzt werden müssen:

EU-Richtlinie über die Resilienz kritischer Einrichtungen (CER-Richtlinie)

Die CER-Richtlinie verpflichtet die Mitgliedstaaten, kritische Einrichtungen zu identifizieren und deren physische Widerstandsfähigkeit gegenüber Bedrohungen wie *Naturgefahren*, *Terroranschläge* oder *Sabotage* zu stärken.

EU-Richtlinie für ein hohes gemeinsames Cybersicherheitsniveau in der Union (NIS-2-Richtlinie)

Die NIS2-Richtlinie verpflichtet die Unternehmen, die in den Anwendungsbereich fallen, IT-, Cyber- und Informationssicherheit einzuführen.

Die Richtlinie ist für jeden Mitgliedstaat, an den sie gerichtet wird, hinsichtlich des zu erreichenden Ziels verbindlich, überlässt jedoch den innerstaatlichen Stellen die Wahl der Form und der Mittel.

GESETZLICHE RAHMENBEDINGUNGEN

EU Richtlinien müssen in den Mitgliedstaaten in nationales Recht umgesetzt werden.

Die Umsetzungsfrist für NIS2 und CER war der 17.10.2024.

In Deutschland sind das für:

NIS2 › BSIG 3.0/ITSiG 3.0

CER › KRITIS-Dachgesetz

Die EU Kommission hat ein Vertragsverletzungsverfahren gegen Deutschland eingeleitet, da diese Richtlinien nicht fristgerecht umgesetzt wurden.

GESETZLICHE RAHMENBEDINGUNGEN

Wegen der Neuwahlen im Februar ist nicht damit zu rechnen, dass noch im 1. Quartal 2025 die Umsetzungsgesetze in Kraft treten.

Ein genaues Datum kann nicht prognostiziert werden.

Die wesentlichen Anforderungen stehen mit den jeweiligen Entwürfen jedoch fest.

Das bedeutet, dass die Unternehmen, die in den Anwendungsbereich fallen, jetzt schon wissen, welche Maßnahmen implementiert werden müssen.

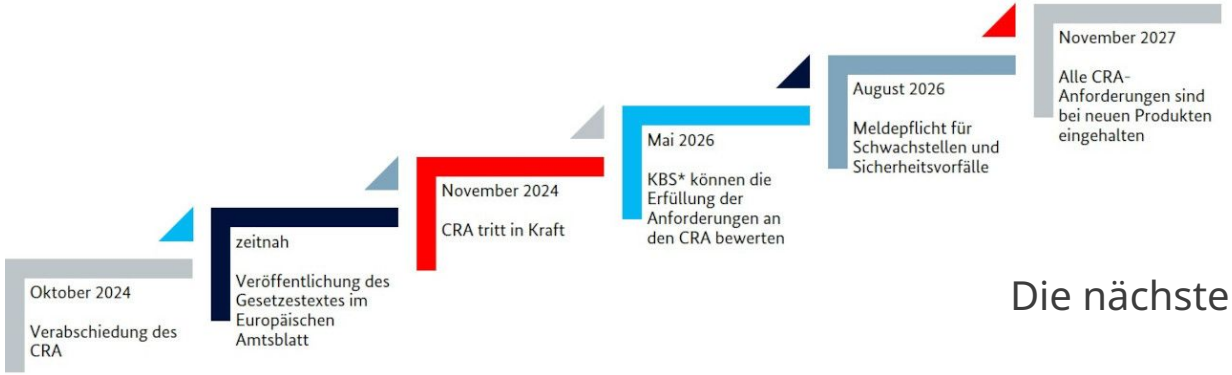
GESETZLICHE RAHMENBEDINGUNGEN

Cyber Resilience Act Resilience Act (CRA) - VERORDNUNG (EU) 2024/2847 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 23. Oktober 2024 über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen und zur Änderung der Verordnungen (EU) Nr. 168/2013 und (EU) 2019/1020 und der Richtlinie (EU) 2020/1828 (Cyberresilienz-Verordnung)Regulation (EU) 2022/2554.

Die Verordnung hat allgemeine Geltung. Sie ist in allen ihren Teilen verbindlich und gilt unmittelbar in jedem Mitgliedstaat.

Alle Produkte, die in der EU verkauft werden und „digitale Elemente“ enthalten, müssen den Anforderungen des CRA entsprechen. Ziel ist es, die Widerstandsfähigkeit gegen Cyberangriffe zu erhöhen und die Sicherheit digitaler Produkte während ihres gesamten Lebenszyklus zu gewährleisten. Dies betrifft sowohl Hardware als auch Software, die mit Netzwerken oder anderen Geräten verbunden sind, oder generell Produkte mit digitalen Elementen.

GESETZLICHE RAHMENBEDINGUNGEN



Die nächsten Schritte des CRA

*KBS = Konformitätsbewertungsstellen
Quelle:
https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Cyber_Resilience_Act/cyber_resilience_act_node.html

GESETZLICHE RAHMENBEDINGUNGEN

Mit dem CRA wird die Cybersicherheit von Produkten, die miteinander oder mit dem Internet verbunden werden können, verbessert.

Diese Produkte werden von Unternehmen hergestellt und an Kunden vertrieben. Sie werden aber auch in Unternehmen für die Produktion eingesetzt sowie als Vorprodukte bezogen und weiter verbaut beziehungsweise veredelt und sind damit Bestandteil von Lieferketten.

Da es sich um eine EU Verordnung handelt, gelten alle Anforderungen unmittelbar zwingend. Deutschland hat hier keinen politischen Einfluss.

AGENDA

1 VORSTELLUNG

2 GESETZLICHE RAHMENBEDINGUNGEN

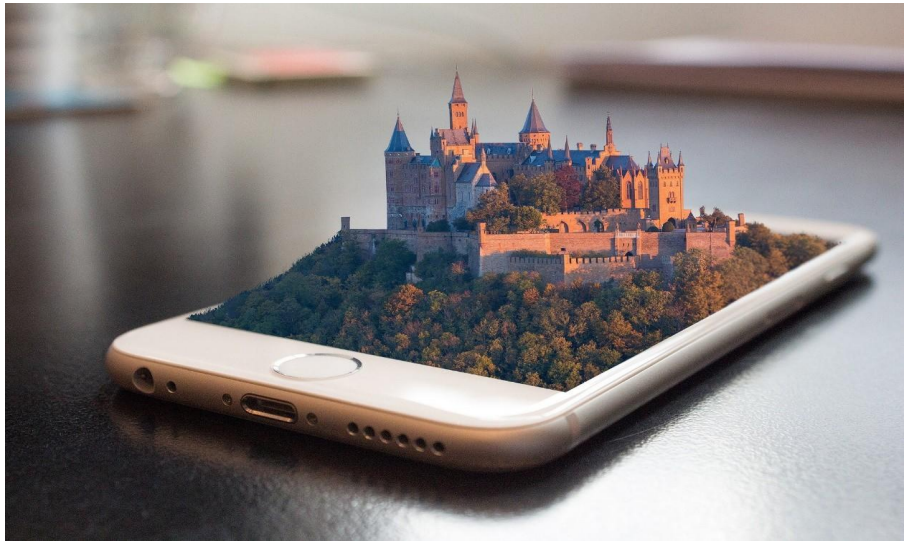
3 KRITIS-DACHGESETZ

4 NIS 2

5 CYBER RESILIENCE ACT

KRITIS-DACHGESETZ

Das KRITIS-Dachgesetz wird ein eigenständiges Gesetz, das Resilienz bei Betreibern kritischer Anlagen regeln wird.



KRITIS-DACHGESETZ

1. Das KRITIS-Dachgesetz hat den physischen bzw. „analogen“ Schutz kritischer Infrastrukturen zum Gegenstand.

2. Insgesamt ist der Anwendungsbereich des KRITIS-DachG kleiner und die Regelungsintensität im Vergleich zum NIS2UmsuCG geringer. Deshalb auch enthält das KRITIS-DachG keine sektoralen oder branchenspezifischen Regelungen, sondern will lediglich abstrakt vorgeben, dass in sämtlichen KRITIS-Sektoren geeignete und verhältnismäßige Maßnahmen zum physischen Infrastrukturschutz von den Betreibern kritischer Anlagen zu treffen sind.

KRITIS-DACHGESETZ

Der Begriff „kritische Infrastruktur“ ist gesetzlich nicht einheitlich definiert. Es gibt mehrere Gesetze, die als spezifischer Beitrag zum Schutz kritischer Infrastrukturen angesehen werden.

Bisher galt (NIS 1):

Kritische Infrastrukturen im Sinne dieses Gesetzes sind Einrichtungen, Anlagen oder Teile davon, die

1. den Sektoren Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung, Finanz- und Versicherungswesen sowie Siedlungsabfallentsorgung angehören und

2. von hoher Bedeutung für das Funktionieren des Gemeinwesens sind, weil durch ihren Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden.

KRITIS-DACHGESETZ

Regierungsentwurf von November 2024 “Entwurf eines Gesetzes zur Umsetzung der Richtlinie (EU) 2022/2557 und zur Stärkung der Resilienz von Betreibern kritischer Anlagen ”

§ 2 Begriffsbestimmungen
Im Sinne dieses Gesetzes ist
1. „Betreiber kritischer Anlagen“ eine natürliche oder juristische Person oder eine rechtlich unselbständige Organisationseinheit einer Gebietskörperschaft, die unter Berücksichtigung der rechtlichen, wirtschaftlichen und tatsächlichen Umstände bestimmenden Einfluss auf eine kritische Anlage ausübt; .....

KRITIS-DACHGESETZ

Nach § 2 wird Resilienz wie folgt definiert:

„Resilienz“ die Fähigkeit eines Betreibers kritischer Anlagen, einen Vorfall zu verhindern, sich davor zu schützen, darauf zu reagieren, einen solchen abzuwehren, die Folgen eines solchen Vorfalls zu begrenzen, einen Vorfall aufzufangen, zu bewältigen und sich von einem solchen Vorfall zu erholen; …

KRITIS-DACHGESETZ

Folgende Mindestmaßnahmen stehen fest:

- Vorsorge: Präventionsmaßnahmen gegen Vorfälle, Disaster und Klimawandel
- Physische Sicherheit: Absicherung der ihrer Liegenschaften und Kritischen Infrastruktur mit physischen Schutzmaßnahmen, Perimeterüberwachung, Detektion und Zutrittskontrolle
- Krisen: Risiko- und Krisenmanagement zur Bewältigung von Krisen, mit definierten Prozeduren, Protokollen und Alarmierung

KRITIS-DACHGESETZ

Folgende Mindestmaßnahmen stehen fest:

- Wiederherstellung: Business Continuity Management (BCM) und Maßnahmen zur Wiederherstellung nach Vorfällen — inkl. alternative Lieferketten
- Personal: Sicherheitsmanagement und besondere personelle Sicherheit, Zutrittskontrolle, Sicherheitsüberprüfung, einschließlich externem Personal und Dienstleistern
- Awareness: Beim Personal über die Resilienz-Maßnahmen

KRITIS-DACHGESETZ

Folgende Mindestmaßnahmen stehen fest:

- nationale Risikobewertungen,
- betreiberseitige Risikobewertungen,
- Erstellung von Resilienzplänen durch die Betreiber,
- Erarbeitung branchenspezifischer Schutzstandards durch die zuständigen Verbände sowie
- Äquivalenzprüfungen durch die fachlich zuständigen Behörden.
- Die zentralen Betreiberpflichten zu Risikoanalysen und Risikobewertungen, Resilienzmaßnahmen, Nachweispflichten und für das Meldewesen treten am 17.07.2026 in Kraft?

KRITIS-DACHGESETZ

Betreiber *kritischer Anlagen fallen unter den Anwendungsbereich des Gesetzes*, wenn diese (grundsätzlich) über 500 Tsd. Personen versorgen.

Betreiber ist eine natürliche oder juristische Person, die unter Berücksichtigung der rechtlichen, wirtschaftlichen und tatsächlichen Umstände bestimmenden Einfluss auf die Beschaffenheit und den Betrieb einer Anlage oder Teilen davon ausübt.

Die „neue“ KRITIS-VO muss noch erlassen werden. Hier werden die Schwellenwerte definiert werden.

Man geht in Deutschland von ca. 1.800 Unternehmen aus.

KRITIS-DACHGESETZ

Die betroffenen Unternehmen in Deutschland umfassen Betreiber kritischer Anlagen in den (bisherigen) KRITIS-Sektoren. Das KRITIS-Dachgesetz wird diese Betreiber regulieren.

Betreiber	Größe	Sektor
Kritische Anlagen § 2 Abs.1	Anlagen mit Schwellenwerten § 4 Abs. 1	Energie, Transport und Verkehr, Finanz-/Versicherungswesen, Gesundheitswesen, Trinkwasser, Abwasser, Ernährung, Informationstechnik und Telekommunikation, Weltraum, Siedlungsabfallentsorgung

KRITIS-DACHGESETZ

Die betroffenen Unternehmen in Deutschland umfassen Betreiber kritischer Anlagen in den (bisherigen) KRITIS-Sektoren. Das KRITIS-Dachgesetz wird diese Betreiber regulieren.

Sektor § 4 Abs.1	Kritische Dienstleistung § 3 Abs. 3	Kritische Anlagen § 16 Abs.1
Kritische Anlagen § 2 Abs.1	Anlagen mit Schwellenwerten § 4 Abs. 1	Fehlt noch. Es ist auf die zur Zeit gültige KRITIS-VO zurückzugreifen

KRITIS-DACHGESETZ

§ 4 Anwendungsbereich; kritische Anlagen; Geltungsumfang

(1) Eine Anlage ist ab dem durch die Rechtsverordnung nach § 16 festgelegten Stichtag eine kritische Anlage, wenn sie einer der durch Rechtsverordnung nach § 16 Absatz 1 festgelegten Anlagenarten in den Sektoren Energie, Transport und Verkehr, Finanz- und Versicherungswesen, Gesundheitswesen, Trinkwasser, Abwasser, Ernährung, Informationstechnik und Telekommunikation, Weltraum oder Siedlungsabfallentsorgung zuzuordnen ist und diese die durch Rechtsverordnung nach § 16 Absatz 1 festgelegten Schwellenwerte erreicht oder überschreitet.

Der Regelschwellenwert von 500.000 zu versorgenden Einwohnern ist dabei zugrunde zu legen.

KRITIS-DACHGESETZ

Nach § 9 Abs. 1 müssen Betreiber alle vier Jahre **Risikoanalysen** durchführen.

Es ist der sogenannte *„All-Gefahren-Ansatz“* anzusetzen.

- Das bedeutet, alle möglichen Gefahrenlagen wie z.B. Klimawandel, Geopolitische Lagen etc. in die Bedrohungsanalyse zu übernehmen und entsprechende Maßnahmen zu definieren.

Die Behörden werden diese Risikoanalysen bewerten, zumindest dann, wenn ein Risiko eingetreten ist.

KRITIS-DACHGESETZ

Nach § 10 müssen Betreiber geeignete und verhältnismäßige Maßnahmen umsetzen, um die Resilienz zu gewährleisten. Dabei haben sie den **Stand der Technik** einzuhalten.

Ebenfalls müssen sie Maßnahmen zur Gewährleistung der Resilienz treffen, um

- das Auftreten von **Vorfällen** zu **verhindern**,
- einen angemessenen **physischen Schutz** ihrer Liegenschaften und kritischen Anlagen zu gewährleisten,
- auf Vorfälle zu reagieren, sie abzuwehren und die negativen Auswirkungen solcher Vorfälle zu begrenzen,

KRITIS-DACHGESETZ

Nach § 10 Abs. 1 müssen Maßnahmen zur Gewährleistung der Resilienz getroffen werden, um

- nach Vorfällen die **Wiederherstellung** der kritischen Dienstleistung zu gewährleisten,

- ein angemessenes **Sicherheitsmanagement** hinsichtlich der **Mitarbeiter** zu gewährleisten, einschließlich des Personals externer **Dienstleister**, und

- das Personal für die unter den Nummern 1 bis 5 genannten Maßnahmen durch Informationsmaterialien, Schulungen und Übungen zu **sensibilisieren.**

KRITIS-DACHGESETZ

§ 10 Abs. 3 gibt Beispiele vor:

- Maßnahmen der Notfallvorsorge,
- Maßnahmen zur Anpassung an den Klimawandel,
- Maßnahmen des Objektschutzes, darunter das Aufstellen von Zäunen und Sperren
- Instrumente und Verfahren für die Überwachung der Umgebung,

KRITIS-DACHGESETZ

§ 10 Abs. 3 gibt Beispiele vor:

- der Einsatz von Detektionsgeräten und Zugangskontrollen,
- Risiko- und Krisenmanagementverfahren und,
- vorgegebene Abläufe im Alarmfall,
- Maßnahmen zur Aufrechterhaltung des Betriebs, darunter die Notstromversorgung,
- die Ermittlung alternativer Lieferketten, um die Erbringung des wesentlichen Dienstes wiederaufzunehmen.

Sichere Lieferkette (1/2)

Betreiber (KRITIS) müssen im Rahmen der regulierten Dienstleistungen Lieferanten, Dienstleister und Externe schützen und steuern.

Mit dem KRITIS-Dachgesetz erhöhen sich die Anforderungen an Sicherheit bei Dienstleistern.

Supply Chain Security ist ebenfalls neu und vertiefend reguliert.

Sichere Lieferkette (2/2)

Daraus folgt, dass sie verpflichtet sind, vor allen Dingen innerhalb des Ausschreibungsverfahrens, das adäquate Sicherheitsniveau vom Lieferanten Dienstleister zu fordern. Insbesondere sind hier die folgenden Richtlinien verbindlich:

- Richtlinie zum Umgang mit und Sicherheitsanforderungen an Dienstleister des KRITIS-Betreibers.

- Kontrolle der Leistungserbringung und der Sicherheitsanforderungen an Dienstleister und Lieferanten des KRITIS-Betreibers.

AGENDA

1 VORSTELLUNG

2 GESETZLICHE RAHMENBEDINGUNGEN

3 KRITIS-DACHGESETZ

4 NIS 2

5 CYBER RESILIENCE ACT

NIS2

Der Anwendungsbereich der sogenannte NIS2 Richtlinie orientiert sich nicht an Schwellenwerte.

Maßgeblich ist die size-cap-rule, also die Größe des Unternehmens.

Hinzukommen muss, dass das Unternehmen in einem der Sektoren tätig ist.

Folgende Unternehmensgrößen sind zu unterscheiden:

Besonders wichtige Einrichtungen

Dies sind zunächst die Betreiber kritischer Anlagen. (§ 28 V)

Es ändert sich im Grunde hier nicht viel. Die bisherige Logik von Kritis-Sektoren, kritischen Dienstleistungen und die Anlagen mit Schwellenwerten bleibt erhalten.

Besonders wichtige Einrichtungen

Neben ben KRITIS-Betreibern sind dies Großunternehmen aus den Sektoren in NIS2-Anlage 1 und einige Unternehmen unabhängig ihrer Größe und KRITIS-Betreiber.

Dies sind Unternehmen ab 250 MA oder einem Umsatz von 50 Mio. und 42 Mio. Bilanz.

Hier sind nicht mehr die Schwellenwerte entscheidend, sondern “nur” die Tätigkeit in einem der Sektoren der Anlage 1.

Wichtige Einrichtungen

Dies sind Unternehmen ab 50 Mitarbeitern

oder

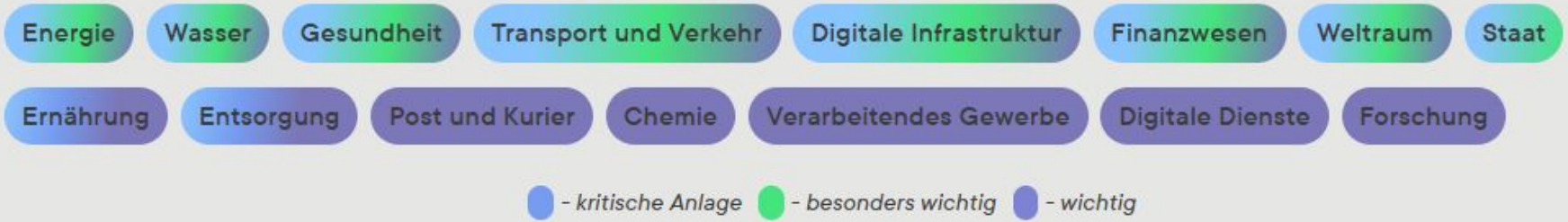
einem Umsatz und Bilanz über 10 Millionen,

die in den Sektoren der Anlage 1 und Anlage 2 tätig sind.

NIS2

Sektoren ab 2025

Mit der NIS2-Umsetzung und dem KRITIS-Dachgesetz gibt es ab 2025 zwei Gruppen von Sektoren: Die *besonders wichtigen* und *wichtigen Einrichtungen* sind mittlere und große Unternehmen sowie die *Betreiber kritischer Anlagen* (KRITIS).



Quelle: https://www.openkritis.de/it-sicherheitsgesetz/kritis-sektoren.html

NIS2

Grundsätzlich lassen sich die Anforderungen in drei Gruppen aufteilen:

- Hauptaufgaben
- Cyber Security Maßnahmen
- Physische Sicherheitsmaßnahmen

NIS2

Hauptanforderungen:
Implementierung eines Risikomanagementsystems nach internationalem Standard (für NIS2UmsCG z.B. ISO 2700xx)

Implementierung/Nachweis der notwendigen Security Maßnahmen
(siehe Folgefolien)

Implementierung der Lieferketten-Sicherheit (Supply Chain Security)
(inkl. Regelungen zum Komponenteneinsatz)

Implementierung eines Störungsmeldungsmanagement/Incident Reporting
(innerbetrieblich und auch zu den zuständigen Behörden)

Hauptanforderungen:
Bei der Umsetzung der genannten Hauptanforderungen ist ein All-Gefahren-Ansatz (jedwede Ursache) zu berücksichtigen.

Die Mindestanforderungen müssen nach dem Stand der Technik und unter Berücksichtigung relevanter europäischer und internationaler Normen und technischer Spezifikationen umgesetzt werden.

NIS2

Hauptanforderungen:
Den Leitungsorganen kommt die Verantwortung zu, die Umsetzung der Maßnahmen nicht nur zu billigen, sondern auch zu überwachen. Sie können bei Verstößen persönlich haftbar gemacht werden.

Bei Verstößen gegen den wirksamen Einsatz der Risikomanagementmaßnahmen oder gegen die Berichtspflichten drohen empfindliche Geldbußen: bei wesentlichen Einrichtungen bis 10 Mio. EUR oder 2% des jährlichen Gesamtumsatzes, bei wichtigen Einrichtungen bis 7 Mio. EUR oder 1,4 % des jährlichen Gesamtumsatzes.

Cyber Security Maßnahmen

- Konzepte in Bezug auf die Risikoanalyse und Sicherheit für Informationssysteme,
- Bewältigung von Sicherheitsvorfällen,
- Aufrechterhaltung des Betriebs, wie Backup-Management und Wiederherstellung nach einem Notfall, und Krisenmanagement

Cyber Security Maßnahmen

- Sicherheit der Lieferkette einschließlich sicherheitsbezogener Aspekte der Beziehungen zwischen den einzelnen Einrichtungen und ihren unmittelbaren Anbietern oder Diensteanbietern,
- Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von informationstechnischen Systemen, Komponenten und Prozessen, einschließlich Management und Offenlegung von Schwachstellen,
- Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen im Bereich der Cybersicherheit.

Cyber Security Maßnahmen

- Grundlegende Verfahren im Bereich der Cyberhygiene und Schulungen im Bereich der Cybersicherheit,
- Konzepte und Verfahren für den Einsatz von Kryptografie und Verschlüsselung,
- Sicherheit des Personals, Konzepte für die Zugriffskontrolle und Management von Anlagen,

Cyber Security Maßnahmen

- Verwendung von Lösungen zur MultiFaktor-Authentifizierung oder kontinuierlichen Authentifizierung, gesicherte Sprach-, Video- und Textkommunikation sowie gegebenenfalls gesicherte Notfallkommunikationssysteme innerhalb der Einrichtung.

Physische Sicherheitsmaßnahmen, um…

- … um das Auftreten von Vorfällen zu verhindern (Notallvorsorge, Anpassungen an den Klimawandel)
- … um angemessenen physischen Schutz ihrer Räumlichkeiten und kritischen Infrastrukturen zu gewährleisten (Objektschutz (u.a. Zäune/Sperren), Umgebungsüberwachung, Detektionsgeräte, Zutrittskontrollen)
- … um auf Vorfälle zu reagieren, abzuwehren oder Folgen zu begrenzen (Risiko- und Krisenmanagementverfahren und -protokolle, Abläufe im Alarmfall

Physische Sicherheitsmaßnahmen, um…

- … die Wiederherstellung zu gewährleisten (Aufrechterhaltung des Betriebes (z.B. Notstromversorgung), Alternative Lieferketten)
- … zum Sicherheitsmanagement hinsichtlich Mitarbeiter (Festlegung welches Personal kritische Funktionen wahrnimmt, Festlegung von Zugangsrechten zu sensiblen Informationen, Sicherheitsüberprüfung)

Berichtspflichten

NIS2 regelt den Zeitpunkt und Inhalt der Informationen, die betroffene Unternehmen bei erheblichen Sicherheitsvorfällen als Meldung übermitteln müssen.

Demnach kann ein Sicherheitsvorfall erheblich sein, wenn er „schwerwiegende Betriebsstörung der Dienste oder finanzielle Verluste verursacht oder verursachen kann“ oder aber „natürliche oder juristische Person durch erhebliche materielle oder immaterielle Schäden beeinträchtigt“.

Berichtspflichten

- So hat unverzüglich nach Kenntnisnahme eines Sicherheitsvorfalls, der „schwerwiegende Betriebsstörungen der Dienste“ verursachen kann, eine Frühwarnung zu erfolgen.
- Innerhalb von 24 Stunden müssen betroffene Unternehmen relevante Informationen zu Ursachen, Schweregrad und Folgen an ein CSIRT und gegebenenfalls an zuständige Behörden übermitteln.
- Innerhalb von 72 Stunden müssen verfügbare Informationen aktualisiert und erste Bewertungen geliefert werden.

Sichere Lieferkette

Folgende Vorgaben sind heut schon verbindlich:

- Die Sicherheitsanforderungen des ISMS müssen für Dienstleister, Lieferanten und Externe in den KRITIS-Anlagen verbindlich gemacht werden.
- Dies umfasst KRITIS-relevante Mindestanforderungen für Externe, Schutz von Informationen, Incident Management und Vorfallmeldungen und die Integration ins eigene Risiko-Management.
- Die Anforderungen an Externe müssen vertraglich festgehalten und kontrolliert, und operativ durch Audits, Tests, Zertifizierungen überprüft werden.

AGENDA

1 VORSTELLUNG

2 GESETZLICHE RAHMENBEDINGUNGEN

3 KRITIS-DACHGESETZ

4 NIS 2

5 CYBER RESILIENCE ACT

CYBER RESILIENCE ACT

Wie schon ausgeführt, ist der CRA als EU-Verordnung unmittelbar geltendes und zwingendes Gesetz. Einer Umsetzung in Deutschland in nationales Recht bedarf es daher nicht.

Am 10. Oktober ist er in Kraft getreten und muss bis zum 10. Oktober 2027 in den Unternehmen umgesetzt sein.

Vom CRA sind alle Unternehmen, die Produkte herstellen, importieren oder vertreiben, die in der EU verfügbar sind und irgendeine Art von Datenkommunikation beinhalten erfasst.

Die Verordnung stellt somit eine ergänzende Regelung zusätzlich zu NIS2 dar, die die Sicherheit der Unternehmen im Fokus hat, während CRA sich auf die Sicherheit der Produkte selbst, unabhängig von der Umgebung, in der sie eingesetzt werden konzentriert.

CYBER RESILIENCE ACT

Anwendungsbereich:

Hersteller: Unternehmen, die Hardware oder Software mit digitalen Komponenten entwickeln und produzieren, müssen sicherstellen, dass ihre Produkte den festgelegten Sicherheitsstandards entsprechen

Importeure: Unternehmen, die solche Produkte aus Drittländern in die EU einführen, sind dafür verantwortlich, dass die importierten Waren den CRA-Anforderungen genügen.

Händler: Unternehmen, die Produkte mit digitalen Elementen innerhalb der EU vertreiben, müssen gewährleisten, dass die von ihnen verkauften Produkte den Cybersicherheitsstandards entsprechen.

CYBER RESILIENCE ACT

Produkte werden nach Kritikalität unterschieden:

Nicht-kritische Produkte mit digitalen Elementen

Diese Kategorie umfasst etwa 90 % der betroffenen Produkte und beinhaltet typische Verbraucherprodukte wie:

- Basis-IoT-Geräte
- einfache Netzwerkgeräte
- Standard-Sensoren
- Smart-Home-Komponenten
- Hausautomatisierungssysteme
- Fotobearbeitungssoftware

Für diese Produkte gelten allgemeine Sicherheitsanforderungen, die sich auf den Schutz vor Cyberbedrohungen und den Umgang mit Schwachstellen konzentrieren.

CYBER RESILIENCE ACT

Produkte werden nach Kritikalität unterschieden:

Kritische Produkte mit digitalen Elementen

Diese Kategorie ist weiter unterteilt in zwei Klassen:

- Klasse I:
  - Router
  - VPN-Produkte
  - Firewalls
  - Smart Meter Gateways
  - Sicherheitskameras
  - IoT-Konnektivitätsmodule (z. B. für Industrieanwendungen).
  - Passwort-Manager
  - Identitätsmanagement-Systeme

CYBER RESILIENCE ACT

Produkte werden nach Kritikalität unterschieden:

Kritische Produkte mit digitalen Elementen

Diese Kategorie ist weiter unterteilt in zwei Klassen:

- **Klasse II**:
  - Betriebssysteme
  - Mikroprozessoren
  - Hardware-Sicherheitsmodule
  - Chipkarten
  - serverseitige Prozessoren
  - Netzwerkspeichergeräte (NAS)
  - Switches.

Hochkritische Produkte mit digitalen Elementen sind noch nicht definiert.

CYBER RESILIENCE ACT

Energiespeicheranlagen sind mit digitalen Steuerungs- und Überwachungssystemen ausgestattet, die eine Verbindung zu Netzwerken oder anderen Geräten ermöglichen, um den Betrieb zu optimieren und die Integration in intelligente Netze (Smart Grids) zu gewährleisten.

Wenn eine Energiespeicheranlage über solche digitalen Elemente verfügt, die eine direkte oder indirekte Verbindung zu anderen Geräten oder Netzwerken ermöglichen, fällt sie unter den Anwendungsbereich des CRA.

CYBER RESILIENCE ACT

Folgende Mindestmaßnahmen sind umzusetzen:

1. Risikobewertung

- Durchführung umfassender Risikoanalysen zur Identifikation von Sicherheitslücken und Schwachstellen.

2. Sicheres Design

- Standardmäßig sichere Konfiguration von Produkten.
- Einsatz sicherer Komponenten, Vermeidung bekannter Schwachstellen, Nutzung von Sicherheitsmechanismen wie Verschlüsselung.
- Minimierung der Angriffsfläche und Auswirkungen von Sicherheitsvorfällen.
- Gewährleistung von Vertraulichkeit und Integrität gespeicherter, bearbeiteter und übertragener Daten.

CYBER RESILIENCE ACT

Folgende Mindestmaßnahmen sind umzusetzen:

3. Sicherheitsupdates und Schwachstellenmanagement

- Regelmäßige Bereitstellung von Security Updates während des gesamten Produktlebenszyklus.
- Einrichtung einer zentralen Anlaufstelle für User zur Meldung von Schwachstellen.
- Öffentliche Bekanntgabe einer Kontaktadresse und Durchführung eines Coordinated Vulnerability Disclosure (CVD).
- Zeitnahe Bereitstellung von Patches für betroffene Produkte.
- Bei Drittkomponenten: Information des Komponentenanbieters über Schwachstellen und Maßnahmen.
- Anlegen einer Software-Stückliste (SBOM) zur Nachverfolgung von Produktkomponenten und Schwachstellen.

CYBER RESILIENCE ACT

Folgende Mindestmaßnahmen sind umzusetzen:

4. Transparenz

- Bereitstellung klarer Sicherheitsinformationen für Verbraucher*innen und Interessengruppen (technische Dokumentation, Updates, Support- und Kontaktinformationen).

5. Nachweisbarkeit

- Sicherstellung und Dokumentation der Einhaltung der CRA-Anforderungen (z. B. durch Zertifizierungen oder Audits).

CYBER RESILIENCE ACT

Folgende Mindestmaßnahmen sind umzusetzen:

6. Dokumentation

- Erstellung umfassender technischer und nutzerorientierter Dokumentationen mit Sicherheitsinformationen und Anweisungen zur sicheren Nutzung und Aktualisierung.

7. Einhaltung der Vorgaben

- Produkte müssen während des gesamten Support-Zeitraums den Anforderungen entsprechen, nicht nur bei Markteinführung.

CYBER RESILIENCE ACT

Folgende Mindestmaßnahmen sind umzusetzen:

8. Meldepflichten

- Berichterstattung über sicherheitsrelevante Vorfälle über eine zentrale EU-Meldeplattform
- Vorabmeldung innerhalb von 24 Stunden nach Entdeckung einer Schwachstelle oder eines schwerwiegenden Vorfalls.
- Detaillierte Beschreibung des Vorfalls und der Maßnahmen innerhalb von 72 Stunden.
- Abschlussbericht spätestens 14 Tage nach Bereitstellung einer Schadensbegrenzungsmaßnahme oder bei schwerwiegenden Vorfällen innerhalb eines Monats.
- Nutzende müssen zeitnah über Vorfälle und erforderliche Sicherheitsmaßnahmen informiert werden.

CYBER RESILIENCE ACT

Anforderungen für Hardwarekomponenten und digitale Produkte

Anforderung	Standardprodukte	Kritische Produkte Klasse I	Kritische Produkte Klasse II
Cybersicherheit in der Entwicklung: Sicherheitsmaß-nahmen während der gesamten Entwicklungsphase.	Ja	Ja	Ja
Risikobewertung: Analyse und Bewertung potenzieller Cyber-sicherheitsrisiken.	Ja	Ja	Ja

CYBER RESILIENCE ACT

Anforderungen für Hardwarekomponenten und digitale Produkte

Anforderung	Standardprodukte	Kritische Produkte Klasse I	Kritische Produkte Klasse II
Konformitätsbewertung: Nachweis der Einhaltung der Anforderungen.	Selbstbewertung	Bewertung durch Dritte	Strenge Bewertung durch unabhängige Stellen
CE-Kennzeichnung: Verpflichtende CE-Kennzeichnung als Nachweis der Konformität.	Ja	Ja	Ja

CYBER RESILIENCE ACT

Anforderungen für Hardwarekomponenten und digitale Produkte

Anforderung	Standardprodukte	Kritische Produkte Klasse I	Kritische Produkte Klasse II
Technische Dokumentation: Bereitstellung umfassender technischer Unterlagen.	Ja	Ja	Ja
Meldepflicht bei Sicherheitsvorfällen Meldung innerhalb von 24 Stunden.	Ja	Ja	Ja

CYBER RESILIENCE ACT

Anforderungen für Hardwarekomponenten und digitale Produkte

Anforderung	Standardprodukte	Kritische Produkte Klasse I	Kritische Produkte Klasse II
Sicherheitsupdates: Bereitstellung von Updates über mindestens fünf Jahre.	Ja	Ja	Ja
Information der Nutzer: Bereitstellung von Anleitungen und Sicherheitsinformationen.	Ja	Ja	Ja

VIELEN DANK FÜR IHRE AUFMERKSAMKEIT!

Kontakt:

Holger Berens
holger.berens@bski.de
h.berens@concepture.de