KPMG

Wir schaffen Vertrauen in der digitalen Welt.

EU Regulierung zur Cybersecurity

Ein Update

Regionalgruppe Köln der Gesellschaft für Informatik
Dr. Frank Damm und Lysander Lenzen

24.11.2025

Wieso sehen wir Regulierung zur Cybersecurity?

Wir verlagern mehr und mehr Daten und menschliche Interaktion in den Cyberraum.

Infrastruktur

- Energieversorgung
- Transport und Verkehr
- Telekommunikation
- Gesundheit
- Wasser und Ernährung

Alltagsprodukte

- Smartphone & Tablets
- Computer
- Smart Home Geräte
- Kühlschränke
- Blutzuckermessgeräte
- Alarmanlagen

Geld

- Geldautomaten
- bargeldlose Zahlungen
- Überweisungen
- Geldanlagen und Vermögensbildung

⇒ Unsere Abhängigkeit vom Cyberraum nimmt zu.

Auch böswillige Akteure nutzen den Cyberraum: die Bedrohungslage wächst.
Freier Markt und globale Handelsbeziehungen lösen diese Herausforderungen nicht.

Übersicht

01 Timeline 04

02 NIS 2 06

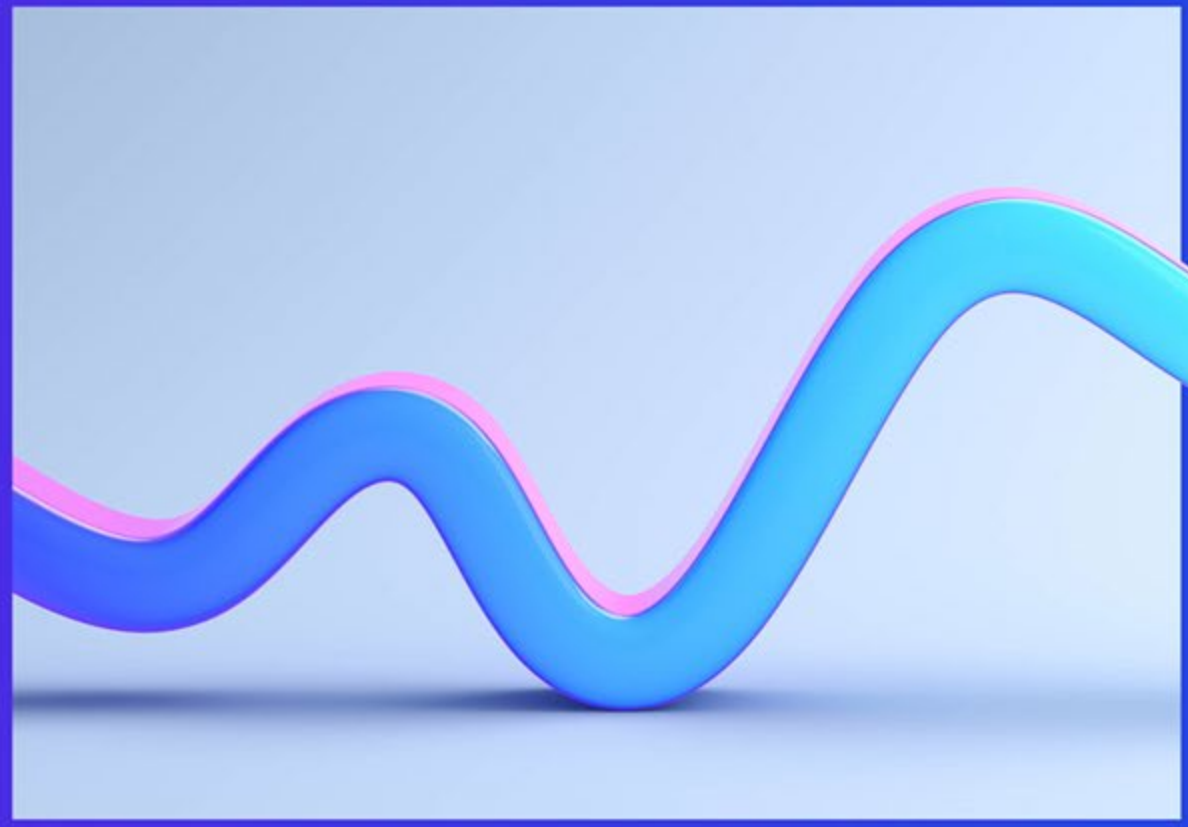
03 CRA 17

KPMG

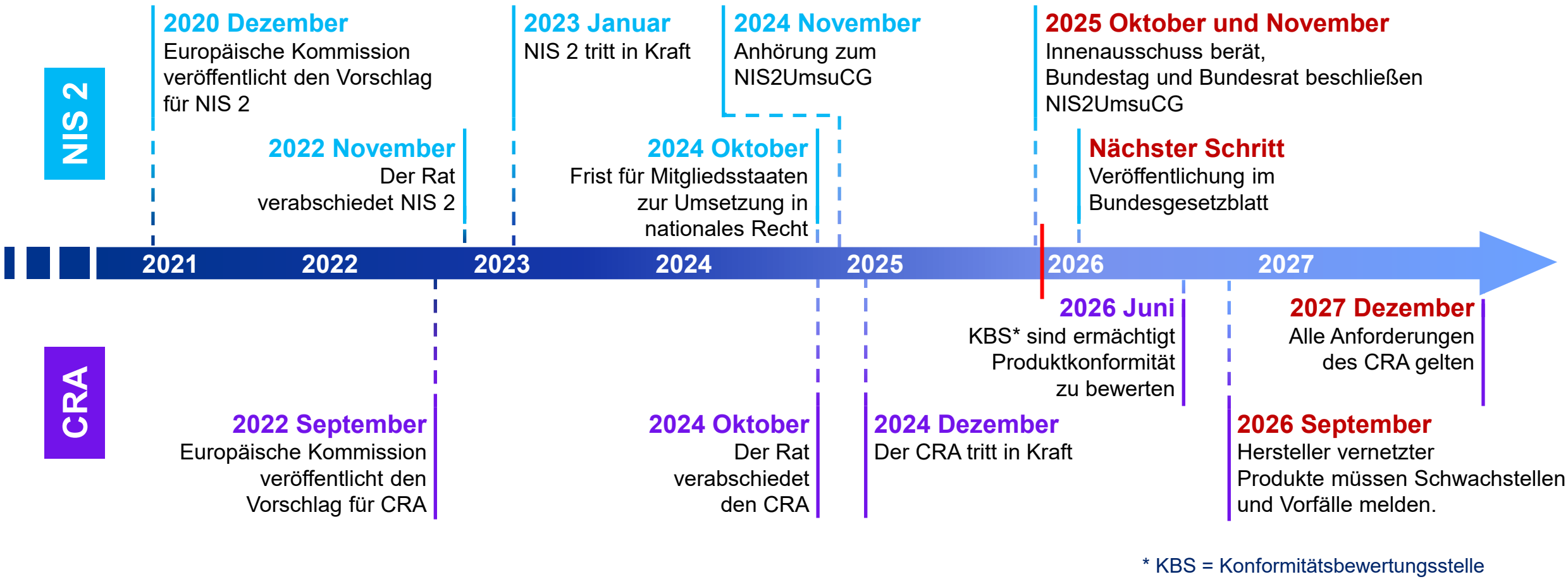
01

Timeline

Regulatorische Meilensteine: NIS 2 & CRA



Timeline



* KBS = Konformitätsbewertungsstelle

KPMG

02

NIS 2

Network and Information Security Directive

Einführung in NIS 2

NIS 2 vereinheitlicht die EU-weite Resilienz kritischer Infrastrukturen gegen Cyber-Bedrohungen, unterstützt die grenzüberschreitende Zusammenarbeit und gewährleistet eine sichere Digitalisierung im Binnenmarkt.

2015

IT-Sicherheitsgesetz 1.0
- Erhöhung der Sicherheit von kritischen Informationstechnischen Systemen

2016

NIS Verordnung
- Festlegung grundlegender Normen für wesentliche Dienstleistungen

2021

IT Sicherheitsgesetz 2.0
- Erweiterung der Sektoren und der Befugnisse des BSI

2022

NIS 2 – Directive
- Erweiterte Version von NIS1, die mehr Sektoren abdeckt und EU-weit einheitliche Cybersicherheitsstandards festlegt

NIS 2 Transposition Deadline
- Alle EU-Mitgliedsstaaten sind verpflichtet, NIS 2 in ihre nationalen Gesetze zu integrieren

2024

NIS 2 Durchführungsverordnung
- Nennung von technischen und methodischen Anforderungen

Betroffen sind in DE ca. 30.000 Unternehmen, die eine wichtige oder besonders wichtige Einrichtung nach NIS 2 sein werden.

Die Verantwortung für die Umsetzung liegt bei der Geschäftsleitung jedes einzelnen Unternehmens.

Anforderungen:

- Netzwerk- und Informationssicherheit
- Risikomanagement
- Incident Management
- Sicherheit der Lieferkette

Drohende Geldbußen

Bis zu

10 Millionen €

Oder

2% des weltweiten Jahresumsatzes

Von NIS 2 betroffene Sektoren

Sektoren besonders wichtiger Einrichtungen
(und wichtiger Einrichtungen)

- Energie
- Digitale Infrastruktur
- Transport und Verkehr
- Weltraum
- Finanzwesen
- Gesundheit
- Wasser

Sektoren wichtiger Einrichtungen

- Post- und Kurierdienste
- Anbieter digitaler Dienste
- Abfallbewirtschaftung
- Forschung
- Produktion, Herstellung und Handel mit chemischen Stoffen
- Produktion, Verarbeitung und Vertrieb von Lebensmitteln
- Verarbeitendes Gewerbe/Herstellung von Waren

NIS 2 Anforderungen auf einen Blick
(für "Besonders wichtige" und "wichtige" Einrichtungen, siehe Kapitel 2 BSIG §§30-36)

Kontinuierliche Verbesserung & Compliance-Überwachung

- Kontinuierliche Überprüfung und Aktualisierung der technischen und organisatorischen Maßnahmen
- Neue Bedrohungen und Schwachstellen angehen
- Audits, Prüfungen und Zertifizierungen durch zuständige Behörden managen

Meldepflichten

- Erhebliche Sicherheitsvorfälle müssen innerhalb von 24 Stunden an die zuständigen Behörden gemeldet werden (Erstmeldung)
- Meldung nach 72 Stunden
- Abschlussmeldung nach 4 Wochen
- Behörden können die Unterrichtung der Kunden und der Öffentlichkeit verlangen

Kooperation mit zuständigen Behörden

- Untersuchungen erleichtern und Abhilfemaßnahmen auf Anforderung der Behörden umsetzen
- Angebote von den Behörden zur Unterstützung bei einem Sicherheitsvorfall

Registrierung

- Betreiber registrieren sich beim Bundesamt für Sicherheit in der Informationstechnik (BSI)
- Die Registrierungspflicht gilt unmittelbar mit Inkrafttreten des NIS2UmsuCG

Risikomanagement

- Angemessene und wirksame technische und organisatorische Maßnahmen umsetzen
- Widerstandsfähigkeit von IT-Netzwerken und Informationssystemen sicherstellen
- Risikobewertungen durchführen und Cybersicherheitsmaßnahmen ergreifen
- Geschäftsleitungen nehmen regelmäßig an Schulungen zur Cybersicherheit teil
- und setzen Risikomanagement-Maßnahmen um und überwachen deren Umsetzung

Dokumentation

- Dokumentation von technischen und organisatorischen Maßnahmen und deren Wirkung
- Meldungen zu Sicherheitsvorfällen

Technische und organisatorische Maßnahmen nach § 30 NIS2UmsuCG

Geeignete, verhältnismäßige und wirksame technische und organisatorische Maßnahmen ergreifen

Stand der Technik einhalten, einschlägige europäische und internationale Normen berücksichtigen, mindestens 10 Detailthemen umsetzen

Vermeidung und Minderung der Auswirkungen von Cybervorfällen

Geschäftsleitung: Risikomanagementmaßnahmen umsetzen und ihre Umsetzung überwachen

Umsetzung und Einhaltung von Maßnahmen angemessen dokumentieren

NIS 2: Hilfestellungen des BSI für Unternehmen

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) unterstützt Unternehmen umfassend bei der Umsetzung der NIS2-Richtlinie mit praxisorientierten Werkzeugen, Informationen, Schulungsinhalten und weiteren Angeboten.

NIS 2 Betroffenheitsprüfungstool

#nis2know Infopakete

#nis2know Roadmap

Geschäftsleitungsschulung

Weitere Angebote

Das BSI stellt ein kostenloses Online-Tool bereit, mit dem Unternehmen in wenigen Schritten prüfen können, ob sie von der NIS2-Richtlinie betroffen sind. Der Fragenkatalog ist präzise und orientiert sich direkt an der Richtlinie. Das Ergebnis liefert eine erste, nicht rechtsverbindliche Einschätzung.

NIS 2: Hilfestellungen des BSI für Unternehmen

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) unterstützt Unternehmen umfassend bei der Umsetzung der NIS2-Richtlinie mit praxisorientierten Werkzeugen, Informationen, Schulungsinhalten und weiteren Angeboten.

NIS 2 Betroffenheitsprüfungstool

#nis2know Infopakete

#nis2know Roadmap

Geschäftsleitungsschulung

Weitere Angebote

Das BSI stellt kostenlose Infopakete bereit, um Unternehmen die wichtigsten Informationen zu spezifischen NIS2-Themen kompakt und verständlich zugänglich zu machen. Sie dienen als praktische Stütze für die Umsetzung der gesetzlichen Anforderungen.

Abgedeckte Themen:

- NIS 2 Meldepflicht
- NIS 2Risikoanalyse
- Sichere Lieferkette
- DORA und NIS 2
- BCM
- Geschäftsleitungsschulung

NIS 2: Hilfestellungen des BSI für Unternehmen

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) unterstützt Unternehmen umfassend bei der Umsetzung der NIS2-Richtlinie mit praxisorientierten Werkzeugen, Informationen, Schulungsinhalten und weiteren Angeboten.

NIS 2 Betroffenheitsprüfungstool

#nis2know Infopakete

#nis2know Roadmap

Geschäftsleitungsschulung

Weitere Angebote

Das BSI stellt eine Roadmap bereit, die Unternehmen unterstützt, die NIS2-Anforderungen strukturiert und praxisorientiert umzusetzen. Dazu wird die Umsetzung in Phasen unterteilt, um den Prozess übersichtlich und planbar zu gestalten:

1. Analyse & Grundsatzklärung
2. Organisation & Verantwortung
3. Ist-Zustand & Risikobewertung
4. Ressourcen sichern & Umsetzung vorbereiten
5. Umsetzung Kernmaßnahmen
6. Verstetigung & kontinuierliche Verbesserung

NIS 2: Hilfestellungen des BSI für Unternehmen

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) unterstützt Unternehmen umfassend bei der Umsetzung der NIS2-Richtlinie mit praxisorientierten Werkzeugen, Informationen, Schulungsinhalten und weiteren Angeboten.

NIS 2 Betroffenheitsprüfungstool

#nis2know Infopakete

#nis2know Roadmap

Geschäftsleitungsschulung

Weitere Angebote

Das BSI stellt eine Handreichung bereit (als Teil der #nis2know Infopakete), die eine Orientierung zur Schulungspflicht der Geschäftsleitung nach § 38 Abs. 3 BSIG-E bietet und als Hilfestellung für Schulungsanbieter und Geschäftsleitungen dient.

Exemplarische SOLL-Lerninhalte sind wie folgt:

- „Geschäftsleitungen SOLLEN die übergreifenden **Inhalte und Ziele der NIS-2-Richtlinie** bzw. deren nationaler Umsetzung kennen."
- „Geschäftsleitungen SOLLEN die **Meldepflicht für erhebliche Sicherheitsvorfälle** kennen."
- „Geschäftsleitungen SOLLEN die **mögliche Haftung** der Geschäftsleitungen für schuldhaft verursachte Schäden kennen."
- „Geschäftsleitungen SOLLEN einen Überblick über mögliche **technische und physische Gefährdungen** erhalten."

NIS 2: Hilfestellungen des BSI für Unternehmen

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) unterstützt Unternehmen umfassend bei der Umsetzung der NIS2-Richtlinie mit praxisorientierten Werkzeugen, Informationen, Schulungsinhalten und weiteren Angeboten.

NIS 2 Betroffenheitsprüfungstool

#nis2know Infopakete

#nis2know Roadmap

Geschäftsleitungsschulung

Weitere Angebote

Das BSI bietet weitere Unterstützung für Unternehmen bei der Umsetzung der NIS2-Richtlinie an. Dazu gehören unter anderem Webinare, Veranstaltungen, ein FAQ-Bereich und sektorspezifische Informationen, die praxisnah und hilfreich sind. Diese und weitere Angebote ergänzen die vorhandenen Werkzeuge und Informationsmaterialien und sollen Unternehmen beim Einhalten der neuen Anforderungen unterstützen.

Wir helfen Ihnen bei der Umsetzung von NIS 2.

01 Betroffenheitsanalyse

Identifizierung des Betroffenheitsgrades von Unternehmensbereichen/ Geschäftseinheiten und Festlegung des betroffenen Scopes.

03 NIS-2-Maßnahmenumsetzung

Begleitung bei der effektiven Erfüllung der NIS 2-Richtlinie und der Implementierung aller erforderlichen Maßnahmen und Anforderungen.

05 Berichterstattung an die Behörden

Design des Prozesses zur verpflichtenden Berichterstattung an die entsprechende Aufsichtsbehörde auf Basis bestehender Prozesse und Systeme für das Vorfalls- und Krisenmanagement.

06 Regulatory Monitoring in der Umsetzung

Das Ziel des Regulatory Monitoring ist es, die nationalen Besonderheiten, wie z.B. regulatorische, behördliche Praxis in die Umsetzung einzubringen.

02 Readiness Assessment

Das NIS-2 Readiness-Assessment prüft ab, wie das Unternehmen auf die kommenden Herausforderungen eingestellt ist und welche Maßnahmen noch zu ergreifen sind.

04 NIS-2 Governance

Sicherstellen einer effizienten Steuerung der NIS-2-Maßnahmen zur effektiven Erfüllung der Anforderungen.

07 Workshops und Schulungen

Durchführung von Schulungen und Workshops mit erfahrenen und interdisziplinären Expert:innen.

Digitale Abbildung und Automatisierung auf GRC-Plattformen (z. B. ServiceNow)

KPMG

03

CRA

Cyber Resilience Act

Einführung in den CRA

Warum der CRA?

1. **Mangel an Cybersicherheit bei Produkten**
2. **Unzureichendes Nutzerbewusstsein**

Schäden durch Cyberattacken in DE:
202.4 Milliarden € (2025 - Bitkom)

Effekt des CRA

- Integration von **Cybersicherheit** durch den Hersteller über den **gesamten Produktlebenszyklus**

Entwurf → Produktion → Verkauf → Nutzung

Kennzeichnung

Produkte mit digitalen Elementen sollten mit der **CE-Kennzeichnung** versehen sein, aus der die **Konformität mit dem CRA** hervorgeht.

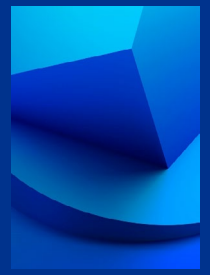
CE

Konformitätsbewertung

Klasse I Kein bis niedriges Risiko ...	…für kritische Infrastrukturen, sensible Daten, lebenswichtige Funktionen	IoT Geräte, Standardsoftware für Endanwender **Keine Konformitätsbewertung durch Dritte notwendig, Selbstbewertung**
Klasse II Moderates bis hohes Risiko ...		Betriebssysteme, Netzwerksicherheitssysteme (Firewalls, VPNs), Software in Industrieanlagen **Konformitätsbewertung durch Dritte benötigt**

Vorteile des CRA

- **Höheres Vertrauen und Datenschutz** für Verbraucher und Partnerunternehmen
- **Vereinfachtes Risikomanagement** durch zertifizierte, sichere Produkte

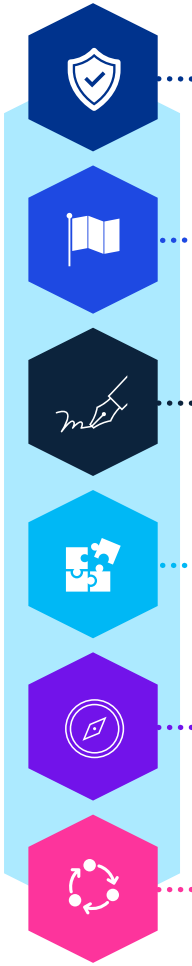


Sanktionen

Für Verstöße gegen Cybersicherheitsanforderungen:

Bis zu **15 Millionen €** oder **2.5%** des weltweiten Umsatzes

Überblick über die Anforderungen des Cyber Resilience Act



Sichere Produktentwicklung: Integration von Sicherheitsmaßnahmen während des gesamten Produktlebenszyklus.

Schwachstellenbearbeitung: Implementation von Mechanismen zur Identifizierung und Minderung von Schwachstellen in Produkten

Incident Reporting: Signifikante Sicherheitsvorfälle (Incidents) innerhalb 24 Stunden melden.

Nachweis der Compliance: Konformität durch (Produkt) Zertifizierungen nachweisen (IEC 62443-4-1 / 4-2, …).

Dokumentation: Bereitstellung von Dokumentationen und Anweisungen für die sichere Nutzung der Produkte.

Sicherheitsupdates: Kostenlose und unverzügliche Bereitstellung von Sicherheitsupdates für mindestens fünf Jahre.

BSI TR-03183: Cyber-Resilienz-Anforderungen

Die BSI TR-03183 ist eine Technische Richtlinie, die Hersteller und Produkte bei der Umsetzung der CRA-Anforderungen unterstützt. Sie bietet praktische Leitlinien und Orientierungshilfen zur Gestaltung sicherer, netzwerkfähiger Produkte.

General Requirements

Definiert fundamentale Anforderungen an Hersteller und Produkte – vom Produktdesign bis zur Support-Phase.

Behandelt:

- Risikobasierte Cybersecurity während des kompletten Produktlebenszyklus
- Security-by-Design und Security-by-Default Prinzipien
- Schwachstellenverwaltung und Updates
- Sichere Entwicklungs- und Produktionsprozesse

Software Bill of Materials (SBOM)

Definiert Anforderungen für maschinenlesbare Stücklisten zur Transparenz der Software-Lieferkette.

Behandelt:

- Definition und Zweck von SBOMs
- Erforderliche Datenfelder und Komponenten-Informationen
- Unterstützte Formate (CycloneDX 1.6+, SPDX 3.0.1+)
- Abhängigkeits- und Lizenzinformationen

Vulnerability Reports and Notifications

Regelt den Coordinated Vulnerability Disclosure (CVD) Prozess für sichere Schwachstellenmeldungen.

Behandelt:

- Sicherheitskontakte und Schwachstellenmeldung (security.txt, CVD-Policy)
- Reaktionszeiten (5 Tage einfach, 10 Tage detailliert)
- Öffentliche Offenlegung im CVD-Prozess
- Zusammenarbeit mit nationalen CSIRTs

Wie Sie sich auf die Regulierung vorbereiten können

Regulierung

Die Regulierung verlangt einen **risikobasierten Ansatz** für die Sicherheit und die Auslieferung **ohne bekannte Schwachstellen**

- **Cyber Resilience Act**
- Radio Equipment Directive
- Machinery Regulation
- Automotive (UNECE R.155)
- Medical Device Regulation
- …

Konformitätsnachweis

Für **kritische Maschinen und Produkte / Komponenten** müssen Sie eine **KBS*** einbeziehen

KBS verlangen von Ihnen **Nachweise zur Konformität**

Um die Konformität nachzuweisen, muss die KBS oder ein neutraler Dritter Ihre **Prozesse und Produkte bewerten**

Empfehlung

Führen Sie einen sicheren Produktentwicklungszyklus auf Basis der **IEC 62443-4-1** oder dessen Ableitungen ein

Unterziehen Sie Ihr Produkt einem **Penetrationstest**, damit Sie alle Defekte rechtzeitig beheben können

Lassen Sie sich **zertifizieren**, um einen **Konformitätsnachweis** zu erhalten und diesen für **Marketingzwecke** verwenden zu können

* KBS = Konformitätsbewertungsstelle

Kontakt

KPMG AG
Wirtschaftsprüfungsgesellschaft

Markus Limbach
Partner
Consulting – Cyber Security & Resilience
T +49 174 3001998
mlimbach@kpmg.com

Frank Damm
Senior Manager
Consulting – Cyber Security & Resilience
T +49 151 65775523
fdamm@kpmg.com

kpmg.de/socialmedia

kpmg.de