asvin

CYBERSECURITY – AKTUELLE EU-REGULATORIK

HERAUSFORDERUNGEN FÜR UNTERNEHMEN AUS NIS2 UND CRA

asvin.io

DISCLAIMER

- Es handelt sich um eine allgemeine Betrachtung der EU Regulatorik zu Cybersicherheit
- Es werden nur allgemeingültige Rechtsakte betrachtet, keine branchenspezifischen Verordnungen
- Irrtümer und Änderungen sind vorbehalten
- Es besteht kein Anspruch auf Vollständigkeit
- Es handelt sich um keine Rechtsberatung.

ALLGEMEINE EINORDNUNG – WAS PASSIERT DA GRADE BEI DER EU?

EU forciert aktuell die Gesetzgebung zur Verbesserung der Cybersicherheit von Unternehmen und Produkten. Das Ziel sind „Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union“. Es sollen verbindliche Regeln für Cybersicherheit EU-weit geschaffen und umgesetzt werden. Um dies zu erreichen, ist eine umfangreiche Gesetzgebungsinitiative der EU zu beobachten. Es werden umfassende Pflichten definiert, bei Nichterfüllung drohen empfindliche Strafen.

DIE AKTUELLEN EU-DIREKTIVEN UND -ACTS IM ÜBERBLICK (1)

IT Sicherheitsgesetz 2.0
→ KRITIS + Unternehmen im besonderem öffentlichen Interesse (UBI)

CRA = CYBER RESILIENCE ACT
→ neue Cybersicherheitsanforderungen für Connected Devices

NIS2 = EU Network and Information Security Directive
→ Festlegung von Cyber Security Mindeststandards für Unternehmen

RCE = RESILIENZ FÜR CRITICAL ENTITIES
→ reguliert die Resilienz von Kritischen Infrastrukturen in der EU

DIE AKTUELLEN EU-DIREKTIVEN UND -ACTS IM ÜBERBLICK (2)

CYBERSECURITY ACT
→ EU Cybersecurity Rahmenwerk für ITK-Produkte und -Dienstleistungen

Data Act
→ EU Regulierung zur Förderung eines wettbewerbsfähigen Datenmarktes

AI Act
→ EU Regulierung des Einsatzes Künstlicher Intelligenz

RED = Radio Equipment Directive
→ Vorschriften für „funkende“ Devices

NIS2 UND CRA - IMPACT AUF DIE DEUTSCHE WIRTSCHAFT

Von den o.g. Richtlinien und Verordnungen werden nach Einschätzung von Cybersecurity Experten die NIS2 Direktive und der Cyber Resilience Act (CRA) die größten Auswirkungen auf die Breite der Unternehmen haben.

NIS2 UND CRA - IMPACT AUF DIE DEUTSCHE WIRTSCHAFT

Auf der einen Seite wegen ihres recht zeitnahen Inkrafttretens und der daraus resultierenden kurzen Vorbereitungszeit, auf der anderen Seite wegen der Betroffenheit einer Vielzahl von Unternehmen, die bisher keiner Cybersecurity-Regulierung unterworfen waren.

NIS2 UND CRA - IMPACT AUF DIE DEUTSCHE WIRTSCHAFT

Das Impact Assessment der EU Kommission hat allein zu NIS2 ergeben, dass durch den erhöhten Aufwand bei der Einführung und Umsetzung des Rechtsaktes bei neu betroffenen Unternehmen mit einer Erhöhung des Cybersicherheitsbudgets in Höhe von ca. 22 Prozent zu rechnen ist.

NIS2 = RICHTLINE / DIREKTIVE
MUSS VON DEN EU MITGLIEDSSTAATEN IN NATIONALES RECHT UMGESETZT WERDEN.

Die NIS-2-Richtlinie wurde am 27.12.2022 im Amtsblatt L333 der Europäischen Union veröffentlicht. Sie trat am zwanzigsten Tag nach ihrer Veröffentlichung in Kraft. Die Mitgliedstaaten müssen die Richtlinie innerhalb von 21 Monaten (bis 17.10.2024) nach ihrem Inkrafttreten in nationales Recht umsetzen.

REFERENTENENTWURF FÜR DAS „NIS2UmsuCG“

Referentenentwurf des Bundesministeriums des Innern, für Bau und Heimat

Entwurf eines Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung (NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz – NIS2UmsuCG)[1]

Vom ...

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
0		**Artikel 1** **Änderung des BSI-Gesetzes**	
1	Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz – BSIG)[2]	Gesetz über das Bundesamt für Sicherheit in der Informationstechnik und über die Sicherheit in der Informationstechnik von Betreibern und Einrichtungen (BSI-Gesetz – BSIG)	Berücksichtigung des Umstands, dass es sich nicht mehr um ein reines Errichtungsgesetz einer Bundesbehörde handelt.
2	Nichtamtliches Inhaltsverzeichnis § 1 Bundesamt für Sicherheit in der Informationstechnik § 2 Begriffsbestimmungen § 3 Aufgaben des Bundesamtes § 3a Verarbeitung personenbezogener Daten § 4 Zentrale Meldestelle für die Sicherheit in der Informationstechnik des Bundes	Inhaltsübersicht Teil 1 Allgemeine Vorschriften § 1 Bundesamt für Sicherheit in der Informationstechnik § 2 Begriffsbestimmungen Teil 2 Das Bundesamt	Schaffung einer (amtlichen) Inhaltsübersicht aufgrund des gestiegenen Umfangs des Gesetzes sowie Strukturierung des Gesetzes in Teile (und Kapitel) zur besseren Übersicht für den Rechtsanwender.

INKRAFTTRETEN DES „NIS2UmsuCG“

999		**Artikel 15** **Inkrafttreten**	
1000		(1) Dieses Gesetz tritt vorbehaltlich des Absatzes 2 am 1. Oktober 2024 in Kraft.	Bei einer Verkündung im März 2024 stehen den Einrichtungen noch sechs Monate für die Umsetzung der in diesem Gesetz enthaltenen Verpflichtungen zur Verfügung. Der hier genannte Zeitpunkt ist der letzte Quartalsbeginn vor Ablauf der Umsetzungsfrist des Artikel 41 NIS-2-Richtlinie am 17. Oktober 2024. Im Übrigen sind die für die Verpflichtungen von wesentlichen und wichtigen Einrichtungen maßgeblichen Inhalte der NIS-2-Richtlinie bereits seit dem Kommissionsentwurf aus Dezember 2020 bekannt.
1001		(2) Artikel 2 tritt am Tag nach der Verkündung in Kraft.	Die überarbeitete Ermächtigung zum Erlass einer Rechtsverordnung nach § 10 Abs. 1b BSIG muss bereits zuvor in Kraft treten, damit diese zum Tag des Inkrafttretens des Gesetzes im Übrigen bereits erlassen sein kann.

* * *

CRA = VERORDNUNG / ACT
GILT UNMITTELBAR IN ALLEN MITGLIEDSSTAATEN

Proposal der EU Kommission wurde am 15.09.2022 veröffentlicht. Der CRA ist als produktbezogene Verordnung geplant und befindet sich derzeit im Trilog zwischen EU-Kommission, EU-Parlament und Rat. Eine Umsetzung in nationales Recht ist nicht erforderlich, allerdings ist eine Übergangsfrist von bis zu 36 Monaten vorgesehen. Ziel der EU ist es, dass der CRA noch vor der Europawahl im Frühjahr 2024 in Kraft tritt.

NIS 2

NIS2 enthält umfassende Cybersicherheitspflichten für Unternehmen mit mehr als 50 Mitarbeitern und einem Jahresumsatz oder einer Jahresbilanzsumme von mehr als 10 Millionen Euro, wenn das Unternehmen einem kritischen Sektor (Anhang I und II) angehört und in der EU Dienstleistungen erbringt oder Tätigkeiten ausübt.

NIS 2

Darüber hinausgehend gilt NIS-2 auch unabhängig von der Größe eines Unternehmens oder einer Einrichtung, soweit bestimmte qualifizierende Voraussetzungen erfüllt sind.

NIS 2

Es wird erwartet, dass allein in Deutschland über 11.000 Unternehmen des Maschinen- und Anlagenbaus zusätzlich betroffen sind, indem sie zukünftig der „kritischen Infrastruktur“ zugeordnet werden.

(Quelle: VDMA)

CRA

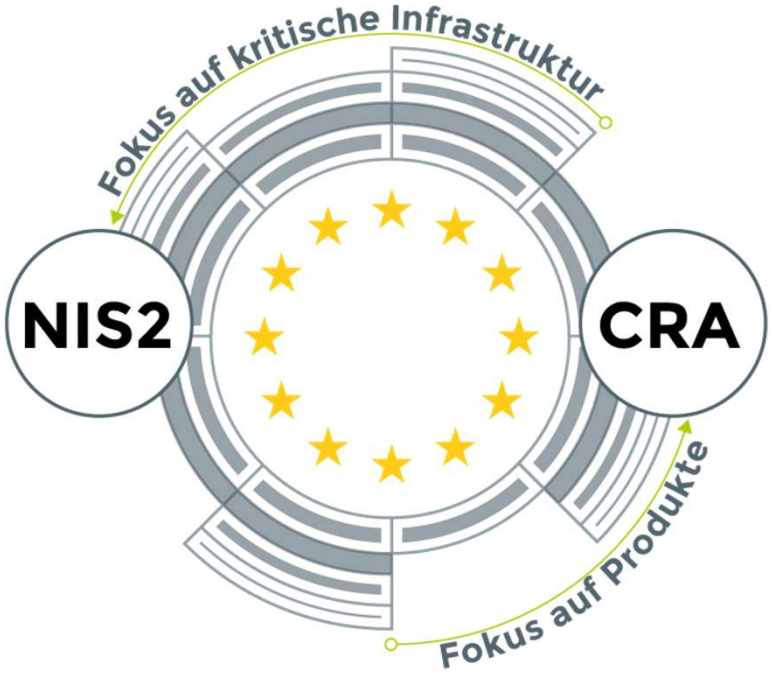
Der CRA enthält umfassende Cybersicherheitspflichten für alle Unternehmen, die Produkte mit digitalen Komponenten (drahtlos oder drahtgebunden) sowie dazugehörige Nebenleistungen im EU-Raum anbieten.

Im Sinne des Grundsatzes „Security by Design“ sollen die Anforderungen aus dem CRA den gesamten Lebenszyklus eines Produktes abdecken.

CRA

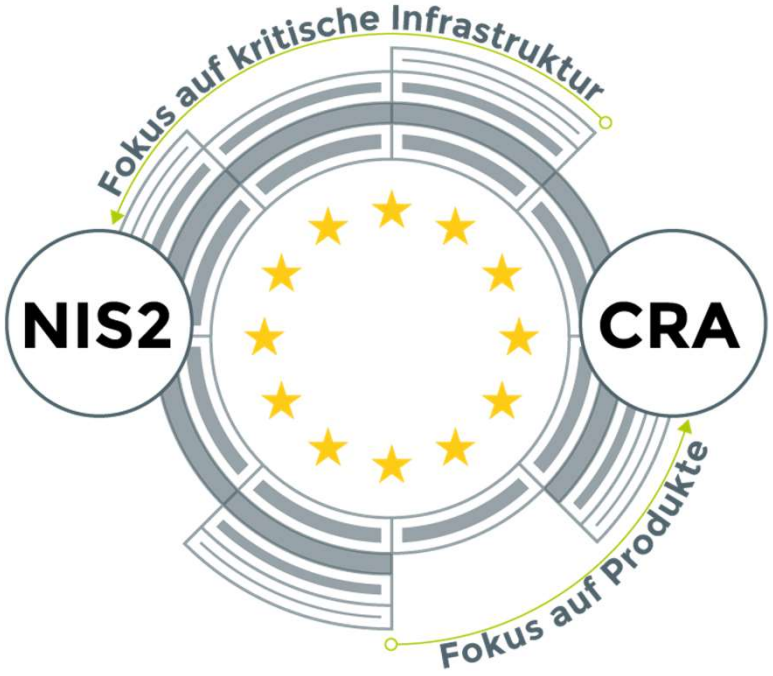
Ausnahmen gelten nur für bestimmte Branchen (z.B. Automotive, Defence, Medizinprodukte) die eh schon von spezifischen Branchennormen betroffen sind.

UNTERSCHIEDE NIS2 UND CRA



NIS-2 richtet sich an Unternehmen und deren Cybersicherheit. Die Direktive betrifft innerbetriebliche Vorgänge zur Cybersicherheit aber auch physischen Sicherheit, hat also zum Thema, wie ich ein Unternehmen schütze.

UNTERSCHIEDE NIS2 UND CRA



CRA betrifft primär digitale Produkte, sogenannte Connected Devices und deren Hersteller oder EU-Inverkehrbringer.

Inhalt des CRA ist also, ob die digitalen Produkte und Dienste, die ich meinen Kunden anbiete, cybersicher sind.

NIS2 – EIN ÜBERBLICK (73 SEITEN)

Die NIS2-Richtlinie adressiert
die Cybersecurity der Netz- und Informationssysteme unter eigener Verantwortung. Darunter fallen unter anderem die eigene Netzwerkinfrastruktur, interne IT-Systeme, Anwendungssysteme, Digitale Dienste, IT-basierte Dienste gegenüber Dritten und industrielle Steuerungssysteme.

NIS2 – EIN ÜBERBLICK

Die wichtigsten Punkte des aktuellen Entwurfs
der NIS2-Richtlinie sind:

- Adressierung der Netz- und Informationssysteme unter eigener Verantwortung
- Erwerb ausreichender Risikomanagement-Kenntnisse in der Geschäftsführung Berücksichtigung von Security bei der Beschaffung von Systemen, Diensten
- Einhaltung von technisch, organisatorischen Maßnahmen im Betrieb
- Erhalt des beabsichtigten Sicherheitsniveaus über die Nutzungszeit
- Meldung erheblicher Sicherheitsvorfälle an zuständige Behörden innerhalb von 24h

BESONDERHEITEN

Die Geschäftsführung muss sicherstellen, dass ein angemessenes Risikomanagement für Systeme und Anwendungen etabliert wird. Dafür muss die Geschäftsführung in Zukunft ausreichende Kenntnisse und Fähigkeiten zur Erkennung und Bewertung von Risiken und deren Auswirkungen auf den Geschäftsbetrieb verpflichtend erwerben.

BESONDERHEITEN

Die Geschäftsführung wird persönlich haftbar gemacht werden können für eine nicht vollumfängliche Implementierung der Cybersicherheitsmaßnahmen und kann in besonders gravierenden Fällen auch von der nationalen Aufsichtsbehörde von ihren Funktionen entbunden werden.

BESONDERHEITEN

Die technischen und organisatorischen Maßnahmen, die zur Absicherung der Netz- und Informationssysteme umgesetzt werden, müssen den Risiken entsprechend angemessen sein und dem Stand der Technik entsprechen.

ANFORDERUNGEN (1/4)

Die Richtlinie setzt einen engen Rahmen, folgende Mindestmaßnahmen müssen betrachtet werden:

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

ANFORDERUNGEN (2/4)

- 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 Netz- und Informationssystemen, einschließlich Management und Offenlegung von Schwachstellen;
- Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen im Bereich der Cybersicherheit.

ANFORDERUNGEN (3/4)

- grundlegende Verfahren im Bereich der Cyberhygiene und Schulungen im Bereich der Cybersicherheit;
- Konzepte und Verfahren für den Einsatz von Kryptografie und gegebenenfalls Verschlüsselung;
- Sicherheit des Personals, Konzepte für die Zugriffskontrolle und Management von Anlagen;
- Verwendung von Lösungen zur Multi-Faktor-Authentifizierung oder kontinuierlichen Authentifizierung

ANFORDERUNGEN (4/4)

- gesicherte Sprach-, Video- und Textkommunikation sowie gegebenenfalls gesicherte Notfallkommunikationssysteme innerhalb der Einrichtung.

Insbesondere werden Unternehmen angehalten, die Cybersecurity bereits bei der Beschaffung von Netz- und Informationssystemen zu berücksichtigen.
Es ist nicht auszuschließen, dass in Bezug auf die Beschaffung ausgewählte Dienste und Systeme Zertifizierungsanforderungen unterliegen werden.

BERICHTSPFLICHTEN UND GELDBUßEN

Über jeden Sicherheitsvorfall, der erhebliche Auswirkungen auf die Erbringung ihrer Dienste gemäß Absatz 3 (erheblicher Sicherheitsvorfall) hat, muss die zuständige Behörde unverzüglich unterrichtet werden. Spätestens hat dies innerhalb von 24 Stunden zu geschehen, ab dem Zeitpunkt, an dem das Unternehmen Kenntnis von dem Sicherheitsvorfall erlangt hat.
Ebenso haben die die betreffenden Einrichtungen die Empfänger ihrer Dienste unverzüglich über diese erheblichen Sicherheitsvorfälle zu unterrichten, die die Erbringung des jeweiligen Dienstes beeinträchtigen könnten.

BERICHTSPFLICHTEN UND GELDBUßEN

Nach 72 Stunden ist der zuständigen Behörde ein erster Zwischenbericht vorzulegen, in dem eine Aktualisierung der in der Frühwarnung enthaltenen Informationen und erste Bewertung des erheblichen Sicherheitsvorfalls, einschließlich seines Schweregrads und seiner Auswirkungen, abgegeben wird.

BERICHTSPFLICHTEN UND GELDBUßEN

Geldbußen haben einen Höchstbetrag von 10.000.000 € oder einen Höchstbetrag von mindestens 2 % des gesamten weltweiten, im vorangegangenen Geschäftsjahr, getätigten Umsatzes des Unternehmens, dem die wesentliche Einrichtung angehört, je nachdem, welcher Betrag höher ist.

CRA – EIN ÜBERBLICK (87 SEITEN)

Der CRA adressiert produktübergreifende, europäisch vereinheitlichte und lebenszyklusbezogene Anforderungen an die Cybersicherheit von Produkten mit digitalen Komponenten (Connected Devices) und zugehöriger Nebendienstleistungen, die im EU-Raum angeboten werden.

BESONDERHEITEN

Erstmalig geht ein EU-Gesetz explizit auf den Schutz von Software-Lieferketten ein. Weiterhin wird verpflichtend geregelt werden, über welchen Zeitraum für ein Produkt Updates zur Verfügung gestellt werden müssen. Dies setzt voraus, dass das Produkt updatefähig ist und ein Software-Update-Management-System (SUMS), wie wir es u.a. aus der Automobilindustrie kennen (UN ECE R156), implementiert werden muss.

Je nach Kritikalität des Produktes werden verschiedene Stufen definiert, die „normale“, „kritische“ und „hochkritische“ Devices unterscheidet.

BESONDERHEITEN

Die Erklärung, dass ein Produkt den Anforderungen des CRA entspricht, soll in die CE-Erklärung des Produktes einfließen. Das bedeutet, dass es sich im Wesentlichen um eine Eigenerklärung des Unternehmens handelt, dass seine Produkte und zugehörigen Dienstleistungen den Forderungen des CRA entsprechen. Nur bei „hochkritischen“ Devices ist ein externes Auditverfahren vorgesehen. Dies läuft in der Praxis darauf hinaus, dass der Unternehmer gegenüber der entsprechenden Behörde (ENISA) erklären muss, dass im definierten Servicezeitraum bei seinem Produkt keine Cyber-Risiken auftreten.

ANFORDERUNGEN

Der CRA unterteilt die sich aus der Verordnung ergebenden Pflichten in „Anforderungen an Hersteller“, „Anforderungen an Importeure“ und „Anforderungen an Distributoren“.

Alle müssen die Konformität des Produktes mit digitalen Komponenten (Connected Device) mit den Anforderungen des CRA gegenüber der Behörde (ENISA) erklären. Dies soll innerhalb der CE-Konformitätserklärung geschehen.

ANFORDERUNGEN

Es soll sichergestellt werden und es muss erklärt werden, dass ein Connected Device über seinen Produktlebenszyklus oder mindestens über einen Zeitraum von 5/7 Jahren Cybersicher betrieben werden kann. Werden Schwachstellen entdeckt, müssen diese berichtet und behoben werden. Dafür ist in der praktischen Umsetzung ein Secure Update Management System (SUMS) notwendig. Hierbei muss dargelegt und dokumentiert werden, wie sichergestellt wird, dass der Software-Update-Prozess sicher gestaltet ist.

BERICHTSPFLICHTEN UND GELDBUßEN

Über jede entdeckte Schwachstelle, die Auswirkungen auf die Sicherheit des Produktes hat, muss die zuständige Behörde (ENISA) unverzüglich unterrichtet werden. Spätestens hat dies innerhalb von 24 Stunden zu geschehen, ab dem Zeitpunkt, an dem das Unternehmen Kenntnis von dem Sicherheitsvorfall erlangt hat.

BERICHTSPFLICHTEN UND GELDBUßEN

Ebenso haben die die Hersteller oder Inverkehrbringer ihre Kunden unverzüglich über diese erheblichen Schwachstellen zu unterrichten. Sowohl bei der Meldung an die ENISA als auch im Rahmen der Kundeninformation müssen die Schwachstelle beschrieben sein und Maßnahmen zur Abwehr oder Vermeidung von schädlichen Auswirkungen benannt werden.

BERICHTSPFLICHTEN UND GELDBUßEN

Die Nichterfüllung von essentiellen Cybersecurity-Anforderungen an ein Produkt kann mit Geldbußen bis zu einem Höchstbetrag von 15 000 000 € oder einem Höchstbetrag von mindestens 2,5 % des gesamten weltweiten im vorangegangenen Geschäftsjahr getätigten Umsatzes des Unternehmens, dem die wesentliche Einrichtung angehört, je nachdem, welcher Betrag höher ist, geahndet werden.

Bei der Nichterfüllung von „nicht essentiellen“ Anforderungen verringern sich die Geldbußen auf 10 Mio. bzw. 2% des Umsatzes.

ZUSAMMENFASSUNG

Eines wird klar: Die EU meint es ernst mit der Cybersecurity-Gesetzgebung und 2024 wird das Cybersecurity-Jahr dieses Jahrzehnts werden. Der Impact der neuen nationalen und europäischen Regulatorik wird definitiv mit den Auswirkungen des Wirksamwerdens der DSGVO in 2018 vergleichbar sein.

ZUSAMMENFASSUNG

Der Zeitrahmen bis zum Inkrafttreten der nationalen und europäischen Regulatorik ist schon jetzt absehbar knapp bemessen, wenn man bedenkt, dass die Einführung entsprechender Prozesse sowie organisatorischer und technischer Maßnahmen mindestens ein Jahr, in größeren Organisationen auch gut 18 Monate dauern kann.

ZUSAMMENFASSUNG

Umso wichtiger, schon jetzt präventiv vorzusorgen und sich richtig zu informieren!

In einem individuellen Workshop erläutern wir gern mehr Details, können Ihren „Readiness-Level“ analysieren und klare Handlungsempfehlungen für eine „Regulatory-Compliance“ geben.

NÜTZLICHE LINKS:

NIS2 Quickcheck:	https://www.surveymonkey.de/r/KMPC72T
CRA Quickcheck:	https://www.surveymonkey.de/r/asvinCRA
asvin CRA Seite:	https://asvin.io/cyber-resilience-act/
asvin NIS2 Seite:	https://asvin.io/eu-nis-2/
Workshop Landing Page:	https://asvin.io/eu-nis-2/eu-nis-2-workshop/

Vielen Dank für Ihr Interesse!

asvin GmbH
Stuttgart, Germany
www.asvin.io

contact@asvin.io

asvin.io