iStock.com/Riuma72

NIS2-Richtlinie und Umsetzung ins Deutsche Recht – was Sie jetzt tun müssen!

Dr. Lutz Martin Keppeler

1.03.2024

Überblick über neue EU-Digitalrecht

Data Act
(in Kraft)
Regelungen für die Nutzung von Daten

KI-Verordnung
(Trilog abgeschlossen)
Regulierung von KI-Anwendungen

Cyber Resilience Act
(Trilog abgeschlossen)
Umfassende Sicherheitsanforderungen
für Produkte mit digitalen Elementen

Digital Services Act
(in Kraft)
Schutz für die Nutzer digitaler Dienste (insbesondre Plattformen)

Data Governance Act
(in Kraft)
Anforderungen für den Datenaustausch

Digital Operational Resilience Act (DORA)
(in Kraft)
Bereichsspezifische Cybersecurity-Compliance

NIS-2-Richtlinie (in Kraft) **und BSIG-neu** (Entwurf)

- Neue Pflichten für KRITIS-Betreiber
- Mehr betroffene Unternehmen
- Mehr Befugnisse für das BSI
- Sanktionen und Verbraucherschutz

NIS-2-Richtlinie und das BSIG-neu

iStock.com/Nikada

Cyber Resilience Act: Key Facts

3. Referentenentwurf:
27. September 2023

Status:
In Verhandlung

Umsetzungsfrist:
17. Oktober 2024

Geplante Verkündigung:
Termin verschoben

Betrifft:

- Informations-sicherheits-Management
- Organisatorische Prozesse
- Technische Prozesse
- Netzwerk-Infrastruktur

Pflichten für:
Wichtige und besonders wichtige Einrichtungen

Befugnisse für:
Aufsichtsbehörden

Bußgelder
Bis zu 7 bzw. 10 Mio. EUR oder 1,4% bzw. 2 % des weltweiten Vorjahresumsatzes

Sanktionen
durch zuständige Behörde

BSIG und KRITIS galt bislang für Exoten

BSIG gilt bisher für

- Unternehmen aus definierten Branchen: Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung, Finanz- und Versicherungswesen sowie Siedlungsabfallentsorgung **und** von hoher Bedeutung für das Funktionieren des Gemeinwesens sind
  - Schwellwerte in BIS-KRITISV
- Unternehmen im besonderen öffentlichen Interesse (UBI) sind Unternehmen, die nicht Betreiber Kritischer Infrastrukturen sind
  - Unternehmen, die Wehrtechnik oder IT-Sicherheitsprodukte für staatliche Einrichtungen herstellen (Verschlusssachen)
  - DAX-Konzerne
  - die Betreiber eines Betriebsbereichs der oberen Klasse im Sinne der Störfall-Verordnung
- Digitale Dienste
  - Online-Marktplätze
  - Online-Suchmaschinen
  - Cloud-Computing-Dienste

Verpflichtungen aus dem aktuellen BSIG

Verpflichtungen nach BSIG

- angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit
  - Berücksichtigung des Standes der Technik
  - In Einzelfällen Detailvorgaben
  - Für KRITIS-Betreiber „B3S“ Kataloge
- Nur KRITIS- Betreibern: Nachweispflicht der Einhaltung
  - Typischerweise ISO 27001 + Nachweis nach § 8a Abs. 3 BSIG
- Meldepflichten bei Vorfall

Anwendungsbereich NIS2 (und BSIG-neu?)

Anhang I NIS2 „Sektoren mit hoher Kritikalität“

Kritikalitätsschwelle NIS2 „unabhängig von der Größe, wenn.....“

Unterscheidung in NIS2 „Wesentliche und wichtige Einrichtungen“ (z.B. Abhängig von der Größe des Unternehmens)

Energie

Transport und Verkehr

Finanz- und Versicherungs-wesen

Gesundheit

Wasser und Abwasser

Informationstechnik & Telekommunikation

Weltraum

Verwaltung von IKT-Diensten

Im letzten Diskussionspapier nicht enthalten

Anhang II NIS2 „Sonstige kritischen Sektoren“

Kritikalitätsschwelle NIS2 „unabhängig Von der Größe, wenn.....“

Unterscheidung in BISG „Besonders wichtig und wichtige Einrichtungen“ (z.B. Abhängig von der Größe des Unternehmens)

Logistik

Siedlungsabfall -entsorgung

Produktion, Herstellung und Handel mit chemischen Stoffen

Produktion, Verarbeitung und Vertrieb von Lebensmitteln

Verarbeitendes Gewerbe/Her-stellung von Waren

Anbieter digitaler Dienste

Forschung

Anwendungsbereich NIS2 Artikel 2 (Auszug)

(2) Unabhängig von der Größe der Einrichtungen gilt diese Richtlinie auch für Einrichtungen der in den Anhang I oder II genannten Art, wenn

a) die Dienste erbracht werden von:

   i) Anbietern von öffentlichen elektronischen Kommunikationsnetzen oder von öffentlich zugänglichen elektronischen Kommunikationsdiensten;

   ii) Vertrauensdiensteanbietern;

   iii) Namenregistern der Domäne oberster Stufe und Domänennamensystem-Diensteanbietern;

b) es sich bei der Einrichtung in einem Mitgliedstaat um den einzigen Anbieter eines Dienstes handelt, der für die Aufrechterhaltung kritischer gesellschaftlicher oder wirtschaftlicher Tätigkeiten unerlässlich ist;

c) sich eine Störung des von der Einrichtung erbrachten Dienstes wesentlich auf die öffentliche Ordnung, die öffentliche Sicherheit oder die öffentliche Gesundheit auswirken könnte;

d) eine Störung des von der Einrichtung erbrachten Dienstes zu einem wesentlichen Systemrisiko führen könnte, insbesondere in Sektoren, in denen eine solche Störung grenzübergreifende Auswirkungen haben könnte;

e) die Einrichtung aufgrund der besonderen Bedeutung, die sie auf nationaler oder regionaler Ebene für den betreffenden Sektor oder die betreffende Art des Dienstes oder für andere voneinander abhängige Sektoren in dem Mitgliedstaat hat, kritisch ist;

f) die Einrichtung eine Einrichtung der öffentlichen Verwaltung:

Anwendungsbereich NIS2 Artikel 3 (Auszug)

Artikel 3

Wesentliche und wichtige Einrichtungen

(1) Für die Zwecke dieser Richtlinie gelten als wesentliche Einrichtungen:

a) Einrichtungen der in Anhang I aufgeführten Art, die die in Artikel 2 Absatz 1 des Anhangs der Empfehlung 2003/361/EG genannten Schwellenwerte für mittlere Unternehmen überschreiten;

b) qualifizierte Vertrauensdiensteanbieter und Domänennamenregister der Domäne oberster Stufe sowie DNS-Diensteanbieter, unabhängig von ihrer Größe;

c) Anbieter öffentlicher elektronischer Kommunikationsnetze oder öffentlich zugänglicher elektronischer Kommunikationsdienste, die nach Artikel 2 des Anhangs der Empfehlung 2003/361/EG genannten als mittlere Unternehmen gelten;

d) Einrichtungen der öffentlichen Verwaltung nach Artikel 2 Absatz 2 Buchstabe f Ziffer i;

(2) Für die Zwecke dieser Richtlinie gelten Einrichtungen der in Anhang I oder II aufgeführten Art, die nicht als wesentliche Einrichtungen im Sinne von Absatz 1 des vorliegenden Artikels gelten, als wichtige Einrichtungen. Dies schließt Einrichtungen ein, die von den Mitgliedstaaten gemäß Artikel 2 Absatz 2 Buchstaben b bis e als wichtige Einrichtungen eingestuft wurden.

(3) Bis zum 17. April 2025 erstellen die Mitgliedstaaten eine Liste von wesentlichen und wichtigen Einrichtungen und von Einrichtungen, die Domänennamen-Registrierungsdienste erbringen. Die Mitgliedstaaten überprüfen diese Liste danach regelmäßig, mindestens jedoch alle zwei Jahre, und aktualisieren sie gegebenenfalls.

Anwendungsbereich BSIG-neu § 28

(6) Eine besonders wichtige Einrichtung ist

1. ein Großunternehmen, das einer der durch Rechtsverordnung nach § 57 Absatz 1 bestimmten Einrichtungsarten der Sektoren Energie, Transport und Verkehr, Finanz- und Versicherungswesen, Gesundheitswesen, Trinkwasser, Abwasser, Informationstechnik und Telekommunikation, Verwaltung von IKT-Diensten (Business-to-Business) oder Weltraum zuzuordnen ist,

2. ein qualifizierter Vertrauensdiensteanbieter, Top Level Domain Name Registries oder DNS-Diensteanbieter, jeweils unabhängig von der Unternehmensgröße,

3. ein mittleres Unternehmen, das Anbieter von Telekommunikationsdiensten oder öffentlich zugänglichen Telekommunikationsnetzen ist,

4. ein Betreiber kritischer Anlagen oder

5. eine Einrichtung, die gemäß Rechtsverordnung nach § 57 Absatz 1 dem Teilsektor Zentralregierung des Sektors öffentliche Verwaltung angehört,

BSIG-neu: Vergleich der Schwellenwerte

NIS-2-Richtlinie:

Großunternehmen:

>249 Mitarbeiter und >50 Mio. EUR Jahresumsatz oder >43 Mio. EUR Jahresbilanzsumme

Mittlere Unternehmen:

Müssen den Schwellenwert für „mittlere Unternehmen“ einhalten, d.h.:

50-249 Mitarbeiter und 10-50 Mio. EUR Jahresumsatz oder 10-43 Mio. EUR Jahresbilanzsumme

BSIG-neu:

Großunternehmen:

> 249 Mitarbeiter oder mind. 50 Mio. EUR Jahresumsatz und zudem mind. 43 Mio. EUR Jahresbilanzsumme

Mittlere Unternehmen:

Mind. 50 und höchstens 249 Mitarbeiter und weniger als 50 Mio. EUR Jahresumsatz oder weniger als 43 Mio. EUR Jahresbilanzsumme

oder:

Weniger als 50 Mitarbeiter und Jahresumsatz und Jahresbilanzsumme von jeweils 10 Mio. EUR und einen Jahresumsatz von höchstens 50 Mio. EUR und eine Bilanzsumme von höchstens 43 Mio. EUR.

Mindestanforderungen des BSIG-neu und NIS2

Artikel 21

Risikomanagementmaßnahmen im Bereich der Cybersicherheit

(1) Die Mitgliedstaaten stellen sicher, dass wesentliche und wichtige Einrichtungen geeignete und verhältnismäßige technische, operative und organisatorische Maßnahmen ergreifen, um die Risiken für die Sicherheit der Netz- und Informationssysteme, die diese Einrichtungen für ihren Betrieb oder für die Erbringung ihrer Dienste nutzen, zu beherrschen und die Auswirkungen von Sicherheitsvorfällen auf die Empfänger ihrer Dienste und auf andere Dienste zu verhindern oder möglichst gering zu halten.

§ 30

Risikomanagementmaßnahmen

(1) Besonders wichtige Einrichtungen und wichtige Einrichtungen sind verpflichtet, geeignete, verhältnismäßige und wirksame technische und organisatorische Maßnahmen zu ergreifen, um Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit der informationstechnischen Systeme, Komponenten und Prozesse, die sie für die Erbringung ihrer Dienste nutzen, zu vermeiden und Auswirkungen von Sicherheitsvorfällen auf ihre oder andere Dienste zu verhindern oder möglichst gering zu halten.

Anforderungen des BSIG-neu und NIS2

Mindestanforderungen, § 30 Abs. 4 BSIG-neu und Art 21 NIS2

- Konzepte in Bezug auf die Risikoanalyse und Sicherheit für Informationssysteme (**Sicherheitskonzepte**)
- Maßnahmen zur **Bewältigung von Sicherheitsvorfällen**
- Maßnahmen zur **Aufrechterhaltung des Betriebs** (Backup-Management und die Notfall-Wiederherstellung von Daten, Krisenmanagement)
- **Sicherheit der Lieferkette** und Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von Netz- und Informationssystemen (einschließlich Management und Offenlegung von Schwachstellen)
- Konzepte und Verfahren zur **Bewertung der Wirksamkeit** der Risikomanagementmaßnahmen im Bereich Cybersicherheit
- Grundlegende Verfahren im Bereich der **Cyberhygiene** und **Schulungen** im Bereich Cybersicherheit
- Konzepte und Verfahren für den Einsatz von **Kryptografie** und ggfs. **Verschlüsselung**
- **Sicherheit des Personals**, Konzepte für die **Zugriffskontrolle** und Management von Anlagen
- Verwendung von Lösungen zur **Multi-Faktor-Authentifizierung** oder kontinuierlichen Authentifizierung, gesicherte Sprach-, Video- und Text-kommunikation sowie ggfs. gesicherte Notfallkommunikationssysteme

BSIG-neu und ISO 27001 im Vergleich

Anforderungen des BSIG-neu	Controls nach ISO 27001
Konzepte in Bezug auf die **Risikoanalyse** und Sicherheit für Informationssysteme	5.2 Politik 6.1.2 Informationssicherheitsrisikobeurteilung 6.1.3 Informationssicherheitsrisikobehandlung 8.2 Informationssicherheitsrisikobeurteilung 8.3 Informationssicherheitsrisikobehandlung Anhang A 5.1 Informationssicherheitsrichtlinien
Bewältigung von **Sicherheitsvorfällen**	Anhang A 5.24 Planung und Vorbereitung der Handhabung von Informationssicherheitsvorfällen 5.25 Beurteilung und Entscheidung über Informationssicherheitsereignisse 5.26 Reaktion auf Informationssicherheitsvorfälle 5.27 Erkenntnisse aus Informationssicherheitsvorfällen 5.28 Sammeln von Beweismaterial 6.8 Meldung von Informationssicherheitsereignissen

BSIG-neu und ISO 27001 im Vergleich

Anforderungen des BSIG-neu	Controls nach ISO 27001
Aufrechterhaltung des Betriebs, wie Backup-Management und **Wiederherstellung** nach einem Notfall, und **Krisenmanagement**	Anhang A 5.29 Informationssicherheit bei Störungen 5.30 IKT-Bereitschaft für Business Continuity 8.13 Sicherung von Information 8.14 Redundanz von informationsverarbeitenden Einrichtungen
Sicherheit der Lieferkette einschließlich sicherheitsbezogener Aspekte der Beziehungen zwischen den einzelnen Einrichtungen und ihren unmittelbaren Anbietern oder Diensteanbietern	Anhang A 5.19 Informationssicherheit in Lieferantenbeziehungen 5.20 Behandlung von Informationssicherheit in Lieferantenvereinbarungen 5.21 Umgang mit der Informationssicherheit in der Lieferkette der Informations- und Kommunikationstechnologie (IKT) 5.22 Überwachung, Überprüfung und Änderungsmanagement von Lieferantendienstleistungen 5.23 Informationssicherheit für die Nutzung von Cloud-Diensten

BSIG-neu und ISO 27001 im Vergleich

Anforderungen des BSIG-neu	Controls nach ISO 27001	
Sicherheitsmaßnahmen bei **Erwerb, Entwicklung und Wartung von informationstechnischen Systemen**, Komponenten und Prozessen, einschließlich Management und **Offenlegung von Schwachstellen**	Anhang A 5.37 8.8 8.9 8.20 8.21	 Dokumentierte Bedienabläufe Handhabung von technischen Schwachstellen Konfigurationsmanagement Netzwerksicherheit Sicherheit von Netzwerkdiensten
Konzepte und Verfahren zur **Bewertung der Wirksamkeit** von Risikomanagementmaßnahmen im Bereich der Cybersicherheit	9.1 9.2 9.3 Anhang A 5.35	Überwachung, Messung, Analyse und Bewertung Internes Audit Managementbewertung Unabhängige Überprüfung der Informationssicherheit
grundlegende Verfahren im Bereich der Cyberhygiene und Schulungen im Bereich der Cybersicherheit	7.3 7.4 Anhang A 6.3	Bewusstsein Kommunikation Informationssicherheitsbewusstsein, -ausbildung und -schulung

BSIG-neu und ISO 27001 im Vergleich

Anforderungen des BSIG-neu	Controls nach ISO 27001
Konzepte und Verfahren für den Einsatz von Kryptografie und Verschlüsselung	Anhang A 8.24 Verwendung von Kryptographie
Sicherheit des Personals, Konzepte für die Zugriffskontrolle und Management von Anlagen	Anhang A 5.9 Inventar der Informationen und anderen damit verbundenen Werten 5.10 Zulässiger Gebrauch von Informationen und anderen damit verbundenen Werten 5.15 Zugangssteuerung 5.16 Identitätsmanagement 5.17 Informationen zur Authentifizierung 5.18 Zugangsrechte 6.1 Sicherheitsüberprüfung 6.2 Beschäftigungs- und Vertragsbedingungen 6.4 Maßregelungsprozess 6.5 Verantwortlichkeiten nach Beendigung oder Änderung der Beschäftigung 6.6 Vertraulichkeits- oder Geheimhaltungsvereinbarungen

BSIG-neu und ISO 27001 im Vergleich

Anforderungen des BSIG-neu

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

Controls nach ISO 27001

Anhang A

5.14	Informationsübertragung
5.16	Identitätsmanagement
5.17	Informationen zur Authentifizierung

NIS2 und BSIG-neu: Geschäftsleitungspflichten

Pflichten der Geschäftsleitung

- Pflicht zur **Einführung, Billigung und Überwachung der Umsetzung der Risikomanagement-maßnahmen**
- Pflicht zur **Teilnahme an Schulungen** im Bereich Cybersicherheit

Sanktionen gegenüber der Geschäftsleitung

- **Persönliche Haftung:** Leitungspersonal soll für Verstöße gegen Geschäftsleitungspflichten verantwortlich sein und gegenüber Einrichtung haften (ohne Möglichkeit auf Verzicht oder Vergleich)
- Schadensbegriff soll Regressansprüche und **Bußgeldforderungen** erfassen
- Befugnis der Behörden zur vorübergehenden Untersagung der Wahrnehmung von Leitungsaufgaben, falls Durchsetzungsmaßnahmen nicht oder nicht wirksam umgesetzt werden (nur bei wesentlichen Einrichtungen!)

Konsequenz: Cyber-Security ist Aufgabe der Geschäftsleitung!

Sanktionen

§ 60

Sanktionsvorschriften

2. entgegen § 30 Absatz 1 in Verbindung mit einer Rechtsverordnung nach § 57 Absatz 1 Satz 1 eine dort genannte Vorkehrung nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig trifft,

(6) Handelt es sich bei dem Betroffenen um eine wichtige Einrichtung kann die Ordnungswidrigkeit in den Fällen der Absatz 2 Nummer 2 und 8 mit einer Geldbuße bis zu 7 Millionen Euro oder mit einem Höchstbetrag von mindestens 1,4 % des gesamten weltweiten im vorangegangenen Geschäftsjahr getätigten Umsatzes des Unternehmens, dem der Betroffene angehört, in den Fällen des Absatzes 2 Nummer 3, 5 und 9 mit einer Geldbuße

(7) Handelt es sich bei dem Betroffenen um einen Betreiber kritischer Anlagen oder eine besonders wichtige Einrichtung, kann die Ordnungswidrigkeit in den Fällen der Absätze 1 und 2 Nummer 2, 3 und 8 mit einer Geldbuße bis zu 10 Millionen Euro oder mit einem Höchstbetrag von mindestens 2 % des gesamten weltweiten im vorangegangenen Geschäftsjahr getätigten Umsatzes des Unternehmens, dem der Betroffene angehört, in

BSIG-neu und KRITIS-DachG: Leitfaden zur Umsetzung

- Prüfen, ob Ihre **Organisation in den Anwendungsbereich** fällt. Bei **Konzernunternehmen ist jede Gesellschaft** im Detail zu prüfen.
- Überblick über die **einschlägigen Anforderungen und potentiellen Sanktionen** verschaffen.
- **Geschäftsleitung informieren** und, soweit erforderlich, schulen (insbesondere zu den neuen Geschäftsleitungspflichten).
- **Umsetzungsbedarf ermitteln** durch Abgleich der anwendbaren Anforderungen mit bereits bestehenden Konzepten, Maßnahmen, Prozessen und Verantwortlichkeiten.
- **Planung und Budgetierung des ermittelten Umsetzungsbedarfs** – Wichtig: Ressourcen & Kapazitäten rechtzeitig planen und beschaffen!
- **Beginn mit der Umsetzung**, d.h. insbesondere Umsetzung von Konzepten, Maßnahmen, Prozessen und Verantwortlichkeiten bzgl. der Geschäftsleitungspflichten, Risikomanagementmaßnahmen und der Berichtspflichten.
- **Prüfung der Lieferkette**, insbesondere Anpassung bestehender Verträge (vor allem mit Anbietern von IT-Security Lösungen).
- Rechtzeitige und geeignete **Schulung der Mitarbeiter**.

Cyber Resilience Act: Key Facts

Erster Entwurf:
15. September 2022

Aktuelle Kompromissfassung:
15. Juni 2023

Geltungsbeginn:
36 Monate ab Verkündung

Ausnahme für Meldepflichten der Hersteller:
12 Monate ab Verkündung

Betrifft:

- Produkte mit digitalen Elementen
- Hochrisiko-Produkte mit digitalen Elementen
- Hochrisiko KI

Pflichten für:
Hersteller, Importeure, Händler und Bevollmächtigte

Befugnisse für:
Aufsichtsbehörden

Bußgelder
Mitgliedstaaten legen Sanktionen (max. 15 Mio. € oder 2,5 % des Jahresumsatzes) und zuständige Behörden (noch unklar) fest

Sanktionen
durch zuständige Marktüberwachungs-behörden

Was regelt der CRA-E

Produkte mit digitalen Elementen

Ein **Software-** oder **Hardwareprodukt** und dessen **Datenfernverarbeitungslösungen**, einschließlich Software- oder Hardwarekomponenten, die getrennt **in Verkehr gebracht** werden sollen, Art. 3 Nr. 1 CRA-E

- Hardwareprodukte und –komponenten, die separat auf den Markt gebracht werden (Laptops, Mobilfunkgeräte, Netzwerkausrüstung, CPUs)
- Softwareprodukte und –komponenten, die gesondert in Verkehr gebracht werden (Betriebssysteme, Textverarbeitung, Spiele und Apps)

Nicht umfasst

- Nichtkommerzielle Produkte, einschließlich Open Source Software, sofern diese nicht Teil einer Geschäftstätigkeit ist,
- Produkte und Dienstleistungen die unter die NIS 2-Richtlinie fallen
- Kraftfahrzeuge und ihre Systeme und Bauteile,
- Medizinprodukte, In-vitro Diagnostik,
- Zertifizierte Luftfahreinrichtungen,
- Dienstleistungen, insbesondere Software-as-a-Service.

Pflichten der Wirtschaftsakteure

Hersteller, Art. 10, 11

Prozess- und Dokumentationspflichten

- Durchführung eines Konformitätsbewertungsverfahrens
- Erstellung der technischen Dokumentation
- Überwachungs- und Abhilfepflichten
- Aufbewahrungspflichten
- Verfahrens- und Informationspflichten
- Korrektur- und Rückrufpflichten

Informations- und Meldepflichten bei Schwachstellen

- Meldepflicht ggü. ENISA (24 Stunden ab Bekanntwerden einer Schwachstelle)
- Meldepflicht ggü. Nutzern (unverzüglich nach Bekanntwerden einer Schwachstelle)

Einführer, Art. 13

Prüfungspflichten

- Konformitätsbewertungsverfahren durchgeführt?
- Technische Dokumentation erstellt?
- CE-Kennzeichnung und Gebrauchsanweisung liegen vor?

Handlungspflichten

- Anbringen von Firma & Kontaktinformationen des Einführers am Produkt
- Ergreifen von Abhilfemaßnahmen bei Kenntnis oder begründeter Annahme der Nonkonformität
- Informationspflicht ggü. Hersteller (bei Feststellung von Sicherheitsschwachstellen)
- Informationspflicht ggü. Marktüberwachungsbehörden (bei hohem Risiko)
- Aufbewahrungspflicht der Konformitätserklärung .

Händler, Art. 14

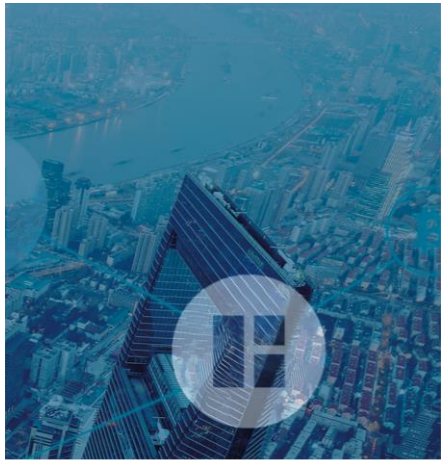
Prüfungspflichten

- Produkt trägt CE-Kennzeichnung?
- Technische Informationen, Gebrauchsanweisung und EU-Konformitätserklärung sind beigefügt?
- Ggf. Einführer hat Namen und Kontaktinformationen beigefügt?

Bei Grund zur Annahme einer Nichtkonformität:

- Keine Bereitstellung des Produkts auf dem Markt, bis die Konformität sichergestellt ist
- Sicherstellen, dass Abhilfemaßnahmen auch tatsächlich durchgeführt werden
- Informationspflichten gegenüber Hersteller und den nationalen Marktüberwachungsbehörden

Anforderungen im Detail



- Produkte mit digitalen Elementen müssen ohne bekannte ausnutzbare Schwachstellen geliefert werden.
- Auf der Grundlage einer verpflichtenden Risikobewertung müssen Produkte mit digitalen Elementen:
  - die Verfügbarkeit wesentlicher Funktionen schützen, einschließlich der Widerstandsfähigkeit gegen und der Abschwächung von Denial-of-Service-Angriffen
  - sicherheitsrelevante Informationen durch Aufzeichnung und/oder Überwachung relevanter interner Aktivitäten speichern („Logfiles“)
- Hersteller sind zur „Marktüberwachung“ bzgl. IT-Sicherheit verpflichtet
- Informationspflichten zur Cybersicherheit gegenüber dem Nutzer („Beipackzettel“)
- Zurverfügungstellung von „Software Bill of Materials“ (umstritten!)
  - Details über alle Komponenten und „Lieferkette“

Anforderungen im Detail

2. VULNERABILITY HANDLING REQUIREMENTS

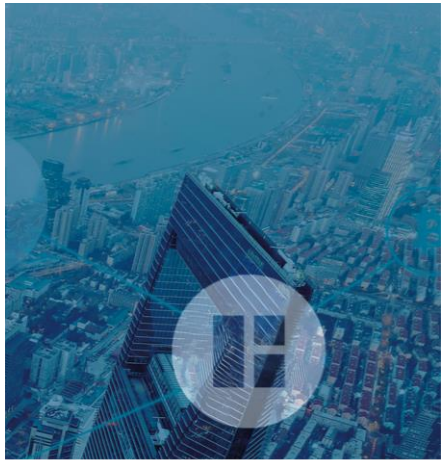
Manufacturers of the products with digital elements shall:

(1) identify and document vulnerabilities and components contained in the product, including by drawing up a software bill of materials in a commonly used and machine-readable format covering at the very least the top-level dependencies of the product;

(6) take measures to facilitate the sharing of information about potential vulnerabilities in their product with digital elements as well as in third party components contained in that product, including by providing a contact address for the reporting of the vulnerabilities discovered in the product with digital elements;

(7) provide for mechanisms to securely distribute updates for products with digital elements to ensure that ~~exploitable~~ vulnerabilities are fixed or mitigated in a timely **and, where applicable, automatic** manner;

Sanktionen (Art. 53 CRA-E)



Sanktionen sind bzgl. Bemessung und Höhe mit DSGVO

- Mitgliedsstaaten sollen Rahmenbedingungen für Sanktionen gegen Wirtschaftsakteure im Falle von Verstößen festlegen.
- Die vorgesehenen Sanktionen müssen wirksam, verhältnismäßig und abschreckend sein.
- Bei Nichteinhaltung der grundlegenden Cybersicherheitsanforderungen gemäß Anhang I und der Herstellerpflichten:

  Bis zu 15 000 000 EUR oder, bei Unternehmen, bis zu 2,5 % des weltweiten Gesamtjahresumsatzes des Unternehmens im vorangegangenen Geschäftsjahr
- Bei Nichteinhaltung sonstiger Verpflichtungen:

  Bis zu 10 000 000 EUR oder, bei Unternehmen, bis zu 2 % des weltweiten Gesamtjahresumsatzes des Unternehmens im vorangegangenen Geschäftsjahr
- Bei Erteilung falscher, unvollständiger oder irreführender Auskünfte an notifizierte Stellen und Marktüberwachungsbehörden in Beantwortung eines Ersuchens:

  Bis zu 5 000 000 EUR oder, bei Unternehmen, bis zu 1 % des weltweiten Gesamtjahresumsatzes des Unternehmens im vorangegangenen Geschäftsjahr

Das Heuking IT-Security Kern-Team

Dr. Lutz Keppeler

Partner

- Fachanwalt für IT-Recht
- ISO 27001 Foundation
- ISO 27001 Security Officer

Manuel Poncza

Associate

- IT-Security-Manager (TÜV)
- IT-Security-Beauftragter (TÜV)
- IT-Compliance Manager (TÜV)

Michael Kuska

Salaried Partner

- ISO 27001 Foundation
- ISO 27001 Security Officer

Dr. Stefan Jöster

Partner

- Fachanwalt für Versicherungsrecht
- Spezialist für Cyber Versicherungen

Gebündelte Kompetenz:

- Weitere Fachanwälte für IT-Recht
- Praxisgruppe IT/IP mit über 40 Anwälten
- Langjährige Praxiserfahrung im Cyber-Strafrecht
- Kontakt zu Polizei / StA
- Kontakt zu BSI
- Kontakt zu Datenschutz-Aufsichtsbehörden
- Regelmäßig in internationalen Mandaten tätig
- Koordination von Behörden-Meldungen in allen Ländern der Welt

Ansprechpartner

Dr. Lutz Martin Keppeler
Rechtsanwalt | Partner
Fachanwalt für IT-Recht
Magnusstraße 13
50672 Köln
T +49 221 2052-426
F +49 221 2052-1
l.keppeler@heuking.de

Kompetenzen

IT-Recht mit Spezialisierung auf IT-Sicherheitsrecht und Open Source Lizenzen
Datenschutzrecht
Telekommunikationsrecht

Mitgliedschaften

Fellow der European Free Software Foundation (FSFE)
International Bar Association (IBA)

Veröffentlichungen (Auszug)

Die Open-Source-Bereichsausnahme im Entwurf des Cyber-Resilience-Act
Zeitschrift für Product Compliance (ZfPC) 2023, S. 117-123
Kapitel „Cyberversicherungen“ in: Wollinger / Schulze (Hrsg.) Handbuch Cybersecurity für die öffentliche Verwaltung, 2020
§ 2, 4a,4b,5b,7a-c,9b BSIG, § 11 EnWG, § 109 TKG in Ritter, Kommentar zum IT-Sig. 2.0 (2021)
„Datenschutz und SSL-Decryption“ K&R 2017, 453 ff.
Technische und rechtliche Probleme bei der Umsetzung der DSGVO Löschpflichten ZD 2017, 314 ff.

HEUKING

Danke für die Aufmerksamkeit