Rechtliche Anforderungen des IT-Sicherheitsgesetzes 2024 (NIS2UmsuCG)

it-sa, Nürnberg, Knowledge Forum A
11.10.2023, RA Karsten U. Bartels LL.M.

HK2 Rechtsanwälte

Mehr dazu heute
15:15 Uhr

Congress@it-sa
NCC Ost
Raum Singapur

Karsten U. Bartels LL.M.*

- Rechtsanwalt/ Partner bei HK2
- Geschäftsführer HK2 Comtection GmbH
- Vorsitzender Arbeitsgemeinschaft IT-Recht im Deutschen Anwaltverein
- Stellv. Vorstandsvorsitzender Bundesverband IT-Sicherheit (TeleTrusT)
- Lehrbeauftragter Hochschule Hof für Datenschutz-Compliance
- Zert. Datenschutzbeauftragter (TÜV)

*Rechtsinformatik

HK2

IT- und Datenrecht
Technik-Recht

IT-Sicherheitsrecht
Datenschutzrecht

Karsten U. Bartels LL.M.
Anwalt des Jahres für Datenschutzrecht, Berlin 2023
Handelsblatt/ best lawyers

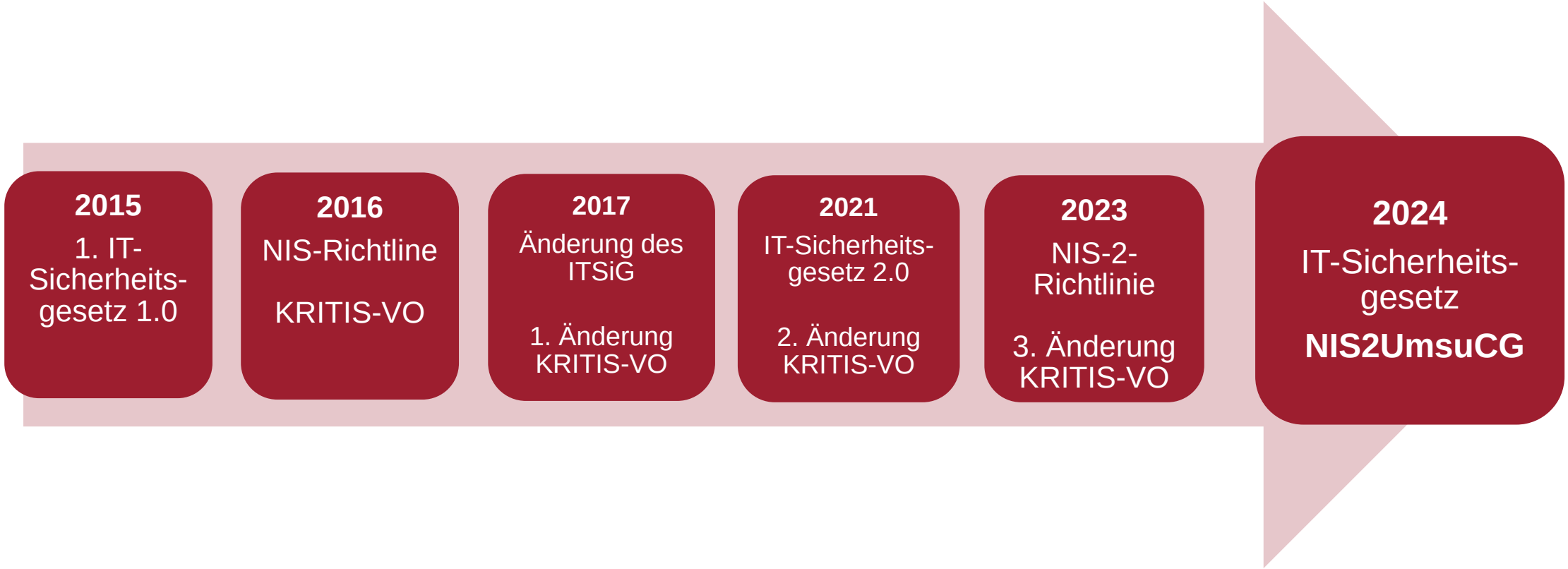
Beste Anwälte Deutschlands 2023
Handelsblatt/ best lawyers

Karsten U. Bartels LL.M.
Dr. Jonas Jacobsen
Bernhard Kloos
Philip Koch

HK2 TOP-Wirtschaftskanzlei 2023 für IT & TK
FOCUS BUSINESS 06/2023

HK2 Rechtsanwälte

Entwicklung des IT-Sicherheitsgesetzes



Gesetzgebungsstand NIS2UmsuCG

2024

IT-Sicherheits-gesetz

NIS2UmsuCG

- Erster Referentenentwurf zum NIS2UmsuCG 03.04.2023
- Zweiter Referentenentwurf vom 03.07.2023
- Diskussionspapier **vom 27.09.2023**
- Ende Umsetzungsfrist: 17.10.2024

Grundlegende Änderungen

- Zahl betroffener Unternehmen
- zusätzliche Sektoren
- Ausweitung und Konkretisierung der Pflichten für Unternehmen
- Ausweitung Befugnisse des BSI
- Erweiterte Sanktionsvorschriften
- Pflichten für Einrichtungen der Bundesverwaltung

Supushpitha Atapattu /pexels.com

HK2 Rechtsanwälte

Unternehmensgrößen im BSIG-E

Großunternehmen
§ 28 Abs. 1 BSIG-E

Mittlere Unternehmen
§ 28 Abs. 2 BSIG-E

Unternehmen jeder Größe

250+ oder

und

50+ Mio. **43+ Mio.**

50+ oder

und

10+ Mio. **10+ Mio.**

HK2
Rechtsanwälte

Betreiber kritischer Anlagen

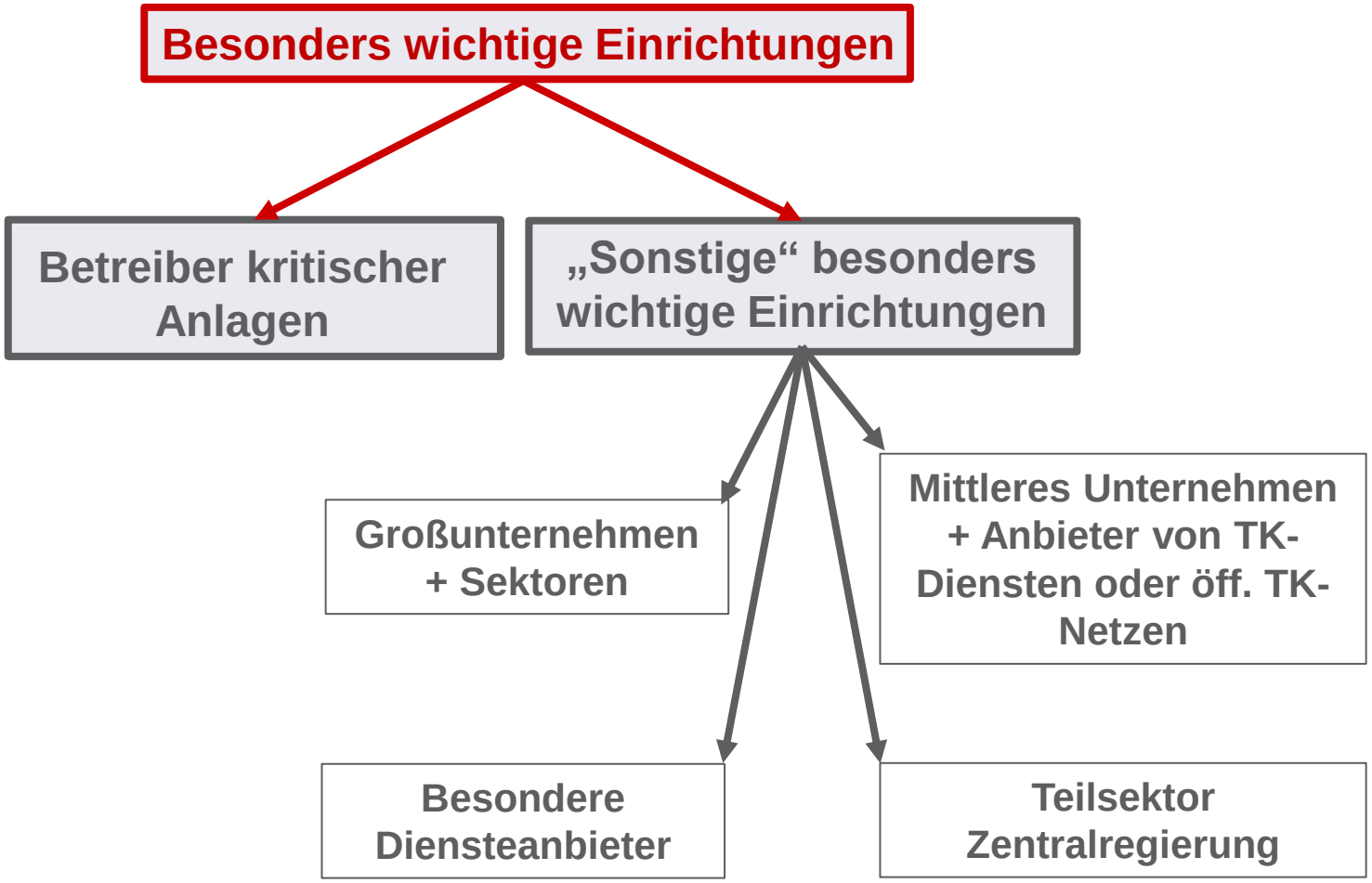
HK2 Rechtsanwälte

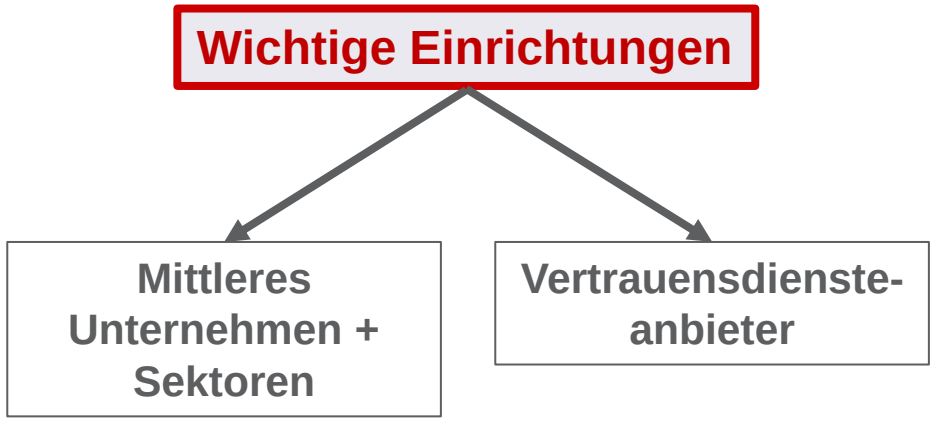
Besonders wichtige Einrichtungen

- Betreiber kritischer Anlagen
- „Sonstige“ besonders wichtige Einrichtungen

Wichtige Einrichtungen

HK2 Rechtsanwälte



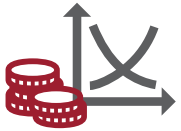


HK2 Rechtsanwälte

Betreiber kritischer Anlagen

Energie

Ernährung



Finanz- u. Versicherungsw.

Weltraum

Vertr.diensteanb (qual./normal)

Öff. Verwaltung (Zentralreg.)

Forschung

Trinkwasser

IT und TK

Transport und Verkehr

TLD Name Registries

Chemie

Verarbeitendes Gewerbe

Abwasser

Gesundheit

Siedlungsabfall-entsorgung

Anb. von TK-Diensten o. öff. zugänglichen TK-Netzen

DNS-Diensteanb.

Lebensmittel

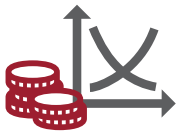
Anb. digitaler Dienste

HK2 Rechtsanwälte

Besonders wichtige Einrichtungen – Großunternehmen


Energie


Ernährung


Finanz- u. Versicherungsw.


Weltraum


Vertr.diensteanb (qual./normal)

Öff. Verwaltung (Zentralreg.)


Forschung


Trinkwasser


IT und TK


Transport und Verkehr

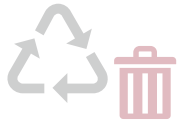

TLD Name Registries


Chemie

Verarbeitendes Gewerbe


Abwasser


Gesundheit


Siedlungsabfall-entsorgung


Anb. von TK-Diensten o. öff. zugänglichen TK-Netzen

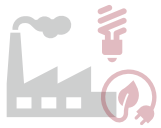
DNS-Diensteanb.

Lebensmittel

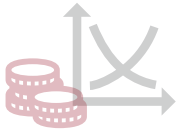

Anb. digitaler Dienste

Besonders wichtige Einrichtungen – Mittlere Unternehmen

HK2 Rechtsanwälte


Energie


Ernährung


Finanz- u. Versicherungsw.


Weltraum

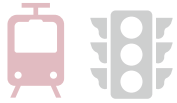

Vertr.diensteanb (qual./normal)

Öff. Verwaltung (Zentralreg.)


Forschung

Trinkwasser

IT und TK


Transport und Verkehr

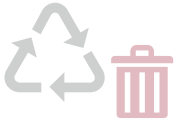

TLD Name Registries


Chemie

Verarbeitendes Gewerbe

Abwasser


Gesundheit


Siedlungsabfall-entsorgung


Anb. von TK-Diensten o. öff. zugänglichen TK-Netzen

DNS-Diensteanb.

Lebensmittel


Anb. digitaler Dienste

HK2 Rechtsanwälte

Besonders wichtige Einrichtungen – Unternehmen jeder Größe

Energie

Ernährung

Finanz- u. Versicherungsw.

Weltraum

Vertr.diensteanb (qual./normal)

Öff. Verwaltung (Zentralreg.)

Forschung

Trinkwasser

IT und TK

Transport und Verkehr

TLD Name Registries

Chemie

Verarbeitendes Gewerbe

Abwasser

Gesundheit

Siedlungsabfall-entsorgung

Anb. von TK-Diensten o. öff. zugänglichen TK-Netzen

DNS-Diensteanb.

Lebensmittel

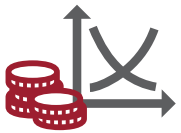
Anb. digitaler Dienste

HK2 Rechtsanwälte

Wichtige Einrichtungen – Mittlere Unternehmen


Energie


Ernährung


Finanz- u. Versicherungsw.


Weltraum


Vertr.diensteanb (qual./normal)

Öff. Verwaltung (Zentralreg.)


Forschung


Trinkwasser


IT und TK


Transport und Verkehr


TLD Name Registries


Chemie


Verarbeitendes Gewerbe


Abwasser


Gesundheit


Siedlungsabfall-entsorgung

Anb. von TK-Diensten o. öff. zugänglichen TK-Netzen

DNS-Diensteanb.


Lebensmittel


Anb. digitaler Dienste

Pflichten für Betroffene, §§ 30 ff. BSIG-E

- **Risikomanagementmaßnahmen**
- Meldepflichten
- Registrierungspflicht
- Unterrichtungspflicht
- Pflichten für Geschäftsleitung
- Nachweispflichten für KRITIS-Betreiber
- Besondere Pflichten für Einrichtungen der Bundesverwaltung

Risikomanagementmaßnahmen für besonders wichtige und wichtige Einrichtungen, § 30 BSIG-E

- geeignete, verhältnismäßige und wirksame **technische und organisatorische Maßnahmen**
  - Risikoexposition, Größe Einrichtung/ Betreiber, Risiko (Eintrittswahrscheinlichkeit und Schwere von Sicherheitsvorfällen, gesellschaftliche Auswirkungen) und Umsetzungskosten zu berücksichtigen.
- Maßnahmen
  - sollen **Stand der Technik** einhalten
  - **Normen** berücksichtigen und
  - müssen auf „gefahrenübergreifendem Ansatz beruhen“
  - Katalog mit **Mindestanforderungen** z. B. Risikoanalysekonzepte, Lieferkettensicherheit, Cyberhygiene, Verschlüsselung u. v. m.
- bleibt möglich: Branchenspezifische Sicherheitsstandards (B3S)

HK2 Rechtsanwälte

Meldepflichten, § 32 BSIG-E

Stufe 1: frühe Erstmeldung, Nr. 1	• **24h; Vorfall wegen rechtswidriger/böswilliger Handlungen? Grenzüberschreitende Auswirkungen?**
Stufe 2: bestätigende Erstmeldung, Nr. 2	• **72h; Bestätigung der Informationen; erste Bewertung: Schweregrad? Auswirkungen? Kompromittierungsindikatoren?**
Stufe 3: Zwischenmeldung, Nr. 3	• **Statusaktualisierung auf Ersuchen des BSI**
Stufe 4: Abschlussmeldung, Nr. 4	• **1 Monat; ausführliche Beschreibung; Art und Ursache; Abhilfemaßnahmen; grenzüberschreitende Auswirkungen**

Abs. 2: ggf. statt Abschlussmeldung Fortschrittsbericht, wenn Vorfall noch andauert

moerschy/Pixabay.com

HK2 Rechtsanwälte

Sanktionen, § 60 BSIG-E

- Bußgelder von EUR 100.000 bis 2 Mio.
- Für wichtige Einrichtungen: EUR 100.000 bis 7 Mio. bzw. 1,4 % des weltweiten Umsatzes
- Für besonders wichtige Einrichtungen (inkl. Betreiber kritischer Anlagen): EUR 100.000 bis 10 Mio. bzw. 2 % des weltweiten Umsatzes

Was ist bereits jetzt zu tun?

Mehr dazu heute
15:15 Uhr

Congress@it-sa
NCC Ost
Raum Singapur

HK2
Rechtsanwälte

Was wäre, wenn mein Unternehmen im Anwendungsbereich liegt? Was, wenn meine Kunden betroffen sind?

Wie wirkt sich das jetzt auf meine IT-Sicherheitsstrategie aus?

Welche weiteren gesetzlichen Anforderung wird es an die IT-Sicherheit geben?

HK2
Rechtsanwälte

Slides + Kontakt

www.hk2.eu

linkedin.com/in/karstenbartels

www.comtection.de