

Im Cybersicherheits-Labyrinth?

**KRITIS-Dachgesetz, Cyber Resilience Act und NIS-2-Umsetzung im BSIG als neues
Regulierungsgefüge**

Dr. Johannes Döveling, LL.M. (Cape Town)

Rechtsanwalt | Counsel

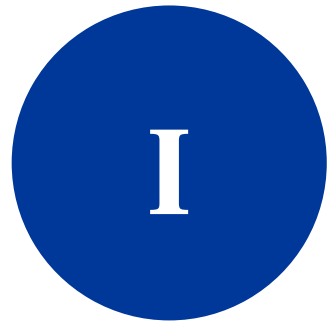
Dr. Felix Hempel, LL.M. (Norwich), CIPP/E

Rechtsanwalt | Senior Associate

Herbstakademie 2026

Agenda

- I. **Ausgangsfall** – Anbieter eines Cloud-Computing-Dienstes
- II. **Überblick** – Das neue Regulierungsgefüge
- III. **NIS-2-Richtlinie** – Anwendungsbereich, Regelungen im Kern, Sonderregelungen, Zusammenspiel
- IV. **CER-Richtlinie** – Anwendungsbereich, Regelungen im Kern, Sonderregelungen, Zusammenspiel
- V. **Cyber Resilience Act** – Anwendungsbereich, Regelungen im Kern, Sonderregelungen, Zusammenspiel
- VI. **Auswirkungen auf den Cloud-Anbieter** – Der Cloud-Anbieter im Sturm der neuen Regelungen
- VII. **Fazit und Ausblick** – Auf zu neuen Gezeiten oder Sturm im Wasserglas?



Ausgangsfall

Ausgangsfall: Cloud-Anbieter

Cloud-Anbieter

- Anbieter eines Cloud-Computing-Dienstes
- Betreibt Rechenzentren und stellt Cloud-Dienste bereit
- Vertriebt zugleich ein eigenes Produkt (z.B. einen Passwortmanager zum Download (Software))

Muss Cybersicherheit gewährleisten – was fällt darunter?

NIS-2 / BSIG

Einrichtungsbezogen

- Cloud-Dienst = Digitale Infrastruktur
- Eigenes Risikomanagement der IT
- Melde- & Registrierungspflichten

CER / KRITIS-DachG

Physische Resilienz kritischer Einrichtungen

- Rechenzentrum grds. kritische Anlage
- Aber: Bereichsausnahme?
- Materielle Pflichten gelten dann nicht

Cyber Resilience Act

Produktbezogen

- Passwortmanager zum Download (Software) = Produkt mit digitalen Elementen
- Grundlegende Anforderungen
- CE-Kennzeichen & Lebenszyklus



Überblick

Das Regulierungsgefüge im Überblick

NIS-2 (umgesetzt im BSIG)

- Cybersicherheit von wichtigen und besonders wichtigen Einrichtungen → wesentlicher Teil der Wirtschaft erfasst
- Einrichtungsbezogene Cybersicherheit → Verfügbarkeit von Einrichtungen
- Anknüpfungspunkt: *Ausübung bestimmter Tätigkeiten & Schwellenwerte*
- ▶ **Cloud-Anbieter:** als Digitale Infrastruktur erfasst – volle NIS-2-Pflichten

CER-RL (umgesetzt im KRITIS-DachG)

- Resilienz von kritischen Einrichtungen
- Fokus auf physische und organisatorische Resilienz
- Anknüpfungspunkt: *Betrieb kritischer Einrichtungen*
- ▶ **Cloud-Anbieter:** grds. erfasst – aber Bereichsausnahme (Art. 8 CER)

Cyber Resilience Act

- Produktbezogene Cybersicherheitsregulierung → Produktsicherheit
- Schnittstelle von Produktrecht und Cybersicherheitsrecht
- Anknüpfungspunkt: *Produkt mit digitalen Elementen*
- ▶ **Cloud-Anbieter:** Passwortmanager zum Download (Software) = Produkt mdE

Weitere Rechtsakte

- Sektorspezifisch (DORA – Finanzsektor)
- ▶ **Lex specialis:** verdrängt allgemeine Vorgaben
- Cybersecurity Act – u.a. Zertifizierungssysteme

Zwei Säulen: einrichtungsbezogene Resilienz (NIS-2, CER) ↔ produktbezogene Sicherheit (CRA)

III

Die Umsetzung der NIS-2-Richtlinie

NIS-2: Zweck, Anwendungsbereich & Regelungen im Kern

Zweck der NIS-2-Richtlinie

- Schutz von Netz- und Informationssystemen („NIS“) – digitale Prozesse gegen Angriffe schützen
- Cybersicherheitsregulierung wird auf große Teile der Wirtschaft ausgeweitet
- Fokus auf gesamtgesellschaftlich relevante Tätigkeiten → durchgehende Verfügbarkeit; risikobasierter Ansatz

Anwendungsbereich

Sachlich

- Tätigkeit in einem Sektor (Anlagen 1 & 2 BSIG)
- Ausübung der erfassten Tätigkeit genügt grdsl. – eng an der Richtlinie

Persönlich – Schwellenwerte

- Besonders wichtige Einrichtungen: große Unternehmen (> 250 MA / > 50 Mio. € Umsatz und > 43 Mio. € Jahresbilanzsumme + jeweils Tätigkeit in Sektor aus Anlage 1)
- Wichtige Einrichtungen: mittlere Unternehmen (> 50 MA / > 10 Mio. € Umsatz und Jahresbilanzsumme + jeweils Tätigkeit in Sektor aus Anlage 1/2)
- Einzelne Sektoren: Größenunabhängig erfasst

Regelungen im Kern

- Eigenverantwortliches Risikomanagement
- Mindestkatalog: Vorfallbewältigung, Betriebskontinuität, Lieferkette, Verschlüsselung, Zugriffskontrolle
- Präventiver + reaktiver Schutz
- Gefahrenübergreifender Ansatz; Umfang der zu treffenden Maßnahmen risikoabhängig
- Melde- & Registrierungspflichten
- Besondere Verantwortung der Leitungsorgane

🏠 **Cloud-Anbieter:** als Cloud-Computing-Dienst + Anbieter von Rechenzentrumsdiensten (Sektor Digitale Infrastruktur in Anlage 1) erfasst – muss einrichtungsbezogene Tätigkeiten umsetzen

NIS-2: Sonderregelungen & Zusammenspiel

Sonderregelungen

§ 28 Abs. 3 BSIG – De-minimis

- „vernachlässigbare“ Nebentätigkeiten bleiben unberücksichtigt
- Verhindert Erfassung als bloßer „Beifang“

Betreiber kritischer Anlagen (§ 2 Nr. 1 KRITIS-DachG)

- Gelten stets als besonders wichtige Einrichtung (§ 28 Abs. 1 Nr. 1 BSIG) – **zusätzlich** zu den NIS-2-Pflichten:
 - Strengerer Zumutbarkeitsmaßstab (§ 31 Abs. 1 BSIG)
 - Systeme zur Angriffserkennung (§ 31 Abs. 2 BSIG)
 - Audit- & Nachweispflichten (§ 39 BSIG)
 - Beschränkung kritischer Komponenten (§ 41 BSIG)

🏔 **Cloud-Anbieter:** Rechenzentrum als kritische Anlage → zusätzlich Audits (§ 39 BSIG) & Angriffserkennung

Zusammenspiel

Verhältnis zur CER-RL

- Digitalsektor: Vorrang von NIS-2 – Bereichsausnahme Art. 8 CER (§ 4 Abs. 2 KRITIS-DachG)
- Andere Sektoren: Doppelbelastung NIS-2 + CER (unterschiedliche Schutzziele)

Verhältnis zum CRA

- Einrichtungsbezogen (NIS-2) vs. produktbezogen (CRA) → kein echtes Spannungsverhältnis

🏔 **Cloud-Anbieter:** Aufsicht am Hauptsitz (Cloud-Dienst); für TK-Dienste zusätzlich BNetzA (siehe nächste Folie)

NIS-2: Aufsicht

Regelfall

- Zuständigkeit am Ort der Niederlassung bzw. der kritischen Anlage
- **§ 59 BSIG**

Digitalsektor

- Abweichend: Hauptniederlassungsprinzip
- One-Stop-Shop
- **§ 60 BSIG**

TK-Dienste

- Abweichend: Marktortprinzip
- Pflichten aus dem TKG (§§ 165, 168)
- Aufsicht BNetzA
- **§ 28 Abs. 5 Nr. 1 BSIG**

IV

Die Umsetzung der CER-Richtlinie

CER: Anwendungsbereich & Regelungen im Kern

Anwendungsbereich

CER-Richtlinie

- Resilienz kritischer Einrichtungen – elf Sektoren (Vorgänger nur Energie/Verkehr)
- Mitgliedstaaten bestimmen kritische Einrichtungen nach Kriterien (Art. 7) – Maßstab: erhebliche Störung

Umsetzung: KRITIS-DachG

- Infrastrukturbezogen: „Betreiber kritischer Anlagen“ (§ 2 Nr. 1)
- Konkretisierung durch BMI-Rechtsverordnung (§ 4 Abs. 3, § 5) – noch ausstehend, daher derzeit nicht anwendbar
- Regelschwelle 500.000 versorgte Einwohner (§ 5 Abs. 2); physischer Nexus zu Deutschland

🏔 **Cloud-Anbieter:** Rechenzentrum grds. kritische Anlage – aber Bereichsausnahme

Regelungen im Kern

Resilienzpflcht

- Geeignete und verhältnismäßige technische, sicherheitsbezogene und organisatorische Maßnahmen (Art. 13 Abs. 1 CER)
- Schutz auch gegen nicht-digitale Gefahren: Naturgefahren, Sabotage, Terror

Risikobewertung & Resilienzplan

- Art. 12, 13 Abs. 2 CER; §§ 12–14 KRITIS-DachG

Registrierung & Aufsicht

- Registrierungspflicht (§ 8 KRITIS-DachG); Resilienzstandards über BBK anerkennbar (§ 14 Abs. 2)
- BBK als zentrale Anlaufstelle; im IT-Bereich BSI (§ 3 Abs. 2 Nr. 9)

🏔 **Cloud-Anbieter:** *müsste* Risikobewertung + Resilienzplan erstellen – greift wegen Bereichsausnahme jedoch nicht

CER: Sonderregelungen & Zusammenspiel

Sonderregelungen

Bereichsausnahme (Art. 8 CER)

- Bankwesen, Finanzmarktinфраstruktur, Digitale Infrastruktur – materielle Pflichten (Kap. III, IV, VI) gelten nicht
- Umsetzung in § 4 Abs. 2 KRITIS-DachG: für Sektor IT/TK entfallen §§ 12–16, 18, 20, 21 Abs. 6 (Resilienzplichten: Risikoanalyse, Resilienzplan, sektorübergreifende Mindestanforderungen, Nachweise, Vorfallmeldungen sowie Umsetzungs- + Berichtspflichten Geschäftsleitung)
- Aber: Registrierungspflicht (§ 8) bleibt; Aufnahme in die Liste kritischer Einrichtungen

Hintergrund & nationale Erweiterung

- Resilienz bereits über DORA (Finanz) bzw. NIS-2 (Digital) gesichert – lex specialis, Doppelarbeit vermeiden
- KRITIS-DachG ergänzt weitere Sektoren: Sozialversicherung/Grundsicherung, Siedlungsabfallentsorgung (§ 4 Abs. 1)
- **Cloud-Anbieter:** als Digitale Infrastruktur grds. nur Registrierung (§ 8) – keine materiellen CER-/KRITIS-Pflichten

Zusammenspiel

Verhältnis zur NIS-2-Richtlinie

- Digitalsektor: Vorrang NIS-2 – CER-Pflichten entfallen (konsistent zur NIS-2-Folie)
- Andere Sektoren: kritische Einrichtung häufig auch NIS-2 → Doppelbelastung (Resilienz vs. Cybersicherheit)

Rumpf-KRITIS im BSIG

- Betreiber kritischer Anlagen = besonders wichtige Einrichtung (§ 28 Abs. 1 Nr. 1 BSIG)
- Zusätzliche BSIG-Pflichten: § 31 (Angriffserkennung), § 39 (Audit), § 41 (krit. Komponenten)

Aufsicht

- CER kennt kein Hauptniederlassungsprinzip (Belegenheitsort) – im Digitalsektor sollte NIS-2-Hauptniederlassungsprinzip gelten
- **Cloud-Anbieter:** nur NIS-2 (nicht CER); Hauptniederlassungsprinzip sollte auch für KRITIS-Zusatzpflichten (z.B. § 39 BSIG) im Digitalsektor gelten



Die Umsetzung des CRA

CRA: Anwendungsbereich & Regelungen im Kern

Anwendungsbereich

Produkt mit digitalen Elementen

- Soft-/Hardware mit Datenverarbeitung (Art. 3) – weiter Anwendungsbereich (z.B. App, vernetzte Kaffeemaschine) und
- bestimmungsgemäße Verwendung schließt Datenverbindung ein (Art. 2 Abs. 1)

Anknüpfung

- Produktregulierung, nicht Einrichtung / Dienst
- Marktortprinzip – Sitz des Herstellers unerheblich

Lieferkette

- Hersteller (Hauptadressat), Einführer, Händler – abgestufte Pflichten

🏔 **Cloud-Anbieter:** Cloud-Dienst selbst i. d. R. nicht erfasst – aber als solche angebotene Software, wie z.B. der Passwortmanager (= Produkt mdE)

Regelungen im Kern

Grundlegende Anforderungen (Anhang I)

- **Pre-market:** Security by Design & by Default; Niveau nach Risikobewertung (Art. 13)
- **Post-market:** Schwachstellenmanagement über den Lebenszyklus – Updates, SBOM (Unterstützungszeitraum regelmäßig mind. 5 Jahre)

Nachweis & Marktzugang

- Technische Dokumentation (Art. 31)
- Konformitätsbewertung (Art. 32)
- CE-Kennzeichen als Voraussetzung des Inverkehrbringens (Art. 29 f.)

Meldepflichten (Art. 14)

- Aktiv ausgenutzte Schwachstellen / Vorfälle an ENISA + CSIRT (24 h / 72 h)
- 🏔 **Cloud-Anbieter:** muss für den Passwortmanager Security by Design umsetzen, SBOM führen, Konformitätsbewertung durchführen lassen & CE-Kennzeichen anbringen

CRA: Sonderregelungen & Zusammenspiel

Sonderregelungen

Drei Produktkategorien

- Gewöhnliche / wichtige / kritische Produkte mdE (Anh. III, IV)
- Abgestufte Konformitätsbewertung (Art. 32):
 - Gewöhnlich: Selbstbewertung
 - Wichtig / kritisch: häufig benannte Stelle
- Konformitätsvermutung bei harmonisierten Normen (Art. 27)

Weitere Ausnahmen

- Sektorspezifisch (Medizin, Kfz, Luftfahrt – Art. 2)
- Open-Source: nicht kommerziell ausgenommen; Verwalter mit Sonderpflichten

🏔 **Cloud-Anbieter:** Passwortmanager = wichtiges Produkt Klasse I → strengeres Konformitätsbewertungsverfahren

Zusammenspiel

Verhältnis zu NIS-2 / CER

- Produkt- statt Einrichtungsregulierung → kein echtes Spannungsverhältnis
- Ergänzt die einrichtungsbezogene Regulierung um die Produktebene

Lex specialis

- Bereits sektorspezifisch regulierte Produkte gehen vor – Doppelregulierung vermieden

Nationale Umsetzung

- CRA gilt als Verordnung unmittelbar; BSI als Marktüberwachungsbehörde
- Zusammenspiel mit NIS-2 / CER nicht ausdrücklich geregelt

🏔 **Cloud-Anbieter:** NIS-2 für den Cloud-Dienst; für den Passwortmanager zusätzlich CRA
Beide Regime parallel, aber getrennt

VI

Auswirkungen auf den Cloud-Anbieter

Cloud-Anbieter im Gesamtgefüge

NIS-2 / BSIG

- Cloud-Dienst = Digitale Infrastruktur → voll erfasst
- Risikomanagement (Art. 21 / § 30), Melde- & Registrierungspflichten
- Rechenzentrum als kritische Anlage: § 31, § 39, § 41 BSIG

CER / KRITIS-DachG

- Grds. kritische Einrichtung / kritische Anlage
- Bereichsausnahme (Art. 8 CER / § 4 Abs. 2 KRITIS-DachG)
- Nur Registrierung (§ 8) – keine materiellen Resilienzplichten

Cyber Resilience Act

- Cloud-Dienst selbst i. d. R. nicht erfasst
- Passwortmanager = Produkt mdE → Security by Design, SBOM, Schwachstellen-management, Konformitätsbewertung, CE-Kennzeichen, Meldepflichten



Handlungsbedarf für den Cloud-Anbieter

- ▶ **Regime zuordnen:** prüfen, welche Dienste/Produkte unter NIS-2, CER und CRA fallen (Bestandsaufnahme und Scoping)
- ▶ **Doppelpflichten koordinieren:** parallele Anforderungen bündeln, Melde-, Nachweis- und Risikoprozesse über die Regelwerke hinweg zusammenführen
- ▶ **Zuständigkeit klären:** Aufsichtsbehörde und Hauptsitz bestimmen; Reichweite der KRITIS-Zusatzpflichten im Blick behalten
- ▶ **Produkt-Compliance aufsetzen:** für den Passwortmanager CRA-Prozesse etablieren

VII

Fazit und Ausblick – Auf zu neuen Gezeiten oder Sturm im Wasserglas?

Auf zu neuen Gezeiten und/oder Sturm im Wasserglas?

1

Tragfähige Grundkonzeption: Die Regulierung differenziert zwischen **einrichtungsbezogener Resilienz** (NIS-2, CER) und **produktbezogener Sicherheit** (CRA) – kein echtes Spannungsverhältnis.

2

Doppelregulierung nur teilweise vermieden: Im **Digitalsektor** Vorrang der NIS-2-Richtlinie; in anderen Sektoren verbleibt eine – durch unterschiedliche Schutzziele gerechtfertigte – Doppelbelastung (CER + NIS-2).

3

Kein Normkonflikt, sondern Fragmentierung: Die Regelwerke folgen je eigener Logik, sind aber **nur begrenzt aufeinander abgestimmt** – zentrales Problem ist das Koordinationsdefizit zwischen den Regimen.

4

CRA ergänzt, ohne zu verzahnen: Er fügt die **Produktperspektive** hinzu; das Zusammenspiel mit den übrigen Regimen hat der Gesetzgeber jedoch nicht näher ausgestaltet.

5

Bewährungsprobe steht aus: Die Herausforderung liegt in der Koordination paralleler Regelwerke; zentrale Konkretisierungen fehlen und erste Änderungen sind bereits absehbar.

Referenten



Dr. Johannes Döveling, LL.M. (Cape Town)

Rechtsanwalt | Counsel

johannes.doeveling@twobirds.com

Recht der IT-Sicherheit

- NIS-2 und Kritische Infrastruktur; IT-Sicherheit im Telekommunikationssektor

Telekommunikationsrecht

- Insbesondere Regulierung und Vertragsgestaltung

Daten- und Datenschutzrecht

- Insbesondere Telekommunikationsdatenschutz und Data Act



Dr. Felix Hempel, LL.M. (Norwich), CIPP/E

Rechtsanwalt | Senior Associate

felix.hempel@twobirds.com

Daten- und Datenschutzrecht

- Regulatorische Anforderungen und Datenschutz-Compliance

IT- und Datensicherheit

- NIS-2, Cybersecurity und Kritische Infrastruktur

Telekommunikationsrecht

- Vertragsgestaltung und Regulierung