Cybersecurity Compliance: Überblick über die aktuelle Regulierung

Prof. Dr. Dennis-Kenji Kipker

Offenbach a.M., 28.09.2022

VDE

Agenda

- A. Deutsche Cybersicherheitsstrategie 2021
- B. Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-SiG 2.0)
- C. The EU’s Cybersecurity Strategy for the Digital Decade
- D. Proposal for a Directive on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148 (NIS 2)
- E. Proposal for a Regulation establishing a framework of measures for strengthening Europe's semiconductor ecosystem (Chips Act)
- F. Radio Equipment Directive (RED) Delegated Act
- G. Ausblick: EU Cyber Resilience Act, hENs und horizontale Cybersecurity-Regulierung in der EU

A. Nationale Cybersicherheitsstrategie 2021

- Evaluierung und Fortschreibung der deutschen Cyber-Sicherheitsstrategie aus 2016
- **Adressierte Handlungsfelder:**
  - Handlungsfeld 1: Sicheres und selbstbestimmtes Handeln in einer digitalisierten Umgebung
  - Handlungsfeld 2: Gemeinsamer Auftrag von Staat und Wirtschaft
  - Handlungsfeld 3: Leistungsfähige und nachhaltige gesamtstaatliche Cyber-Sicherheitsarchitektur
  - Handlungsfeld 4: Aktive Positionierung Deutschlands in der europäischen und internationalen Cyber-Sicherheitspolitik
- **Zentrale Aspekte:** Leitlinien, Handlungsfelder, strategische Umsetzung (strategisches Controlling, Überprüfung der operativen Umsetzung)

A. Nationale Cybersicherheitsstrategie 2021

- Leitlinien als zentrale Querschnittsthemen, die nicht auf ein Handlungsfeld begrenzt sind
- **Digitale Souveränität:**
  - Definition: Fähigkeiten und Möglichkeiten von Individuen und Institutionen, ihre Rolle in der digitalen Welt selbstständig, selbstbestimmt und sicher ausüben zu können
  - Inhalte: Anwendungszentrierte FuE, Cybersecurity als Qualitätsmerkmal „Made in Germany“, Förderung EU-Anbieter, staatliche Prüfkapazitäten, Eigensicherung der Verwaltung, „gemeinsame Vision und Strategie der EU“
- **Sichere Gestaltung der Digitalisierung:** Sichere Ausgestaltung der digitalen Transformation von Staat, Wirtschaft und Gesellschaft (z.B. E-Government, Mobile Work, 5G, Homeschooling)
- **Effektivität und Messbarkeit:** Überprüfbarkeit der Ziele der CSS 2021, strategisches Controlling durch BMI

B. IT-Sicherheitsgesetz 2.0

- In Kraft getreten am 28. Mai 2021
- **Bundestag:** „Wenig Beifall für das geplante IT-Sicherheitsgesetz“
- **Änderung verschiedener Vorschriften:** BSIG, TKG, EnWG, SGB X und Außenwirtschaftsverordnung
- **BSI:** Mehr Kompetenzen – mehr „Unabhängigkeit“ – Aufgabenwahrnehmung auf „Grundlage wissenschaftlich-technischer Erkenntnisse“
- Definition von kritischen Komponenten mit „Steuerungsfunktion“
- **Ergänzung von KRITIS:** „Siedlungsabfallentsorgung“ (ca. 100 weitere Betreiber zu erwarten, knapp 1.700 Unternehmen in der Abfallwirtschaft) → Schwellenwerte in BSI-KritisV bislang undefiniert
- **„Black Box“ insbesondere:** „Unternehmen im besonderen öffentlichen Interesse“ – größte Unternehmen nach Wertschöpfung (UBI der Kategorie 2)

B. IT-Sicherheitsgesetz 2.0

- **UBI 2:** Größte inländische Unternehmen nach Wertschöpfung ungeachtet der Branche → nicht Versorgungssicherheit das Ziel, sondern Absicherung der nationalen Wertschöpfung!
- Wertschöpfungskriterium orientiert sich an TOP 100 im Hauptgutachten der Monopolkommission, BSI: „vordere Plätze“ wohl relativ sicher erfasst
- **Überdies ebenso UBI 2:** Zulieferer, die wegen ihrer Alleinstellungsmerkmale von besonderer Bedeutung sind (systemische Relevanz) → Ausdehnung auf zahlreiche KMU zu erwarten, z.B. Automobilzulieferer
- **Zeitplan?** → Unklar! UBI 2 RVO eigentlich geplant für Herbst 2022, aber politische Realitäten erfordern Warten auf EU NIS 2 (voraussichtlich bis 4. Quartal 2022) → Erneuerung des europäischen Minimalkonsens zur KRITIS-Regulierung
- **Politische Entscheidung des BMI:** Entweder UBI 2 RVO ODER Implementierung der Kriterien in das nationale Umsetzungsgesetz für EU NIS 2 („IT-Sicherheitsgesetz 3.0“)
- → Zurzeit keine Klärung in Sicht, könnte aufgrund EU-Umsetzungsfrist bis 2024/2025 in Anspruch nehmen

B. IT-Sicherheitsgesetz 2.0

- **Ergänzung der TOV für KRITIS-Betreiber:** Anordnung der Verwendung von Systemen zur Angriffserkennung (SzA) ab dem 1. Mai 2023 – „kontinuierliche Erfassung geeigneter Parameter und Merkmale aus dem laufenden Betrieb und deren automatische Auswertung“
- **13. Juni 2022:** BSI veröffentlicht Community Draft zum Einsatz von SzA (Protokollierung – Detektion – Reaktion): https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/KRITIS/oh-sza.pdf (Kommentierungsfrist ist abgelaufen)
- **„Lex Huawei“ - Einsatz von kritischen Komponenten und sog. „Garantieerklärung“:** Anzeigepflicht vor erstmaligem Einsatz ggü. BMI – Anzeige beinhaltet „Garantieerklärung“ zur Sicherstellung der IT-Sicherheit durch den Hersteller
- **Allgemeinverfügung des BMI vom 7. Oktober 2021 zur Konkretisierung der Anforderungen an die Garantieerklärung im TK-Sektor:** https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/2021/11/garantieerklaerung-bsig.pdf (nichtamtliche englische Übersetzung)

B. IT-Sicherheitsgesetz 2.0

- **IT-Sicherheitskennzeichen des BSI:** Zusicherung der Hersteller von IT-Produkten, dass ihre Produkte bestimmte IT-Sicherheitseigenschaften besitzen → keine Zertifizierung!
- Konkretisierung durch BSI-IT-Sicherheitskennzeichenverordnung (BSI-ITSiKV) vom 24. November 2021
- Enthält Angaben u.a. zu Antragstellung, Antragsprüfung, Gegenstand der Herstellererklärung, Laufzeit, Verwendung, Erlöschen und Produktkategorien
- **Stand August/September 2022:** Insgesamt 34 IT-Sicherheitskennzeichen in den Kategorien „Breitbandrouter“ und „E-Mail-Dienste“ erteilt, Hersteller:
  - freenet.de
  - LANCOM Systems
  - Mail.de
  - mailbox.org
  - Zyxel

C. EU Cybersicherheitsstrategie

- Vorstellung am 16. Dezember 2020
- **Zielsetzung:** Krisenfestes und digitales Europa
- **Kernpunkte:**
  - Verbesserung mitgliedstaatlicher Kooperation, Abstimmung und Prävention (z.B. durch EU SOCs)
  - Umgang mit dem aus der Corona-Krise resultierenden Digitalisierungsschub
  - Erhöhung des Investitionsniveaus und der Sicherheit in EU-Einrichtungen
- **3 Aktionsfelder:**
  - Widerstandsfähigkeit, technologische Unabhängigkeit und Führungsrolle
  - Aufbau operativer Kapazitäten zur Prävention, Abschreckung und Reaktion
  - Förderung eines globalen offenen Cyberraums durch verstärkte Zusammenarbeit

D. EU NIS 2-Richtlinie

- **Zielsetzung:** Überarbeitung, Aktualisierung und Erweiterung der Anforderungen aus EU NIS (2016) im Hinblick auf die noch weiter fortgeschrittene Vernetzung von Wirtschaft, Staat + Gesellschaft, geänderte Bedrohungslage und die Erkenntnisse aus der Corona-Pandemie (Übersichtsdokument zum Gesetzgebungsprozess: https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/689333/EPRS_BRI(2021)689333_EN.pdf)
- EU-Kommissionsentwurf vorgestellt am 16. Dezember 2020
- Einigung Trilog im Mai 2022, Inkrafttreten von EU NIS 2 vermutlich bis Quartal 4/2022
- Neben EU Cybersecurity Act (CSA, 2019, „Cybersecurity Certification Schemes“) Kernelement europäischer Cybersecurity-Gesetzgebung
- Gesetzliche Implementierung zahlreicher Vorgaben aus der EU Cybersicherheitsstrategie
- **Umsetzungsfrist von 21 Monaten für EU-Mitgliedstaaten:** Nationales „IT-Sicherheitsgesetz 3.0“ zur Implementierung der neuen europarechtlichen Anforderungen

D. EU NIS 2-Richtlinie

Zentrale regulatorische Eckpunkte und Ziele:

- Fokus auf verbesserte Reaktion auf Cyberangriffe und Störfälle, Förderung der praktischen Zusammenarbeit zwischen zentralen Diensten im öffentlichen + privaten Sektor, angemessene Reaktion auf Vorfälle, Sicherheit von Lieferketten, Verschlüsselung und Umgang mit Schwachstellen
- Beseitigung noch bestehender unterschiedlicher Cybersicherheitsanforderungen in den EU-Mitgliedstaaten und Schaffung von Rechtsrahmen/Mechanismen zur wirksamen Zusammenarbeit
- Förmliche Einrichtung des EU-Verbindungsnetzes für Cyberkrisen (EU-CyCLONe), um großflächige Cybersicherheitsvorfälle koordiniert zu bewältigen
- **Einerseits deutliche Erweiterung des Anwendungsbereiches ggü. EU NIS:** Wesentliche und wichtige Einrichtungen, europäisch vereinheitlichte Bezugnahme auf Unternehmensgröße und Size-Cap-Rule (Empfehlung 2003/361/EC) → Größe und nicht Kritikalität entscheidend → gewisse Vergleichbarkeit mit IT-SiG 2.0 (UBI)
- **Andererseits umfassende Bereichsausnahmen vorgesehen:** Verteidigung, nationale Sicherheit, öffentliche/innere Sicherheit, Strafverfolgung, Justiz, Parlamente, Zentralbanken

E. EU Chips Act

- **EU Chips Survey August 2022:** „The findings of the recent Chips Survey launched by the European Commission highlighted that industry expects demand for chips to double by 2030." (https://digital-strategy.ec.europa.eu/en/library/european-chips-survey)
- Umsetzung der Ziele der europäischen digitalpolitischen Strategie
- Unverzügliche Reaktion auf die bereits bestehende Halbleiterkrise
- Bis 2030: Globaler Marktanteil in der Halbleiterfertigung von 20% aus der EU
- **Gesetze dazu allein nicht ausreichend, vielmehr:** Umfassendes Framework, bestehend aus Regularien, Investitionen, Umstrukturierungsplänen der EU-Digitalwirtschaft (u.a. „Common Union Toolbox")
- Neues „European Semiconductor Board", bestehend aus mitgliedstaatlichen Vertretern
- Arbeit der EU-Kommission wird durch neuen Halbleiterausschuss („Semiconductor Committee") unterstützt
- **EU Chips Act nur ein Bestandteil dieses Rahmenwerks:** Bestehend aus operativen Maßnahmen und Forschungsförderung/Strategien

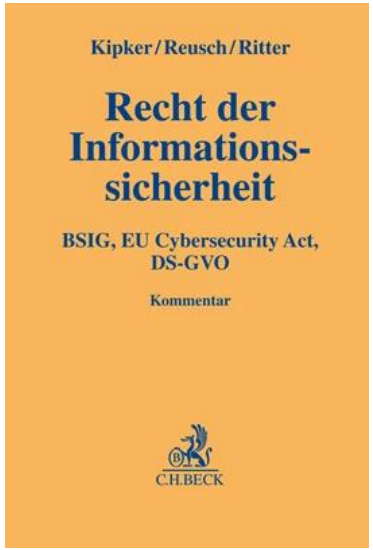
F. RED Delegated Act

- **Cybersecurity und Datenschutz von IoT-Anwendungen:** Problemfeld in Hersteller- und Anwenderkreisen wird seit Jahren diskutiert
- IoT nicht gesetzlich definiert, jedoch über „Funkanlage“ Bezugspunkt in Art. 3 Radio Equipment Directive (RED)
- **Art. 3 Abs. 3 lit. d, e und f RED:** Spezifische Anforderungen für Cybersecurity + Datenschutz
- **Sicherheitsziele abstrakt formuliert:** Technische Konkretisierung durch harmonisierte EU-Normen (hEN)
- **RED Delegated Act:** Gilt ab 1. August 2024 und konkretisiert den Anwendungsbereich der Anforderungen grds. für spezifische Funkanlagen:
  - Mit dem Internet verbundene Funkanlagen
  - Funkanlagen, die personenbezogene Daten, Verkehrsdaten oder Standortdaten verarbeiten
  - Funkanlagen, die Geld, monetäre Werte oder virtuelle Währungen übertragen können

G. EU Cyber Resilience Act

- Stärkung der horizontalen Cybersecurity auf EU-Ebene schon lange Thema/von Branchenverbänden als unzureichend kritisiert
- Verbesserte Anschlussfähigkeit an New Legislative Framework (NLF) zu gewährleisten
- Horizontale Regelungen sollen vertikalen und produktgruppenspezifischen Rechtsakten vorgezogen werden → Ziel: Verhinderung von Fragmentierung/mehr Kohärenz in Anforderungen
- **Cyber Resilience Act:** Kommissionsentwurf vorgestellt am 15. September 2022
- **Regulatorische Aspekte des künftigen EU-Gesetzes:**
  - Breites Spektrum: Materielle digitale Produkte (drahtlos/drahtgebunden), nicht eingebettete Software → „Produkte mit digitalen Elementen“
  - „Security by Design“
  - Schutz der Lieferkette unter Einbeziehung von Produkten aus Drittstaaten
  - Anlehnung an EU-Produkthaftung: Verantwortlichkeit von Herstellern, Importeuren und Vertrieb
  - Pflicht zu Sicherheitsaktualisierungen angelehnt an Produktlebenszyklus, maximal jedoch 5 Jahre
  - Umfassende Reportingpflichten an zuständige Behörden (BSI)

Weiterführende Literatur



Vielen Dank für Ihre Aufmerksamkeit!

Wir gestalten die e-diale Zukunft.
Machen Sie mit.

Ihr Ansprechpartner:

Prof. Dr. Dennis-Kenji Kipker
Legal Advisor
CERT@VDE

Tel. +49 151 40223163
dennis-kenji.kipker@vde.com