Cybersecurity-Regulierung 2021: Update

Dr. Dennis-Kenji Kipker

Übersicht

- Deutsche Cyber-Sicherheitsstrategie 2021
- Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-SiG 2.0)
- The EU's Cybersecurity Strategy for the Digital Decade
- Proposal for a Directive on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148 (NIS 2)
- EU DID- und WK-Richtlinie inkl. nationaler Umsetzungsrechtsakte

Übersicht

- **Deutsche Cyber-Sicherheitsstrategie 2021**
- Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-SiG 2.0)
- The EU's Cybersecurity Strategy for the Digital Decade
- Proposal for a Directive on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148 (NIS 2)
- EU DID- und WK-Richtlinie inkl. nationaler Umsetzungsrechtsakte

Cyber-Sicherheitsstrategie 2021

- Evaluierung und Fortschreibung der deutschen Cyber-Sicherheitsstrategie aus **2016**
- Erste Verfahrensrunde: Sammlung schriftlicher Anmerkungen für alle vier Handlungsfelder
- Zweite Verfahrensrunde: Online-Evaluierungsworkshops in 9/2020
- **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

Cyber-Sicherheitsstrategie 2021

Relevante Anforderungen für die Cyber-Sicherheitsstrategie 2021:

- Explizite Adressierung der digitalen Souveränität
- Möglichkeiten zur Messbarmachung von klar definierten Zielen
- Mehr Usability von IT-Sicherheitslösungen, Aufnahme von „Security by Design“
- Vertiefung der aktiven Einbeziehung von Wissenschaft und Forschung zur Cybersicherheit
- Verbesserung des Unternehmensschutzes durch schnellere Kommunikation und ein optimiertes Krisenmanagement
- Verbesserung der Public Private Partnership (PPP) in der Cybersicherheit

Cyber-Sicherheitsstrategie 2021

Relevante Anforderungen für die Cyber-Sicherheitsstrategie 2021:

- Berücksichtigung nicht nur der Betreiber, sondern auch der Hersteller und Lieferanten von Hard- und Software
- Stärkere Einbeziehung von Unternehmen und Einrichtungen, die keine Kritischen Infrastrukturen darstellen
- Verbesserung der gesamtstaatlichen Cybersicherheitsarchitektur, Intensivierung des Informationsaustausches über Cybervorfälle
- Berücksichtigung, Positionierung und Formulierung der Rolle des zunehmend mit Kompetenzen ausgestatteten BSI innerhalb der gesamtstaatlichen Cybersicherheitsarchitektur
- Schaffung eines einheitlichen EU-Regulierungsrahmens als strategisches Ziel, Deutschland sollte als Vorreiter der europäischen Position agieren

Cyber-Sicherheitsstrategie 2021

→ Aktuell: Beschlussfassung geplant für Mai 2021

Übersicht

- Deutsche Cyber-Sicherheitsstrategie 2021
- **Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-SiG 2.0)**
- The EU's Cybersecurity Strategy for the Digital Decade
- Proposal for a Directive on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148 (NIS 2)
- EU DID- und WK-Richtlinie inkl. nationaler Umsetzungsrechtsakte

IT-SiG 2.0 im Überblick

Ein Thema, zahlreiche Diskussionsstände:

- 27.03.2019 IT-Sicherheitsgesetz 2.0 (90 Seiten, erster Entwurf)
- 05.05.2020 IT-Sicherheitsgesetz 2.0 (73 Seiten, zweiter Entwurf)
- 19.11.2020 IT-Sicherheitsgesetz 2.0 (92 Seiten, dritter Entwurf)
- 01.12.2020 IT-Sicherheitsgesetz 2.0 (92 Seiten, „Diskussionsentwurf“)
- 09.12.2020 IT-Sicherheitsgesetz 2.0 (108 Seiten, Entwurf zur Anhörung der Verbände)
- 11.12.2020 IT-Sicherheitsgesetz 2.0 (119 Seiten)
- 16.12.2020 IT-Sicherheitsgesetz 2.0 (118 Seiten, Kabinettsfassung)

IT-SiG 2.0: Zentrale Aspekte in der Diskussion

Befugnisausbau des BSI:

- Tätigkeit als nationale Behörde für die Cybersicherheitszertifizierung gem. EU CSA
- Entwicklung und Bewertung von Identifizierungs- und Authentisierungsverfahren (Überschneidung mit EU eIDAS-VO), Veröffentlichung eines Stands der Technik bezüglich IT-sicherheitstechnischer Anforderungen von IT-Produkten (Zentralisierung)
- Entwicklung und Festlegung des Stands der Technik durch das BSI (unzureichende Einbindung der Betreiber und von internationalen Standards, Zersplitterung von Anforderungen)
- Ausbau der Funktion des BSI als allgemeine Meldestelle für IT-Sicherheit (zunehmende Frage nach institutioneller Unabhängigkeit)

IT-SiG 2.0: Zentrale Aspekte in der Diskussion

Befugnisausbau des BSI:

- Krisenreaktion: Federführende Entwicklung „Gesamtplan für Reaktionsmaßnahmen des Bundes“
- Erhebliche Störungen: Anforderungsrecht für bestimmte (auch personenbezogene) Daten und Eingriffsbefugnis in Systeme und unternehmerische Prozesse zu ihrer Wiederherstellung (Schutz von Geschäftsgeheimnissen/Umgehung unternehmenseigener Reaktionspläne)
- „Hackerparagraf“: Detektion von Sicherheitslücken in öffentlich erreichbaren Systemen (Portscans, Sinkholes, Honeypots: Gefährdung der Stabilität von Systemen, unzureichende Informationsweitergabe)
- Zentrale „Sammelstelle“ aller möglichen Daten zur IT-Sicherheit und Kooperation mit anderen Bundesbehörden unter BMI-Ägide (auch Datenschutz)

IT-SiG 2.0: Zentrale Aspekte in der Diskussion

Erweiterte Betreiberpflichten für KRITIS:

- Implementierung eines Systems zur Angriffserkennung mit dem Ziel der Störungsvermeidung, Informationsweitergabe an das BSI
- Übermittlung einer Liste aller IT-Produkte mit Bedeutung für die Funktionsfähigkeit der Kritischen Infrastruktur an das BSI (sinnlose Datenakkumulation/Geheimnisschutz/Datenschutz)
- Erweiterung: Unternehmen im besonderen öffentlichen Interesse (mehrfache Änderung der Bezugspunkte und Bestimmungsgrößen, unklare Anknüpfungspunkte) mit ggü. KRITIS herabgesetzten Pflichten

IT-SiG 2.0: Zentrale Aspekte in der Diskussion

Regulierung der Hersteller:

- Freiwilliges nationales IT-Sicherheitskennzeichen (Konflikt mit EU CSA/nationaler Alleingang/konkreter Verbrauchermehrwert?)
- Einsatz von kritischen Komponenten und Garantieerklärung des Herstellers (5G- und Huawei-Debatte: Lieferkettennachweis technisch und organisatorisch möglich?/faktische Auswirkungen auf Nicht-KRITIS/Bestandsschutz?/Verlagerung der politischen Debatte um „Digitale Souveränität“ in nationales Gesetz)

IT-SiG 2.0: Stellungnahmen und Kritik

- **Bestimmung der Unternehmen im besonderen öffentlichen Interesse:** Kriterien und Rechtssicherheit, Notwendigkeit
- **Verarbeitung von Protokolldaten und Bestandsdatenauskunft:** Umfassende Speichermöglichkeiten für Protokoll- und Bestandsdaten inkl. IP-Adressen, Einschränkung datenschutzrechtlicher Betroffenenrechte
- **Detektion von Sicherheitsrisiken für die Netz- und IT-Sicherheit und von Angriffsmethoden:** Fehlende Vorankündigung der Maßnahmen
- **Unübersichtliche Bußgeldvorschriften:** Zweiter RefE Gleichlauf mit EU DS-GVO, darüber hinaus aber auch Verweise auf OWiG vorgesehen
- **Mangelnde Rechtssicherheit und Bestimmtheit:** Essenzielle Festlegungen durch Allgemeinverfügung und RVO

IT-SiG 2.0: Kabinettsfassung

Betroffene Vorschriften:

- BSI-Gesetz
- Telekommunikationsgesetz
- Gesetz über die Elektrizitäts- und Gasversorgung (EnWG)
- Außenwirtschaftsverordnung
- Zehntes Buch Sozialgesetzbuch (SGB X)

IT-SiG 2.0: Kabinettsfassung

BSIG: Was ist geblieben, was wird weiter diskutiert?

- Ergänzung von KRITIS: „Siedlungsabfallentsorgung“
- Regelung und Definition von „Kritischen Komponenten“ („auf Grund eines Gesetzes“)
- Regelung und Definition von „Unternehmen im besonderen öffentlichen Interesse“ (Verweise auf § 60 AWV, größte Unternehmen nach Wertschöpfung, Verweis auf Störfall-VO)
- Aufgabenfestlegungen BSI: Entwicklung und Veröffentlichung eines Stands der Technik bei sicherheitstechnischen Anforderungen an IT-Produkte

IT-SiG 2.0: Kabinettsfassung

BSIG: Was ist geblieben, was wird weiter diskutiert?

- Umfassende Kontrollmöglichkeiten der Kommunikationstechnik des Bundes seitens BSI, Betretensrechte
- BSI als allgemeine Meldestelle für Sicherheit in der Informationstechnik, weiterer Ausbau und Datenumgang
- Erhebung und Verarbeitung von Protokollierungsdaten, die durch den Betrieb der Kommunikationstechnik des Bundes anfallen
- Bestandsdatenauskunft des BSI bei TK-Anbietern, auch nach IP-Adressen inkl. Übermittlungsbefugnis personenbezogener Daten
- Erweiterte Warnmöglichkeiten des BSI inkl. Ausnahmen von der Herstellerbenachrichtigung bei festgestellten IT-Sicherheitslücken

IT-SiG 2.0: Kabinettsfassung

BSIG: Was ist geblieben, was wird weiter diskutiert?

- Untersuchungsmöglichkeit der Sicherheit in der Informationstechnik inkl. Weiterübermittlungsbefugnisse an weitere Behörden
- Detektion von Sicherheitsrisiken für die Netz- und IT-Sicherheit und von Angriffsmethoden **(Portscans)** anhand vorab bestimmter sog. „Weißer Liste“ mit intendiertem Ermessen zur Information des Verantwortlichen; Maßnahmen zur Vortäuschung von Angriffen
- Anordnungsbefugnisse zur IT-Sicherheit ggü. TK-Diensteanbietern mit mehr als 100.000 Kunden, Befugnis zur Datenumleitung (vergleichbare Regelung auch für TM-Diensteanbieter)

IT-SiG 2.0: Kabinettsfassung

BSIG: Was ist geblieben, was wird weiter diskutiert?

- Anordnung der Verwendung von Systemen zur Angriffserkennung durch KRITIS-Betreiber
- Pflicht zur Registrierung und Benennung einer Kontaktstelle von KRITIS-Betreibern beim BSI inkl. Ersatzvornahmemöglichkeit des BSI
- Datenherausgabepflicht von KRITIS-Betreibern ggü. BSI zur Bewältigung erheblicher Störungen
- TOM-Regelungen zur IT-Sicherheit von Unternehmen im besonderen öffentlichen Interesse ggü. KRITIS abgeschwächt (u.a. Selbsterklärung), Registrierung und Kontaktstelle, Meldepflichten

IT-SiG 2.0: Kabinettsfassung

BSIG: Was ist geblieben, was wird weiter diskutiert?

- Untersagung des Einsatzes kritischer Komponenten: Anzeigepflicht vor Einsatz in KRITIS, Garantieerklärung des Herstellers (Festlegung der Anforderungen durch Allgemeinverfügung), Untersagungsbefugnis des BMI, Anforderungen an die Vertrauenswürdigkeit des Herstellers, Herstellerausschluss
- **Freiwilliges IT-Sicherheitskennzeichen:** Festlegung durch TR des BSI und konkretisierende RVO, Freigabe durch BSI vor Verwendung
- **Bußgeldvorschriften:** Abstufungen 2 Millionen Euro, 1 Million Euro, 500.000 Euro, 100.000 Euro, beachte Verweis auf § 30 Abs. 2 S. 3 OWiG (vgl. auch bisherige Kritik)!

IT-SiG 2.0: Zeitplan

- Beschlussfassung Bundeskabinett am 16.12.2020
- Zurzeit Notifizierung durch EU-Kommission (ca. drei Monate)
- Bereits vor Rückmeldung aus Brüssel möglich: Erste Lesung im Bundestag, Verabschiedung jedoch erst nach Ende der Notifizierung
- **Möglicher Termin zur Verabschiedung:** Letzte Sitzungswoche vor Ostern (22.3.21-26.3.21)
- **Wahrscheinlich:** Verabschiedung vor der parlamentarischen Sommerpause (Ende der Legislaturperiode)

Übersicht

- Deutsche Cyber-Sicherheitsstrategie 2021
- Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-SiG 2.0)
- **The EU's Cybersecurity Strategy for the Digital Decade**
- Proposal for a Directive on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148 (NIS 2)
- EU DID- und WK-Richtlinie inkl. nationaler Umsetzungsrechtsakte

The EU's Cybersecurity Strategy for the Digital Decade

- Vorstellung am 16.12.2020
- **Zielsetzung:** Krisenfestes und digitales Europa
- **Kernpunkte:**
  - EU-weites Netz aus Security Operations Centres (SOCs)
  - Verbesserung mitgliedstaatlicher Kooperation, Abstimmung und Prävention
  - 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

Widerstandsfähigkeit, technologische Unabhängigkeit und Führungsrolle

- IT-Sicherheit im öffentlichen und privaten Raum umfasst
- Betrifft u.a. Überarbeitung der **NIS-RL hin zu NIS 2**
- Vorschlag für neue **Richtlinie zur Widerstandsfähigkeit Kritischer Infrastrukturen** (ersetzt entsprechende RL aus 2008)
- Umsetzung der in der **Security Union Strategy 2020-2025** angekündigten Ziele
- **Erweiterung KRITIS:** Energie, Verkehr, Banken, Finanzmarktinfrastrukturen, Gesundheit, Trinkwasser, Abwasser, digitale Infrastruktur, öffentliche Verwaltung, Raumfahrt
- Schutz von digitalisierten demokratischen Prozessen und Institutionen
- Ausbau und Etablierung eines sog. **„EU Cyber Shield“**: Überregionales Monitoring und Datenanalyse (CSIRTs/SOCs/KI)
- Aufbau eines „ultrasicheren Kommunikationsnetzes“/**Quantenkommunikation**/ 5G-Sicherheit und digitale Souveränität (eigener Anhang)
- Softwareupdates, Datenschutz und IoT-Security

Aufbau operativer Kapazitäten zur Prävention, Abschreckung und Reaktion

- Angemessene Reaktion auf Cyberangriffe
- Schaffung einer gemeinsamen Cyber-Union **(Joint Cyber Unit, JCU)**: Gemeinsame Anlaufstelle für private und staatliche Einrichtungen im Bereich der Strafverfolgung und Verteidigung mit Bezug zur IT-Sicherheit
- 2021 detaillierter Plan zum Ausbau der JCU
- **Unionsweite Abschreckungsstrategie:** Reaktion mit Gegenmaßnahmen auf Angriffe im digitalen Raum
- **„Diplomatic toolbox“:** Politisch einheitliche Reaktion auf nachgewiesene Cyberangriffe

Förderung eines globalen offenen Cyberraums durch verstärkte Zusammenarbeit

- Intensivierung der Zusammenarbeit mit Drittstaaten auf internationaler Ebene
- Schutz von Menschenrechten und Grundfreiheiten im gesamten Cyberraum
- Erarbeitung einschlägiger **Normen**, die einem internationalen Standard entsprechen
- Vergrößerung des bisherigen Investitionsvolumens
- Aufbau des neuen **Kompetenzzentrums für Cybersicherheit** in Bukarest/Rumänien
- Stärkung der strategischen Autonomie und Führungsrolle in der Cybersecurity und zum Schutz der digitalen Lieferkette **(z.B. Cloud, Prozessortechnologien, sichere Konnektivität, 6G-Netze)**

Übersicht

- Deutsche Cyber-Sicherheitsstrategie 2021
- Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-SiG 2.0)
- The EU's Cybersecurity Strategy for the Digital Decade
- **Proposal for a Directive on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148 (NIS 2)**
- EU DID- und WK-Richtlinie inkl. nationaler Umsetzungsrechtsakte

EU NIS 2-Richtlinie: Eckpunkte

- Zusammen mit der neuen EU-Cybersicherheitsstrategie am 16.12.2020 als Entwurfsfassung vorgestellt
- **Neufassung und Erweiterung des Anwendungsbereichs:** z.B. öffentliche Verwaltung und Raumfahrt als neue Sektoren; Fernwärme/Fernkälte und Wasserstoff als Teilsektoren
- Identifikations- und Überprüfungspflicht der Mitgliedstaaten hinsichtlich Infrastrukturen, Übermittlung an EU-Kommission
- Pflicht zu Maßnahmen richtet sich danach, ob eine Einrichtung als **„wesentlich“** oder **„wichtig“** eingestuft wird
- Neue Definitionen von „Sicherheitsvorfall“ und „Cyberbedrohung“

EU NIS 2-Richtlinie: Eckpunkte

- Steigerung der Anforderungen an die nationalen Cybersicherheitsstrategien
- CSIRTs der Mitgliedsstaaten sollen Netz- und Informationssysteme proaktiv scannen
- Befugnis zur Durchführung von **„Hackbacks“** weiterhin fraglich
- **ENISA:** Erstellung eines Registers, in das Sicherheitslücken von IKT-Produkten und -Diensten eingetragen werden können
- Weitere Intensivierung des Informationsaustauschs und der Kooperation zwischen den mitgliedstaatlichen Behörden, z.B. im **„EU-CyCLONe“** zur Abwehr großangelegter Cybersecurity-Vorfälle

EU NIS 2-Richtlinie: Eckpunkte

- Berichte zum Stand der EU Cybersecurity, Bewertung der Cybersecurity-Strategien und Umsetzungen der Mitgliedstaaten
- Bestimmung von Anforderungen an das Cybersicherheitsrisikomanagement und für Benachrichtigungspflichten von Unternehmen, **Privacy by Design**
- Widerstreit **„Sicherheit durch Verschlüsselung und Sicherheit trotz Verschlüsselung“** (z.B. bei Ermittlung von Straftaten)
- Sicherheitsrisikobewertung von **Versorgungsketten**, insb. im Bereich IKT
- **Verzahnung mit EU CSA** zur Nachweiserbringung in der IT-Sicherheit

EU NIS 2-Richtlinie: Eckpunkte

- **Einbeziehung europäischer und internationaler Standardisierung**, Anregung der Nutzung von Standards
- Verbesserung des Informationsaustausches zur Cybersicherheit nichtstaatlicher Einrichtungen im Einklang mit der EU DS-GVO (wohl vergleichbar mit UP KRITIS)
- **Mehr behördliche Aufsichts- und Durchsetzungsbefugnisse**, insb. auch im Hinblick auf kritische Unternehmen (z.B. Stichproben, Kontrolle vor Ort und remote, Security Scans, Mitteilungspflichten für Security Breaches, erhebliche finanzielle Sanktionen inkl. Datenschutzverstöße, Betriebsuntersagung, bis hin zu „Temporary Ban“ von Leitungsaufgaben natürlicher Personen und deren Haftbarkeit)

Übersicht

- Deutsche Cyber-Sicherheitsstrategie 2021
- Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-SiG 2.0)
- The EU's Cybersecurity Strategy for the Digital Decade
- Proposal for a Directive on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148 (NIS 2)
- **EU DID- und WK-Richtlinie inkl. nationaler Umsetzungsrechtsakte**

EU DID- und WK-Richtlinie

- **DID-Richtlinie:** Richtlinie über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte (2019/770)
- **WK-Richtlinie:** Richtlinie über bestimmte vertragsrechtliche Aspekte des Warenkaufs (2019/771)
- **Anwendungsbereich:** Streamingportale, Cloud, Datenaustauschdienste, Social Networks, IoT
- **Ziel:** Stärkung der verbraucherbezogenen IT-Sicherheit (B2C), u.a. durch Anordnung von Updatepflichten für Software
- **Relevanz:** Über Lieferketten mittelbar Rückgriff auch auf B2B, allgemeine rechtspolitische Tendenz hin zu mehr IT-Sicherheit
- **Zeitplan:** Veröffentlichung der RL in 5/2019, Umsetzungsgesetz bis 7/2021, Inkrafttreten zu 1/2022

Cybersecurity-Regulierung 2021: Update

Dr. Dennis-Kenji Kipker