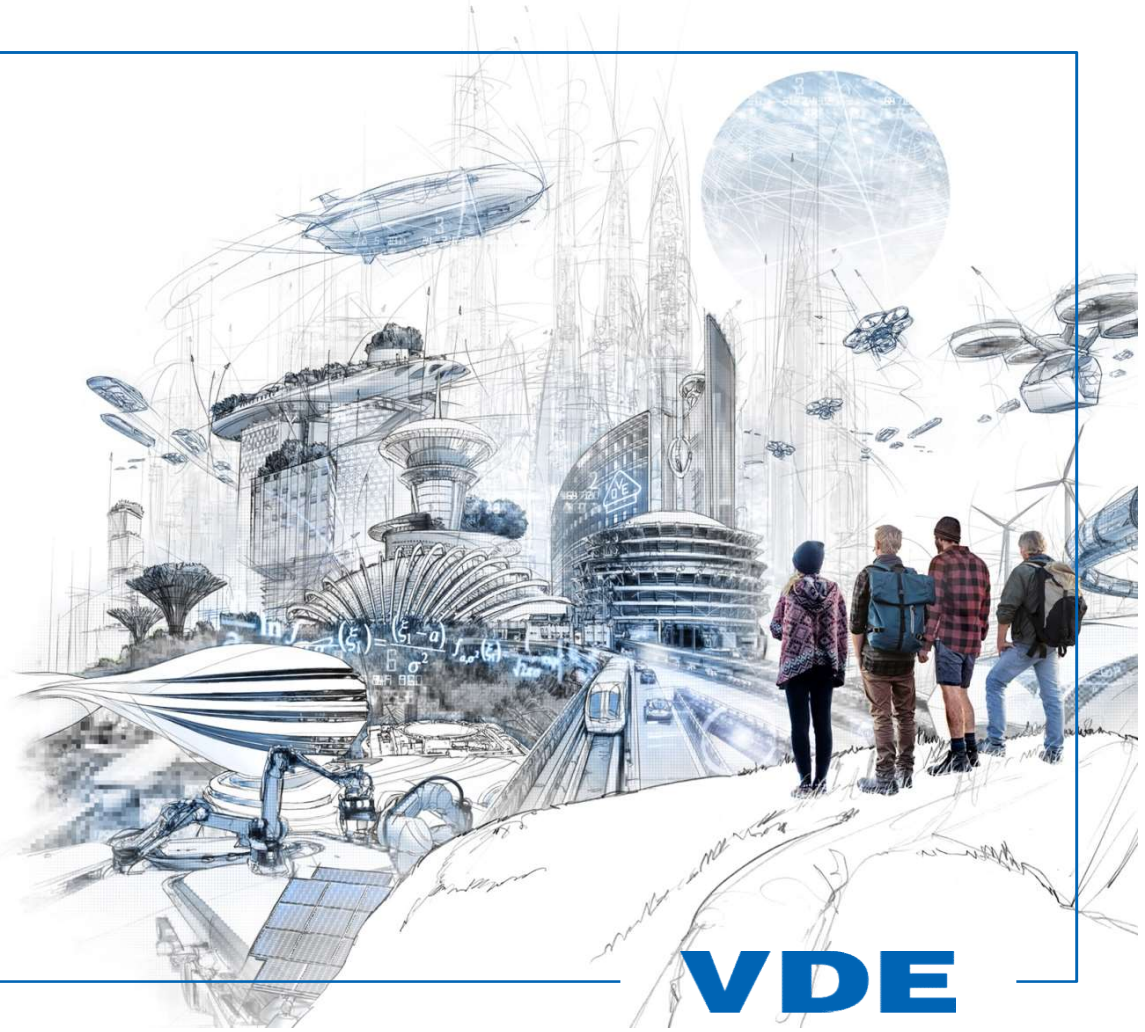
# Update
# IT-Sicherheitsrecht

Dr. Dennis-Kenji Kipker

Frankfurt, 18.05.2021



# Übersicht: „Zoo of Regulations“

- 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
- Dritte Verfahrensrunde: Eckpunktepapier zur CSS 2021 in 3/2021 – gemeinsame, von allen Ressorts der Bundesregierung mitgetragene Grundlage zur Erstellung der CSS 2021
- **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
- **Aspekte:** Leitlinien, Handlungsfelder, strategische Umsetzung (strategisches Controlling, Überprüfung der operativen Umsetzung)

# Cyber-Sicherheitsstrategie 2021

**Leitlinien CSS 2021:**

- Leitlinien sind 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 (zB E-Government, Mobile Work, 5G, Homeschooling)
- **Effektivität und Messbarkeit:** Überprüfbarkeit der Ziele der CSS 2021, strategisches Controlling durch BMI

# Cyber-Sicherheitsstrategie 2021

**Relevante Anforderungen aus dem Handlungsfeld 1:**

- Adressierung „schwächerer“ Gruppen: KMU, Bildungs- und Sozialeinrichtungen, Verbände, Vereine, Verbraucher → Anwenderfreundlichkeit!
- Cybersicherheit als Qualitätsmerkmale für digitale Produkte und Dienstleistungen, die im EU-Binnenmarkt angeboten werden
- Fortschritte für elektronische Identitäten (eIDs)
- Entwicklung eines europaweit gültigen IT-Sicherheitskennzeichens (mit verbindlichem Charakter)
- Weiterverfolgung der Ziele der deutschen Krypto-Strategie
- IT-Sicherheit für KI und IT-Sicherheit durch KI
- Schlüsseltechnologien: Quantencomputing, 6G, Security by Design
- Bekämpfung hybrider Bedrohungen, insb. Desinformation

# Cyber-Sicherheitsstrategie 2021

**Relevante Anforderungen aus dem Handlungsfeld 2:**

- Bessere Vernetzung mit Unternehmen: Stärkerer Beitrag Cyber-Sicherheit, „Cyber-Sicherheit als integraler Bestandteil des Wirtschaftsschutzes“
- Mehr offene Basistechnologien, mehr offene Standards für sichere Hard- und Software
- Neue Prüf- und Abnahmeverfahren unter Berücksichtigung von Time-to-Market
- Mehr Informationen für und Unterstützung von Unternehmen
- Ausbau der Anforderungen für KRITIS-Betreiber
- EU-weite Definition gesetzlicher Anforderungen und Normen und Standards → Vermeidung von Doppelregulierung
- Stärkung der nationalen, europäischen und internationalen Standardisierung → nationale und europäische Standardisierungs- und Zertifizierungsverfahren sollen international führend bleiben

# Cyber-Sicherheitsstrategie 2021

**Relevante Anforderungen aus dem Handlungsfeld 3:**

- Strukturelle und prozessuale Bewertung der Cyber-Sicherheitsarchitektur des Bundes
- Cyber-Abwehrzentrum: Intensivierung und Verbesserung des Informationsaustauschs, Einbeziehung weiterer Akteure, SOC-Verbund von Bund und Ländern
- BSI als dritte Säule einer föderal integrierten Cyber-Sicherheitsarchitektur (neben BKA und BfV)
- Befugnisausbau: Verbunddatenbank für Indicators of Compromise beim BSI, Unterstützung im Verhältnis Bund-Länder, Stärkung der Zentralstellenfunktion des BKA für Cybercrime
- „Ausgleich der Interessen von Cybersicherheit und Sicherheitsbehörden“: Umgang mit Schwachstellen, Ausbau der Rolle von ZITiS
- Mehr Befugnisse der Sicherheitsbehörden des Bundes für Gefahrenabwehr und Cybercrime
- Aufbau eines gesamtstaatlichen Risk Assessment-Prozesses: Übergang zur Cyber-Verteidigung

# Cyber-Sicherheitsstrategie 2021

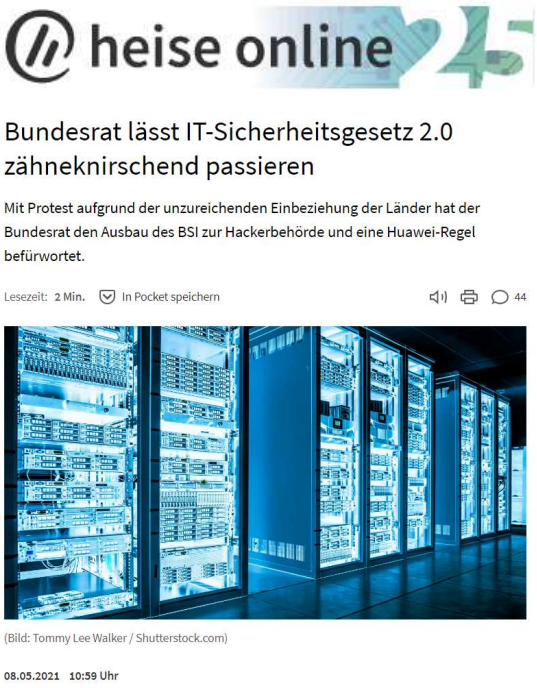
**Relevante Anforderungen aus dem Handlungsfeld 4:**

- Angleichung europäischer und nationaler Ziele zur Cybersicherheit, z.B. mit Blick auf die neue EU Cyber-Sicherheitsstrategie, die NIS-RL und den Entwurf der NIS 2-RL
- Einflussnahme auf EU und internationale Cyber-Sicherheitspolitik inkl. NATO-Standardisierung
- Aktive Einbringung Deutschlands in die EU-Strategie zur Cyber-Sicherheit
- Aktive Positionierung der EU in der internationalen Cyber-Sicherheitspolitik
- Verbesserung internationaler operativer Zusammenarbeit, Bekämpfung von Cybercrime, grenzüberschreitende Strafverfolgung
- Einbringung in und Weiterentwicklung der Cyber-Verteidigungspolitik der NATO (u.a. als „Domäne der Operationsführung“)
- Stärkung der EU-NATO-Zusammenarbeit in Cyber-Verteidigung und Resilienz

# 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 zeitlichen Verlauf



heise online

Bundesrat lässt IT-Sicherheitsgesetz 2.0 zähneknirschend passieren

Mit Protest aufgrund der unzureichenden Einbeziehung der Länder hat der Bundesrat den Ausbau des BSI zur Hackerbehörde und eine Huawei-Regel befürwortet.

Lesezeit: 2 Min. In Pocket speichern 44

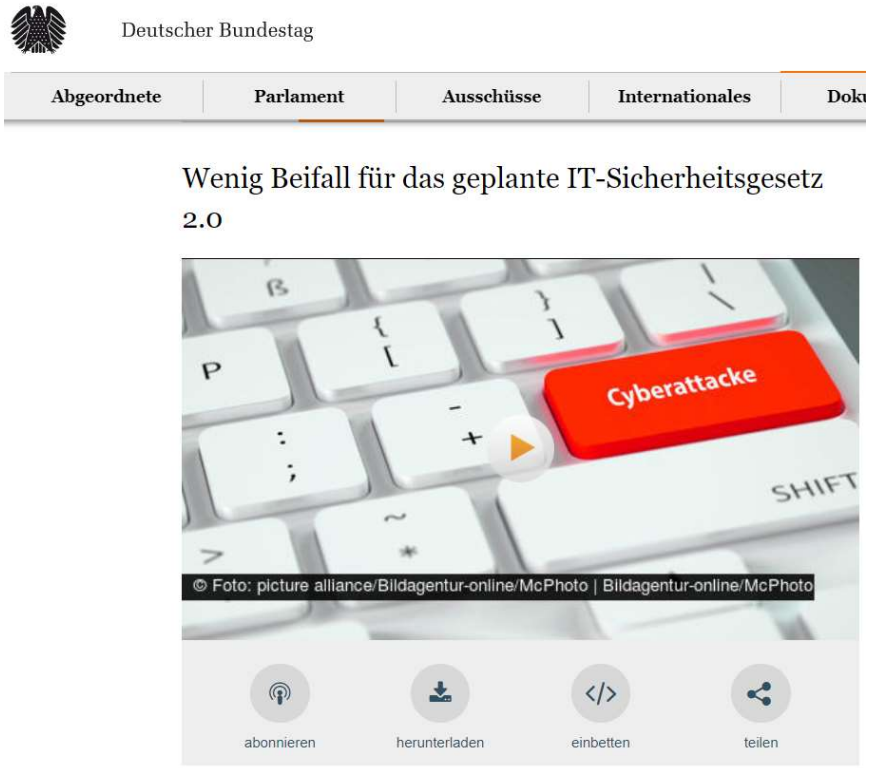
(Bild: Tommy Lee Walker / Shutterstock.com)

08.05.2021 10:59 Uhr

**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)
- …
- 16.12.2020: IT-Sicherheitsgesetz 2.0 (118 Seiten, Kabinettsfassung, Drs. 16/21 vom 01.01.2021)
- 01.03.2021: Anhörung im Ausschuss für Inneres und Heimat
- 23.04.2021: Annahme des Gesetzentwurfs durch den Bundestag
- 07.05.2021: Billigung durch den Bundesrat
- Bis 6/2021: Ausfertigung und Verkündung im BGBl.

# IT-SiG 2.0: „Wenig Beifall für das geplante IT-Sicherheitsgesetz“



# IT-SiG 2.0: Gesetzentwurf der Bundesregierung (Drs. 19/26106)

**Betroffene Vorschriften:**

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

# IT-SiG 2.0: Gesetzentwurf der Bundesregierung (Drs. 19/26106)

- **Ergänzung von KRITIS:** „Siedlungsabfallentsorgung“
  - Ca. 100 zusätzliche Betreiber erwartet
- 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)
  - **Wertschöpfungskriterium:** Orientierung an Gutachten der Monopolkommission S. 80 ff., 100 größte Unternehmen Deutschlands nach inländischer Wertschöpfung
- **Aufgabenfestlegungen BSI:** Entwicklung und Veröffentlichung eines Stands der Technik bei sicherheitstechnischen Anforderungen an IT-Produkte (ohne Berücksichtigung von Normen/Standards, ohne Einbeziehung von betroffenen Wirtschaftsverbänden)

# Hauptgutachten der Monopolkommission 2020 (Auszug)

**Tabelle II.1: Die nach inländischer Wertschöpfung 100 größten Unternehmen im Berichtsjahr 2018[1]**

| Rang/ Trend[2] | | Unternehmen[3] | Wertschöpfung[4] in Mio. EUR (Veränderung in %) | | Beschäftigte | Geschäftsvolumen in Mio. EUR/Branche[5] | |
|---|---|---|---|---|---|---|---|
| 1 | — | Volkswagen AG | 31.517 | (+ 26.8) | 292.729 | 158.844 | i |
| 2 | — | Daimler AG | 18.474 | (- 12.8) | 174.663 | 113.590 | i |
| 3 | — | Bayerische Motoren Werke AG | 14.224 | (+ 0.1) | 92.725 | 80.464 | i |
| 4 | ↑ | Deutsche Bahn AG | 13.347 | (+ 13.3) | 196.334 | 24.970 | d |
| 5 | ↓ | Robert Bosch GmbH | 12.551 | (- 3.0) | 139.422 | 47.668 | i |
| 6 | ↓ | Siemens AG | 12.056 | (+ 0.6) | 113.000 | 35.198 | i |
| 7 | — | Deutsche Telekom AG | 11.443 | (- 2.3) | 98.092 | 24.358 | d |
| 8 | ↑ | INA-Holding Schaeffler GmbH & Co. KG | 8.506 | (+ 12.1) | 96.675 | 20.858 | i |
| 9 | ↓ | Deutsche Post AG | 8.160 | (+ 2.1) | 145.628 | 14.353 | d |
| 10 | — | Bayer AG | 7.672 | (+ 4.5) | 32.140 | 19.002 | i |
| 11 | ↑ | Deutsche Lufthansa AG | 6.951 | (+ 14.6) | 72.716 | 25.231 | d |
| 12 | ↑ | REWE-Gruppe | 6.547* | (+ 31.6) | 178.453 | 43.634 | h |
| 13 | ↓ | BASF SE | 6.483 | (- 2.9) | 53.534 | 18.365 | i |
| 14 | ↑ | Deutsche Bank AG | 6.480 | (+ 55.2) | 41.669 | 845.272 | k |
| 15 | ↓ | SAP SE | 6.078 | (+ 6.7) | 21.122 | 15.718 | d |
| 16 | ↑ | Airbus-Gruppe Deutschland | 5.485* | (+ 16.4) | 45.387 | 17.725 | i |
| 17 | ↓ | Fresenius SE & Co. KGaA | 5.258 | (+ 0.5) | 88.086 | 10.131 | i |
| 18 | ↑ | ZF Friedrichshafen AG | 5.000 | (+ 24.1) | 50.794 | 14.498 | i |
| 19 | — | Vonovia SE | 4.579 | (- 1.2) | 8.989 | 3.684 | d |
| 20 | ↓ | Schwarz-Gruppe | 4.510* | (- 6.9) | 150.000 | 36.600* | h |
| 21 | ↓ | thyssenkrupp AG | 4.360 | (+ 0.5) | 62.227 | 22.391 | i |
| 22 | neu | E.ON SE | 3.866 | | 15.400 | 13.852 | i |
| 23 | ↑ | Roche-Gruppe Deutschland | 3.697* | (+ 6.2) | 13.659 | 6.795 | i |
| 24 | ↓ | Allianz SE | 3.694 | (- 11.8) | 37.566 | 27.566 | v |
| 25 | ↑ | Merck KGaA | 3.654 | (+ 163.1) | 13.056 | 4.612 | i |

# IT-SiG 2.0: Gesetzentwurf der Bundesregierung (Drs. 19/26106)

- **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** bei der Untersuchung der IT-Sicherheit von auf dem Markt bereitgestellten Produkten und Systemen, Weiterübermittlungsbefugnisse an andere Behörden

# IT-SiG 2.0: Gesetzentwurf der Bundesregierung (Drs. 19/26106)

- Detektion von Sicherheitsrisiken für die Netz- und IT-Sicherheit und von Angriffsmethoden **(Portscans)** anhand vorab bestimmter sog. „Weißer Liste“; **Maßnahmen zur Vortäuschung von Angriffen** (Honeypots, Sinkholes)
  - **Weiße Liste:** IP-Adressraum bezieht sich nur auf statische Adressen, weiße Liste enthält IP-Adressbereiche
  - **Quellen der Adressbereiche:** Provider, Domainnamensverwaltung, Adressinformationssysteme, Erfahrungen des und Mitteilungen an das BSI
- **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: Gesetzentwurf der Bundesregierung (Drs. 19/26106)

- Anordnung der Verwendung von **Systemen zur Angriffserkennung durch KRITIS-Betreiber**
  - Ergänzung der TOV
  - Kontinuierliche Erfassung geeigneter Parameter und Merkmale aus dem laufenden Betrieb und deren automatische Auswertung
- Zusätzlich zur Kontaktstelle: Pflicht zur **Registrierung von KRITIS-Betreibern beim BSI** inkl. Ersatzvornahmemöglichkeit des BSI
  - Registrierung erfordert die Angabe zusätzlicher Informationen zur Kritischen Infrastruktur
- **Datenherausgabepflicht inkl. personenbezogener Daten von KRITIS-Betreibern ggü. BSI** zur Bewältigung erheblicher Störungen
- **TOV-Regelungen zur IT-Sicherheit von Unternehmen im besonderen öffentlichen Interesse ggü. KRITIS abgeschwächt** (u.a. Selbsterklärung), Registrierung und Kontaktstelle, Meldepflichten bei Störungen → Nachweispflicht ggü. BSI bei Nichterfüllung

# IT-SiG 2.0: Gesetzentwurf der Bundesregierung (Drs. 19/26106)

- **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 **(neu gefasst mit Drs. 19/28844)**
- **Freiwilliges IT-Sicherheitskennzeichen:** Festlegung durch TR des BSI und konkretisierende RVO, Freigabe durch BSI vor Verwendung **(Änderung durch Drs. 19/28844)**
- **Bußgeldvorschriften:** Abstufungen 2 Millionen Euro, 1 Million Euro, 500.000 Euro, 100.000 Euro, beachte Verweis auf § 30 Abs. 2 S. 3 OWiG (max. 20 Millionen Euro → Kritik an Verhältnismäßigkeit/Leistbarkeit) **(unverändert übernommen)**

# IT-SiG 2.0: Stellungnahmen und Kritik aus dem Gesetzgebungsverfahren

- **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 zur Bußgeldmaximierung vorgesehen
- **Mangelnde Rechtssicherheit und Bestimmtheit:** Essenzielle Festlegungen durch Allgemeinverfügung und RVO

# IT-SiG 2.0: Beschlussempfehlung des Innenausschusses (Drs. 19/28844)

- **Definition des BSI:** Mehr Unabhängigkeit, Aufgabenwahrnehmung auf der „Grundlage wissenschaftlich-technischer Erkenntnisse“
- **Definition der IT-Produkte:** Software, Hardware sowie alle einzelnen oder miteinander verbundenen Komponenten, die Informationen informationstechnisch verarbeiten
- **Definition kritischer Komponenten:** Streichung des Kriteriums „von hoher Bedeutung für das Funktionieren des Gemeinwesens“
- **Definition der Unternehmen im besonderen öffentlichen Interesse (Nr. 2, „Wertschöpfung“):** Ergänzung um Zulieferer, die wegen ihrer Alleinstellungsmerkmale von wesentlicher Bedeutung sind → Konkretisierung? KMU?

# IT-SiG 2.0: Beschlussempfehlung des Innenausschusses (Drs. 19/28844)

- **Ergänzung der Aufgaben des BSI:**
  - Empfehlungen für Identifizierungs- und Authentisierungsverfahren und Bewertung dieser
  - Beschreibung und Veröffentlichung eines Stands der Technik bei sicherheitstechnischen Anforderungen an IT-Produkte unter Berücksichtigung bestehender Normen und Standards sowie Einbeziehung der Wirtschaftsverbände
- **Speicherfrist für Protokolldaten zur Abwehr von Gefahren für die Kommunikationstechnik des Bundes:** Erhebliche Ausdehnung der Maximalspeicherfrist von 3 auf 18 Monate
- **Aktive Detektionsbefugnis des BSI („Hackerbehörde“):** Ausdehnung der Benachrichtigungspflicht ggü. Verantwortlichem durch Streichung der Ausnahme „entgegenstehender überwiegender Sicherheitsinteressen“ und Ergänzung von „Unverzüglichkeit“ der Mitteilung

# IT-SiG 2.0: Beschlussempfehlung des Innenausschusses (Drs. 19/28844)

- **Neufassung der Regelung zum Einsatz kritischer Komponenten („Lex Huawei“):**
  - Grds. Anzeigepflicht ggü. BMI vor erstmaligem Einsatz
  - Untersagungsbefugnis des BSI bis zum Ablauf von zwei Monaten bei Beeinträchtigung von öffentlicher Ordnung oder Sicherheit (Indizien: drittstaatliche Kontrolle, vergangene nachteilige Beteiligungen des Herstellers, sicherheitspolitische Ziele)
  - Aufrechterhaltung der sog. „Garantieerklärung“ ggü. KRITIS-Betreiber, Festlegung der Anforderungen durch Allgemeinverfügung des BMI
  - Nachträgliche Untersagungsbefugnis des Einsatzes durch BMI inkl. Indizienkatalog bis hin zum kompletten Herstellerverbot
- **Freiwilliges IT-Sicherheitskennzeichen („Verbrauchersiegel“):** Vorrang von Normen/Standards und branchenabgestimmten IT-Sicherheitsvorgaben vor TR des BSI zur Festlegung der Anforderungen

# Entwurf einer zweiten Verordnung zur Änderung der BSI-Kritisverordnung (BSI-KritisV)

- Veröffentlichung durch das BMI am 26.04.2021, Frist zur Stellungnahme bis 17.05.2021
- Bestimmt ua zahlenmäßige Schwellenwerte, ab wann eine bestimmte Anlagenkategorie zu KRITIS iSd IT-SiG gehört, sodass eine Pflicht zu TOV gilt
- **Ausgewählte Neuerungen:**
  - Software und IT-Dienste, die für die Erbringung einer kritischen Dienstleistung notwendig sind, werden als Anlagen im Sinne der Verordnung identifiziert
  - Mehrere Anlagen, die durch einen betriebstechnischen Zusammenhang verbunden sind, gelten als gemeinsame Anlage, wenn sie zur Erbringung derselben kritischen Dienstleistung notwendig sind
  - Betreiben zwei oder mehr Personen gemeinsam eine Anlage, so ist jeder für die Erfüllung der Pflichten als Betreiber verantwortlich
  - Teilweise geänderte bzw. deutlichere Aufschlüsselung der Definitionen in den einzelnen Sektoren, Ergänzung neuer Kriterien und kritischer Dienstleistungen, teilweise Änderungen in den Schwellenwerten inkl. Bemessungskriterien
- **Insgesamt führt Herabsetzung der Schwellenwerte zu einer Ausdehnung des Betroffenenkreises der KRITIS-Vorgaben: 270 zusätzliche Betreiber werden erwartet**

# 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)

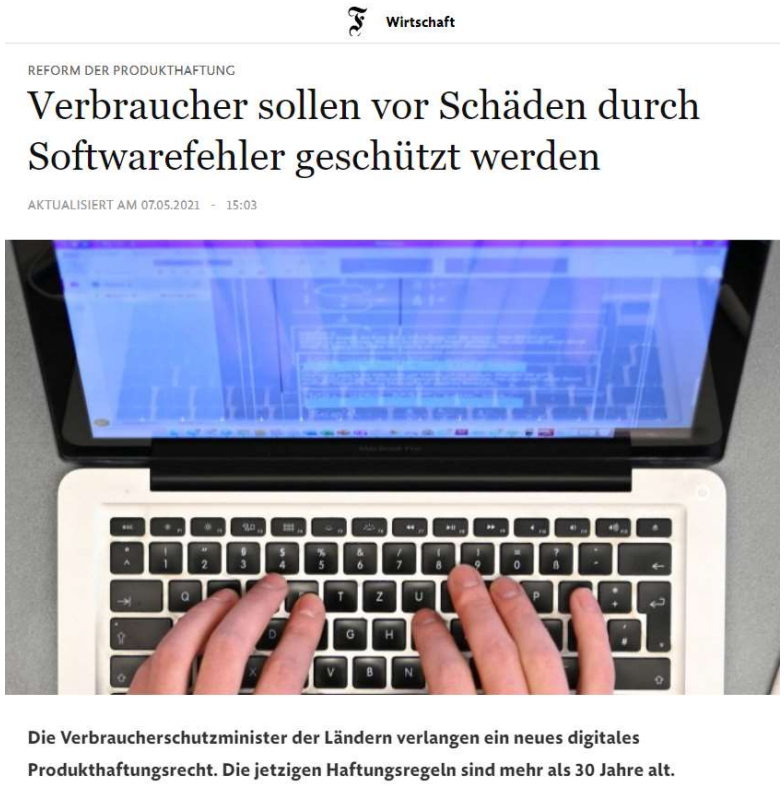
# Übersicht

- 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, nationales Umsetzungsgesetz bis 7/2021, Inkrafttreten zu 1/2022

# Rechtspolitischer Ausblick: Mehr rechtliche Verantwortlichkeit für Softwarefehler



Wirtschaft

REFORM DER PRODUKTHAFTUNG

## Verbraucher sollen vor Schäden durch Softwarefehler geschützt werden

AKTUALISIERT AM 07.05.2021 - 15:03

**Die Verbraucherschutzminister der Ländern verlangen ein neues digitales Produkthaftungsrecht. Die jetzigen Haftungsregeln sind mehr als 30 Jahre alt.**

# Vielen Dank für Ihre Aufmerksamkeit!

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


**Ihr Ansprechpartner:**

Dr. Dennis-Kenji Kipker
Legal Advisor
CERT@VDE

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