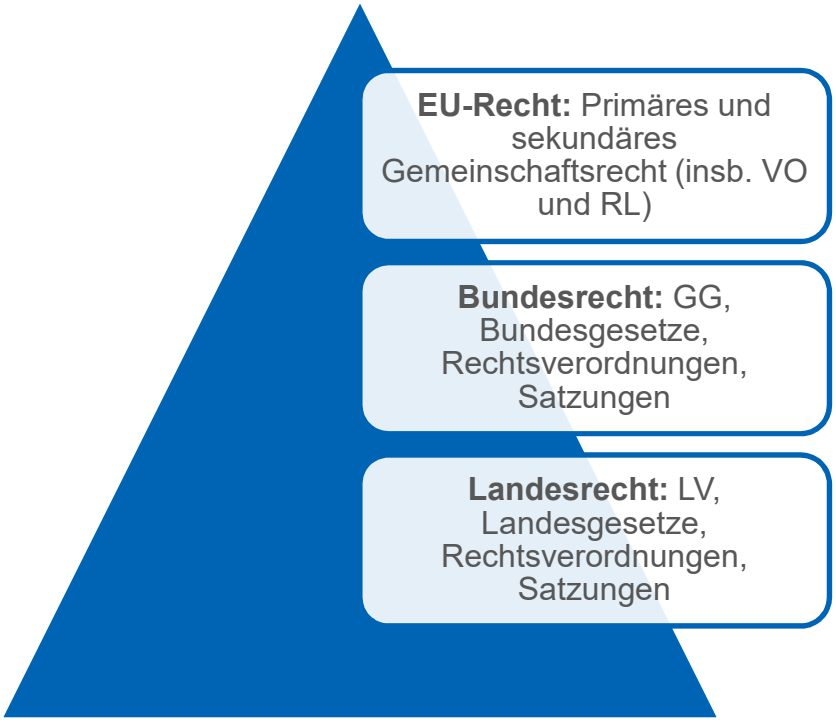
Das IT-SiG 2.0
Neue Rahmenbedingungen für die Cybersicherheit in Deutschland

Dr. Dennis-Kenji Kipker
Legal Advisor
CERT@VDE

DKE
VDE DIN

Aktueller europäischer und deutscher Cybersecurity-Rechtsrahmen

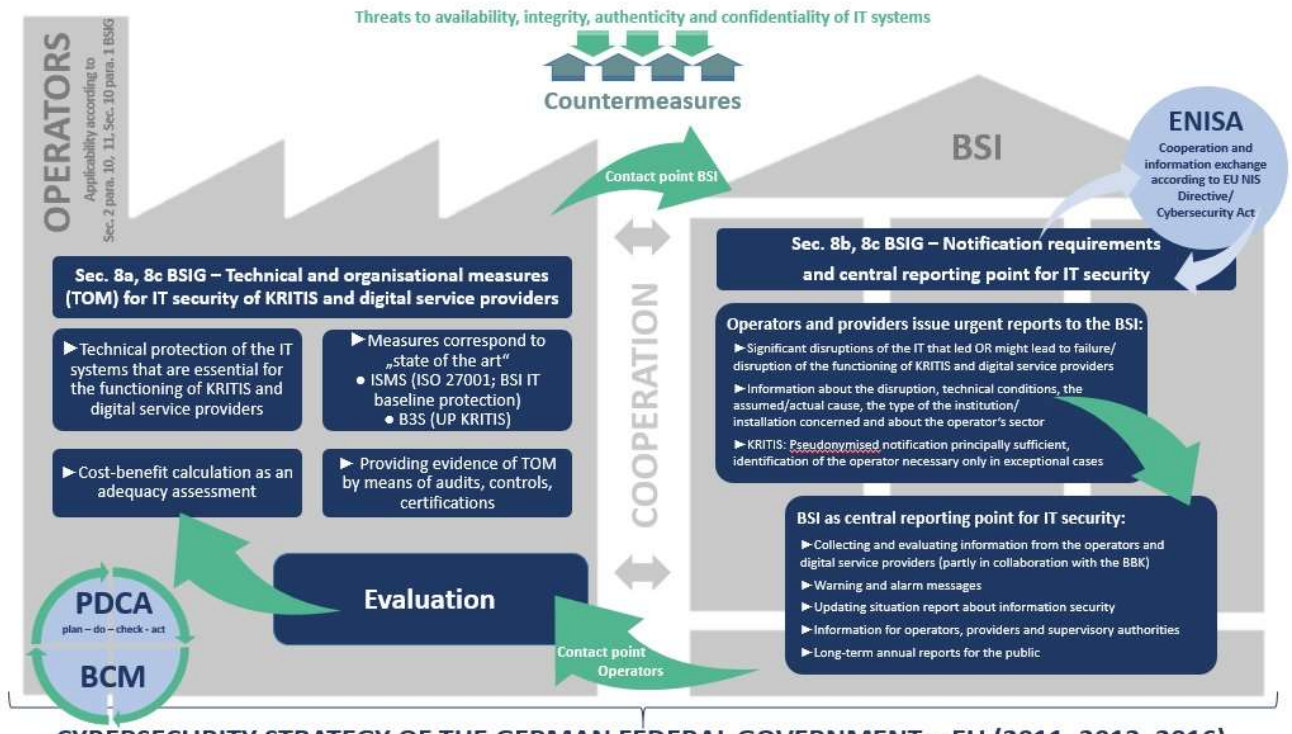


- **EU NIS-RL** (2016)
- **EU DS-GVO** (2016, 2018, auch Vorgaben zur Datensicherheit u.a. gem. Art. 32, soweit personenbezogene Daten betroffen)
- **EU Cybersecurity-Verordnung** (2019)
  - Dauerhaftes Mandat für ENISA, neuer EU-Zertifizierungsrahmen für Cybersicherheit
- **EU DID- und WK-Richtlinie** (2019, mehr Sicherheit und Verbraucherschutz bei Warenkauf und digitalen Inhalten)
- **EU Verordnung für ein Kompetenzzentrum zur Cybersicherheit** (2018, Entwurf)

- **IT-SiG** (2015)
  - BSI-KritisV (2016, 2017)
- **IT-SiG 2.0** (2019, Entwurf)
- **2. DSAnpUG-EU** (2019 umfassende datenschutzrechtliche Änderungen im BSIG)

IT-Sicherheitsgesetz 2.0

INFORMATION FLOWS AND PROTECTION PROCESSES IN THE IT SECURITY OF CRITICAL INFRASTRUCTURES AND DIGITAL SERVICE PROVIDERS



CYBERSECURITY STRATEGY OF THE GERMAN FEDERAL GOVERNMENT + EU (2011, 2013, 2016)

Dr. Dennis-Kenji Kipker, Bremen

IT-Sicherheitsgesetz 2.0 (IT-SiG 2.0)
Hintergründe und Änderungen

- **Lange erwartet, viel spekuliert:** „Veröffentlichung“ des RefE Anfang April 2019
- Federführung **BMI**
- Eigentlich: „Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme“
- Inhaltlich angepasst an die **Cyber-Sicherheitsstrategie** der BReG aus 2016:
  - **Handlungsfeld 1** – Sicheres und selbstbestimmtes Handeln in einer digitalisierten Welt
  - **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
- Damit nicht nur Schutz von Kritischen Infrastrukturen und der Wirtschaft, sondern insbesondere auch mehr **Schutz von Bürgern + Behörden**
- Adressiert z.B. mittelbar auch Fragen & Themen rund um **IoT**, dazu noch im Folgenden…

IT-Sicherheitsgesetz 2.0 (IT-SiG 2.0)
Hintergründe und Änderungen

- Artikelgesetz ändert u.a. folgende **Einzelgesetze**:
  - Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (**BSIG**)
  - Telekommunikationsgesetz (**TKG**): U.a. Informationspflichten, Pflichten zur Blockade/Umleitung schadhaften Datenverkehrs, Schließen von Sicherheitslücken in Nutzer-IT, z.B. zur Bekämpfung von Botnetzen
  - Telemediengesetz (**TMG**): Ähnliche Pflichten zur Unterrichtung/Sperrung/Datenlöschung, siehe zuvor für TKG
  - Strafgesetzbuch (**StGB**): Anhebung Strafmaß IT-Straftaten; Strafbarkeit unbefugter IT-Nutzung
  - Strafprozessordnung (**StPO**): Verbesserung digitaler Ermittlungsmöglichkeiten
  - Bundeskriminalamtsgesetz (**BKAG**)

IT-Sicherheitsgesetz 2.0 (IT-SiG 2.0)
Neue Aufgaben und Befugnisse für das BSI

Schutz der Regierungsnetze:

- Schon bisher: **BSI als zentrale Meldestelle** für Sicherheit der Informationstechnik des Bundes, § 4a BSIG
- Neu: Befugnis, **aktive Sicherheitskontrollen** der Kommunikationstechnik des Bundes durchzuführen (§ 4a BSIG-E)
- Umfasst auch die Einsichtnahme in Unterlagen/Datenträger von die Kommunikationstechnik betreibenden **Drittunternehmen**

IT-Sicherheitsgesetz 2.0 (IT-SiG 2.0)
Neue Aufgaben und Befugnisse für das BSI

Einsichtnahme in Protokoll- und Schnittstellendaten:

- Neu: Befugnis, **Protokoll- und Schnittstellendaten** bei IT-Diensteanbietern zu erheben, soweit diese Leistungen in sicherheitssensiblen Bereichen erbringen, auch **Betretensrechte** sowie **unverschlüsselter Zugriff** auf Schnittstellen- und Protokolldaten verschlüsselter Kommunikation umfasst
- **Verlängerung der Speicherung** von Protokolldaten von drei auf 18 Monate
- Erweiterte Verarbeitungsbefugnisse von (behördeninternen) **Protokolldaten**, § 5a BSIG-E
- Aufgrund der Datenschutzrelevanz umfassende Rechtfertigungs- und Begründungstatbestände
- Mindeststandards für Informationssicherheit gem. § 8 Abs. 1 BSIG: **Ausdehnung auf IT-Dienstleister** in der Kommunikationstechnik des Bundes

IT-Sicherheitsgesetz 2.0 (IT-SiG 2.0)
Neue Aufgaben und Befugnisse für das BSI

BSI als (allgemeine) zentrale Stelle für Informationssicherheit:

- BSI zukünftig wohl nicht nur relevant für Bund und KRITIS, sondern **allgemein zentrale (Melde)stelle** für Informationssicherheit in Deutschland
- § 4b BSIG-E ermöglicht die Entgegennahme von **Informationen aus allgemeinen Quellen**, auch anonym, und die Weiterverteilung/Information an die Öffentlichkeit, z.B. gem. § 7 BSIG
- **Bestandsdatenauskunft** von TK-Anbietern inkl. **IP-Adressen** wird gem. § 5d Abs. 1 BSIG-E ermöglicht, um Betroffene zu identifizieren/Kontakt aufzunehmen

IT-Sicherheitsgesetz 2.0 (IT-SiG 2.0)
Neue Aufgaben und Befugnisse für das BSI

BSI als (allgemeine) zentrale Stelle für Informationssicherheit:

- Ausdehnung der bisherigen Warn- und Informationsmöglichkeiten nach § 7 BSIG: Nicht nur Warnungen vor Sicherheitslücken/Schadprogrammen, sondern auch Informationen über IT-sicherheitsrelevante Eigenschaften von Produkten (**IoT, Router, SmartTV**)
- § 7a Abs. 2 BSIG-E: BSI darf zur Untersuchung der IT-Sicherheit auch **technische Auskünfte vom Hersteller** verlangen
- § 7b BSIG-E: Aktive Detektion von Sicherheitsrisiken für die Netz- und IT-Sicherheit und von Angriffsmethoden („macht das BSI zur **Hackerbehörde**“)

IT-Sicherheitsgesetz 2.0 (IT-SiG 2.0)
Erweiterte Pflichten für die Betreiber Kritischer Infrastrukturen

Registrierung Kritischer Infrastrukturen:

- § 8b Abs. 3 BSIG-E: Detaillierte **Registrierungspflicht von KRITIS** beim BSI
- § 8b Abs. 3a BSIG-E: BSI kann selbst Einrichtung als KRITIS registrieren (**Ersatzvornahme**)

Technisch-organisatorische Maßnahmen (TOM):

- Schon bisher **Pflicht der KRITIS-Betreiber**, angemessene TOM vorzusehen (vgl. § 8a BSIG)
- Auch hier Erweiterung: Ausdrückliche Aufnahme von „**Systemen zur Angriffserkennung**“
  - Quartalsweiser Bericht an betrieblichen DSB, BSI, Aufsichtsbehörde und BfDI
- § 5c BSIG-E: Befugnis des BSI zur **Aufstellung von Krisenreaktionsplänen** für KRITIS oder Anlagen im besonderen öffentlichen Interesse in Kooperation mit den Betreibern

IT-Sicherheitsgesetz 2.0 (IT-SiG 2.0)
Erweiterte Pflichten für die Betreiber Kritischer Infrastrukturen

Nachweisbarkeit von Lieferketten:

- **KRITIS-Kernkomponenten** dürfen nur von Herstellern verwendet werden, die Vertrauenswürdigkeitserklärung abgegeben haben
- KRITIS-Kernkomponente gem. § 2 Abs. 13 BSIG-E: **Kriterium Steuerungsfunktion**
- Erstreckt sich auf **gesamte Lieferkette** des Herstellers
- Mindestanforderungen sollen durch **Allgemeinverfügung des BMI** bestimmt werden

IT-Sicherheitsgesetz 2.0 (IT-SiG 2.0)
Ausdehnung des Adressatenkreises der Regelungen im BSIG

- Neuer KRITIS-Sektor: **Entsorgung** (von Siedlungsabfällen: Seuchengefahr)

- **Infrastrukturen im besonderen öffentlichen Interesse** (§ 2 Abs. 14 BSIG-E):
  - Rüstungsindustrie; Kultur und Medien; bestimmte börsennotierte Unternehmen
  - **Beispiele:** Chemiesektor, Automobilherstellung
  - Pflichten für KRITIS aus den **§§ 8a, 8b BSIG** gelten (TOM + Meldepflicht)
  - Infrastrukturen im besonderen öffentlichen Interesse durch **RVO des BMI** zu bestimmen

IT-Sicherheitsgesetz 2.0 (IT-SiG 2.0)
Ausdehnung des Adressatenkreises der Regelungen im BSIG

Cyberkritikalität (§ 8g BSIG-E):

- **Auffangtatbestand:** Soll Flexibilität bei Änderung der Bedrohungslage/technischen Entwicklung ermöglichen; **Ausfälle mit wie für KRITIS vergleichbaren Folgen**
- Betrifft vor allem bisher unter den KRITIS-Schwellenwerten angesiedelte **KMU**
- Pflichten gem. **§§ 8a, 8b BSIG** gelten (TOM + Meldepflicht)
- **Individuelle Identifizierung** von Betreibern durch BSI

IT-Sicherheitsgesetz 2.0 (IT-SiG 2.0)
Erweiterung produktbezogener Herstellerpflichten

- Hersteller steht Produkt „am nächsten“, sodass ihn auch **IT-sicherheitsbezogene Verantwortlichkeit** trifft
- § 8h BSIG-E: **Unverzügliche Meldepflicht** bei produkt- bzw. softwarebezogenen IT-Sicherheitsgefahren, soweit KRITIS oder Anlagen von besonderem öffentlichen Interesse betroffen
- IT-Produkte in § 9a BSIG-E legaldefiniert, weit gefasst: **Hard- + Software**, embedded systems
- **Inhalt der Meldepflicht:**
  - Angaben zur Störung
  - Grenzüberschreitende Auswirkungen
  - Technische Rahmenbedingungen
  - Vermutete oder tatsächliche Ursache
  - Auswirkungen der Störung

IT-Sicherheitsgesetz 2.0 (IT-SiG 2.0)
Mehr Verbraucherschutz und Transparenz

- **Parallel zu EU Cybersecurity Act**, vgl. Art. 55 EU CSA: Ergänzende Informationen über die Cybersicherheit zertifizierter IKT-Produkte, Prozesse und Dienste
- § 9a BSIG-E: Etablierung eines **freiwilligen IT-Sicherheitskennzeichens**
- **Zweck:** Umsetzung des behördlichen Auftrags zur Warnung vor IT-Sicherheitslücken, Beratung verschiedener Stellen
- Konkretisierung ebenfalls durch ausgestaltende **RVO des BMI**
- **Inhalte:**
  - „Herstellererklärung“ enthält IT-Sicherheitseigenschaften
  - „BSI-Sicherheitsinformation“ informiert über Sicherheitslücken
- **Darstellung:** Körperlich auf Produkt/Umverpackung, „elektronischer Verweis“, wohl **QR-Code**
- **BSI prüft** regelmäßig auf Einhaltung der Anforderungen des IT-Sicherheitskennzeichens

DKE
VDE DIN

Erwartete Auswirkungen auf die Forschung

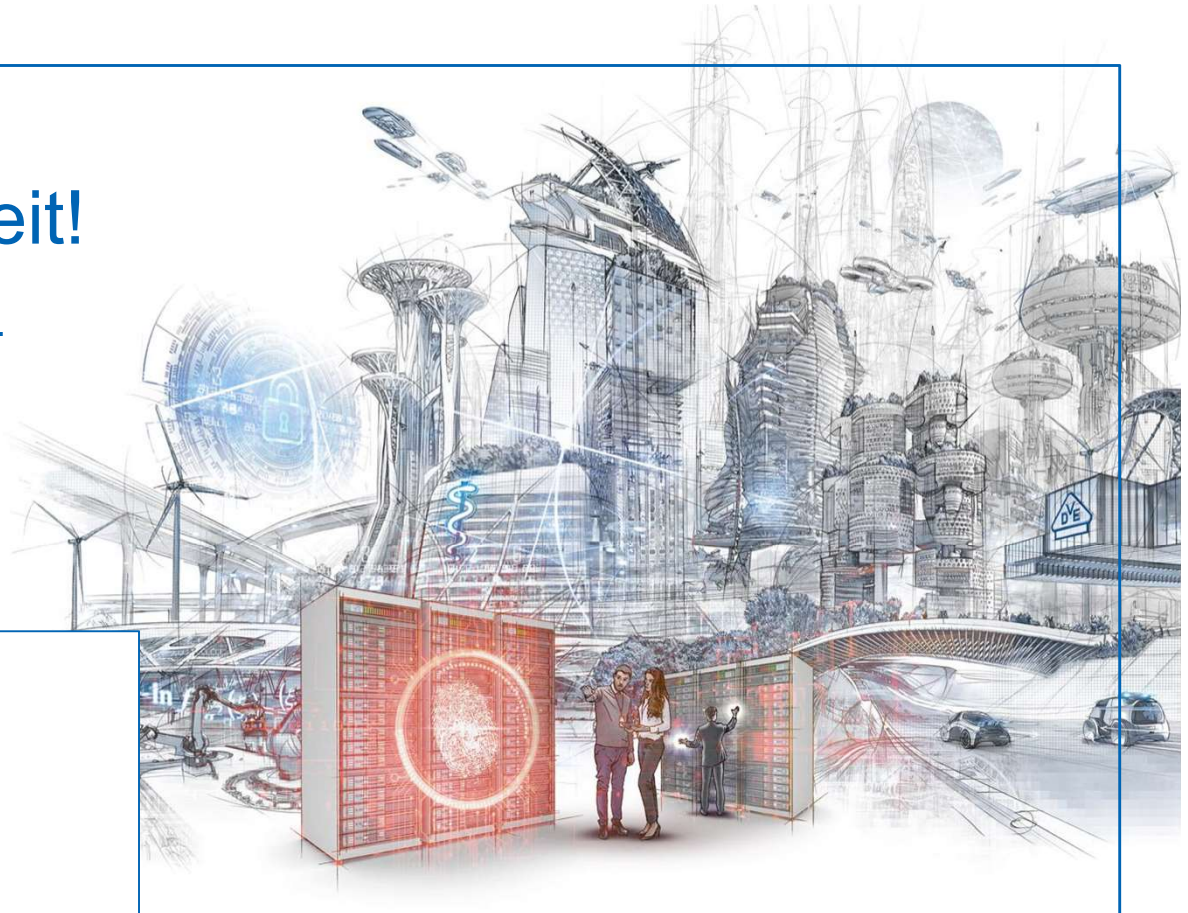
- Hochschulen und Universitäten als solche nach wie vor **keine Kritischen Infrastrukturen**
- Grds. **Entwicklungen im TK- und TM-Recht** beachten
- Entwurf zum IT-SiG 2.0 bringt mehr Mitwirkungsmöglichkeiten auch für Forschungseinrichtungen, z.B. zur **Meldung/Weiterverbreitung von Schwachstellen** an das BSI und damit verbundener Kooperation
- **Forschung zu wichtigen IT-sicherheitsbezogenen Fragestellungen** nach wie vor nicht abgeschlossen und wird durch neue Gesetze befördert, z.B.:
  - „Stand der Technik“
  - Technisch-organisatorische Realisierung des gesetzlich geforderten „Lieferkettennachweises“
- Zunehmende Regulierung der IT-Sicherheit macht es für Forschungseinrichtungen mehr und mehr notwendig, bei **Fördermittelanträgen auch juristische Expertise einzubeziehen**, um compliancekonforme Lösungen zu entwickeln
- Hochschulen und Universitäten deshalb nach wie vor eher als **„Dienstleister“** im Sinne der Weiterentwicklung bisheriger IT-Sicherheitslösungen durch Forschung zu sehen, hier dürften mit dem IT-SiG 2.0 **verstärkte Einbringungs- und Kooperationsmöglichkeiten** zu erwarten sein, die über IT-SiG hinausgehen

Erwartete Auswirkungen auf Wirtschaft und Verbraucher

- EU Cybersecurity-Act: Unternehmen und Verbände können/sollten sich **schon jetzt einbringen**
- Tendenz zur **umfassenden IT-Sicherheitsregulierung** deutlich erkennbar, v.a. auch **IoT**
- **Weitere Gesetzesänderungen** zur IT-Sicherheit erwartbar
- **Verordnungen des BMI** bringen wohl mehr Klarheit über Adressaten, Umfang etc.
- Nicht nur Datenschutz, sondern auch verbraucherbezogene IT-Sicherheit mehr und mehr **Verkaufsargument („Security by Design“)**
- **Erhebliche Sanktionshöhe** passt IT-Sicherheits- an Datenschutzrecht an: max. 20.000.000€ oder 4% des globalen Jahresumsatzes
- V.a. auch **ausländische Unternehmen** werden in Zukunft stärker auf IT-Sicherheitsregulierung in der EU/in Deutschland achten

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

DKE
VDE DIN