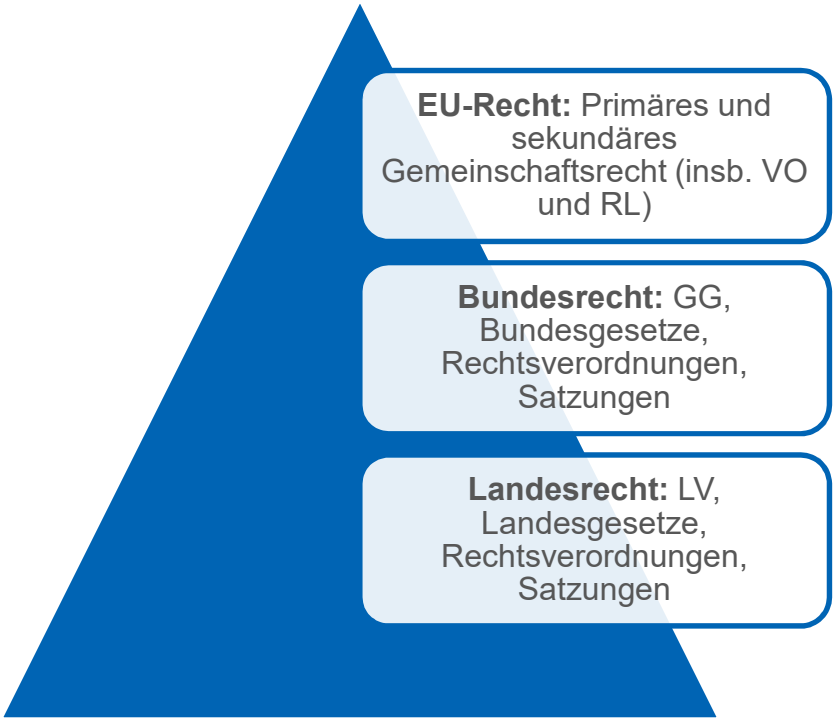
Cybersecurity
Stand der Gesetzgebung

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, Entwurf)
  - Umfassende gesetzliche Berücksichtigung der Normung- und Standardisierung bei Konzeptionierung der Zertifizierungsmaßstäbe
- **EU Verordnung für ein Kompetenzzentrum zur Cybersicherheit** (2018, Entwurf)

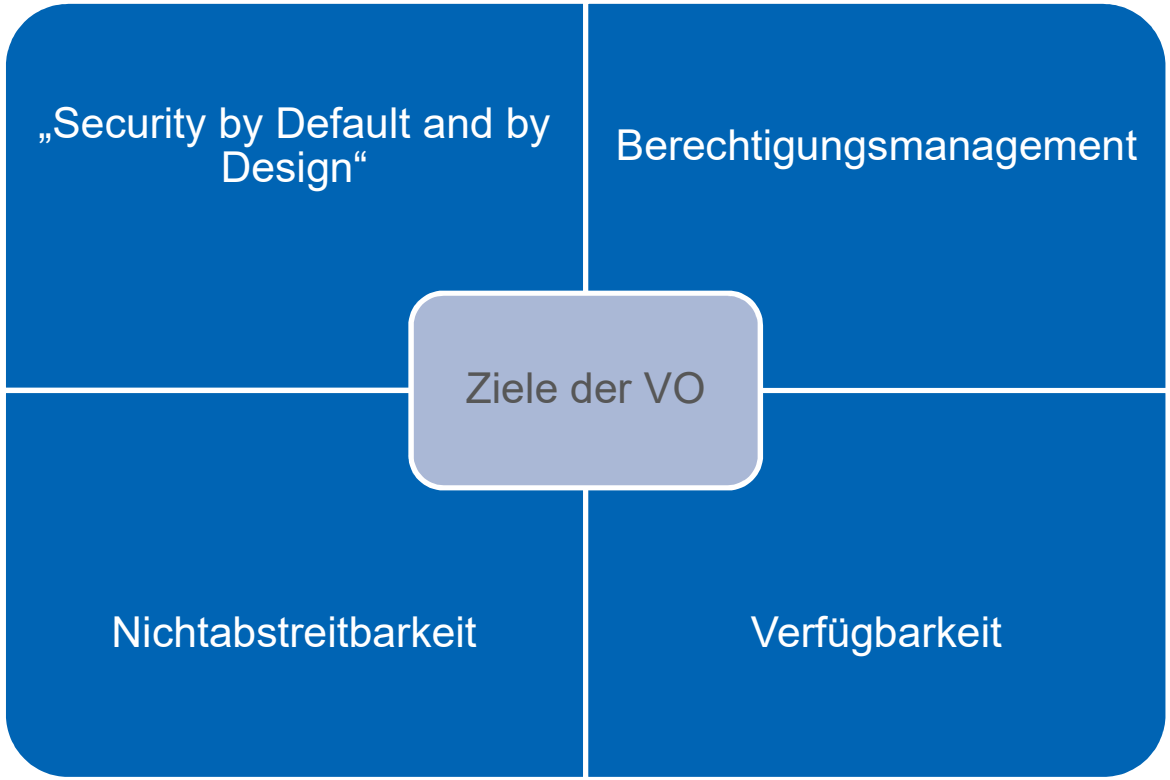
- **IT-SiG** (2015)
  - BSI-KritisV (2016, 2017)
- **„IT-SiG 2.0“** (2019, Entwurf)
- **2. DSAnpUG-EU** (2018, Entwurf, umfassende datenschutzrechtliche Änderungen im BSIG)

EU Cybersecurity Act

EU Cybersecurity-Verordnung („Cybersecurity Act“)

- **Kerninhalt:** Einführung eines dualen europäischen Systems zur (grds. freiwilligen) Zertifizierung der Cybersicherheit (neben Umstrukturierung der ENISA)
- **Zwecksetzung:** Schutz des digitalen EU-Binnenmarkts, Erleichterung des ausländischen Marktzugangs durch Anerkennung in allen Mitgliedstaaten
- **Zentrale Aussagen:**
  - *„Europäisches Schema für die Cybersicherheitszertifizierung bezeichnet ein umfassendes Paket von Vorschriften, technischen Anforderungen, Normen und Verfahren, die auf Unionsebene festgelegt werden und für die Zertifizierung oder Konformitätsbewertung von bestimmten IKT-Produkten, Diensten und Prozessen gelten.“*
  - *„Europäisches Cybersicherheitszertifikat bezeichnet ein Dokument, in dem bescheinigt wird, dass ein bestimmter IKT-Prozess, ein bestimmtes IKT-Produkt oder ein bestimmter IKT-Dienst im Hinblick auf die Erfüllung besonderer Sicherheitsanforderungen, die in einem europäischen System für die Cybersicherheitszertifizierung festgelegt sind, bewertet wurde.“*

EU Cybersecurity-Verordnung („Cybersecurity Act“)



EU Cybersecurity-Verordnung („Cybersecurity Act“)
Ausarbeitung des Zertifizierungsrahmens

Rolle der Normung bei der Ausarbeitung und Implementierung der Cybersicherheitszertifizierung:

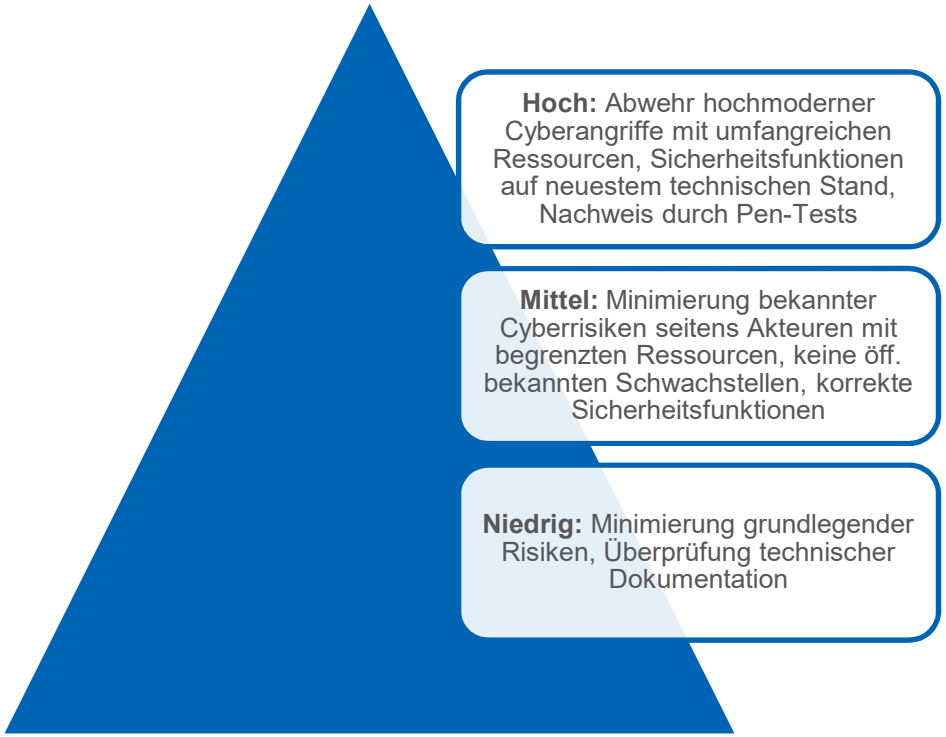
- EU-Kommission oder noch einzurichtende Gruppe für die Cybersicherheitszertifizierung (ECCG) beauftragen ENISA mit der Ausarbeitung der verschiedenen europäischen Cybersicherheitszertifizierungssysteme
  - **ECCG** bestehend aus Vertretern der nationalen Cybersicherheits-Zertifizierungsbehörden, Beteiligung relevanter externer Stakeholder möglich
  - **Umfassender Konsultationsprozess** von Interessenträgern während der Ausarbeitung
  - **Gruppe der Interessenträger für die Cybersicherheitszertifizierung:** U.a. strategische Beratung, Normungsbezüge
- Zur Unterstützung des Erstellungsprozesses kann die ENISA **Arbeitsgruppen** einrichten, zudem wird sie von der **ECCG** beratend unterstützt
- **Mindestinhalt eines EU-Cybersicherheitszertifizierungssystems** umfasst u.a. auch die für die Bewertung maßgeblichen internationalen, europäischen oder nationalen Normen
- **Darüber hinaus:** Einbeziehung der Normungsinteressen durch die **ENISA-Beratungsgruppe**

EU Cybersecurity-Verordnung („Cybersecurity Act“)
Anforderungsniveaus

Anforderungsniveau in Abhängigkeit vom jeweiligen Verwendungsrisiko

„Rolling work programme“ der EU-COM definiert Liste relevanter IKT-Produkte/Dienste bis 1 Jahr nach Inkrafttreten der VO

Produkt- oder dienstbegleitende Informationspflichten des Herstellers/Anbieters



Hoch: Abwehr hochmoderner Cyberangriffe mit umfangreichen Ressourcen, Sicherheitsfunktionen auf neuestem technischen Stand, Nachweis durch Pen-Tests

Mittel: Minimierung bekannter Cyberrisiken seitens Akteuren mit begrenzten Ressourcen, keine öff. bekannten Schwachstellen, korrekte Sicherheitsfunktionen

Niedrig: Minimierung grundlegender Risiken, Überprüfung technischer Dokumentation

DKE
VDE DIN

EU Cybersecurity-Verordnung („Cybersecurity Act“)
Durchführung der Zertifizierung

- **Duales Prüfsystem:** Unterscheidung zwischen Selbstbewertung der Konformität durch den Hersteller oder Anbieter und der Drittzertifizierung
- **Inhalt der Selbstbewertung:** Ausstellung einer EU-Konformitätserklärung, die bestätigt, dass die Erfüllung der im jeweiligen System festgelegten Anforderungen nachgewiesen wurde → Hersteller übernimmt insoweit Eigenverantwortung
  - Ausschließlich für die **Vertrauenswürdigkeitsstufe „niedrig“** möglich
  - Ausstellung der EU-Konformitätserklärung ist **grds. freiwillig**
- **Inhalt der Cybersicherheitszertifizierung („Drittbewertung“):**
  - Ausstellung eines **EU-Cybersicherheitszertifikats** durch eine Konformitätsbewertungsstelle oder durch eine akkreditierte öffentliche Stelle/nationale Cybersicherheitszertifizierungsbehörde
  - **Umfasst alle Vertrauenswürdigkeitsstufen:**
    - „Niedrig“ und „mittel“: Zuständigkeit grds. bei den (privaten) Konformitätsbewertungsstellen
    - „Hoch“: Zuständigkeit grds. bei der nationalen Cybersicherheitszertifizierungsbehörde
  - Ein erteiltes Zertifikat ist für die im jeweiligen Zertifizierungssystem **festgelegte Dauer gültig** und kann bei Vorliegen der Voraussetzungen **verlängert werden**

EU Cybersecurity-Verordnung („Cybersecurity Act“)
Konformitätsbewertungsstellen und Akkreditierung

- **Akkreditierung** der Konformitätsbewertungsstellen durch nationale Akkreditierungsstelle gem. VO (EG) 765/2008 (**DAkkS**) ist notwendig
- **Anlage der VO:** Umfassende Anforderungen an (private) Konformitätsbewertungsstellen insb. zu Unabhängigkeit, Fachkunde, Transparenz
- Akkreditierung wird für Höchstdauer von **fünf Jahren** erteilt
  - Bei weiterer Erfüllung der Anforderungen ist eine **Verlängerung möglich**
- Für jedes angenommene EU-System zur Cybersicherheitszertifizierung erfolgt eine **Notifizierung** der entsprechenden Konformitätsbewertungsstellen durch die nationalen Cybersicherheitszertifizierungsbehörden ggü. der EU-Kommission
- Die EU-Kommission veröffentlicht im EU-Amtsblatt die **Liste der notifizierten Konformitätsbewertungsstellen**
- **Peer-Review** der nationalen Cybersicherheitszertifizierungsbehörde mindestens alle 5 Jahre

IT-Sicherheitsgesetz 2.0

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 „neue“ **Cyber-Sicherheitsstrategie** der BReG aus 2016
- Damit nicht nur Wirtschaftsschutz, sondern insb. auch **Schutz von Bürgern + Behörden**
- Artikelgesetz ändert u.a. folgende **Einzelgesetze**:
  - Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (**BSIG**)
  - Telekommunikationsgesetz (**TKG**): U.a. Informationspflichten, Blockade schadhafter Datenverkehr
  - Telemediengesetz (**TMG**): Ähnliche Pflichten, 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**
  - Neu auch: Befugnis, **Protokoll- und Schnittstellendaten** bei IT-Diensteanbietern zu erheben, soweit diese Leistungen in sicherheitssensiblen Bereichen erbringen (§ 5 Abs. 11 BSIG-E), 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
  - § 5c BSIG-E: Befugnis des BSI zur **Aufstellung von Krisenreaktionsplänen** für KRITIS oder Anlagen im besonderen öffentlichen Interesse in Kooperation mit den Betreibern
  - **Bestandsdatenauskunft** von TK-Anbietern inkl. **IP-Adressen** wird gem. § 5d Abs. 1 BSIG-E ermöglicht, um Betroffene zu identifizieren/Kontakt aufzunehmen
  - 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: 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

- Schon bisher Pflicht der KRITIS-Betreiber, angemessene TOM vorzusehen
- Auch hier Erweiterung: Ausdrückliche Aufnahme von „**Systemen zur Angriffserkennung**“
  - Quartalsweiser Bericht an betrieblichen DSB, BSI, Aufsichtsbehörde und BfDI
- **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
- § 8b Abs. 3 BSIG-E: Detaillierte **Registrierungspflicht von KRITIS** beim BSI
- § 8b Abs. 3a BSIG-E: BSI kann selbst Einrichtung als KRITIS registrieren (**Ersatzvornahme**)

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
  - Infrastrukturen im besonderen öffentlichen Interesse durch RVO des BMI zu bestimmen
- **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
  - Individuelle Identifizierung von Betreibern durch BSI

IT-Sicherheitsgesetz 2.0 (IT-SiG 2.0)
Erweiterung von produktbezogenen 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

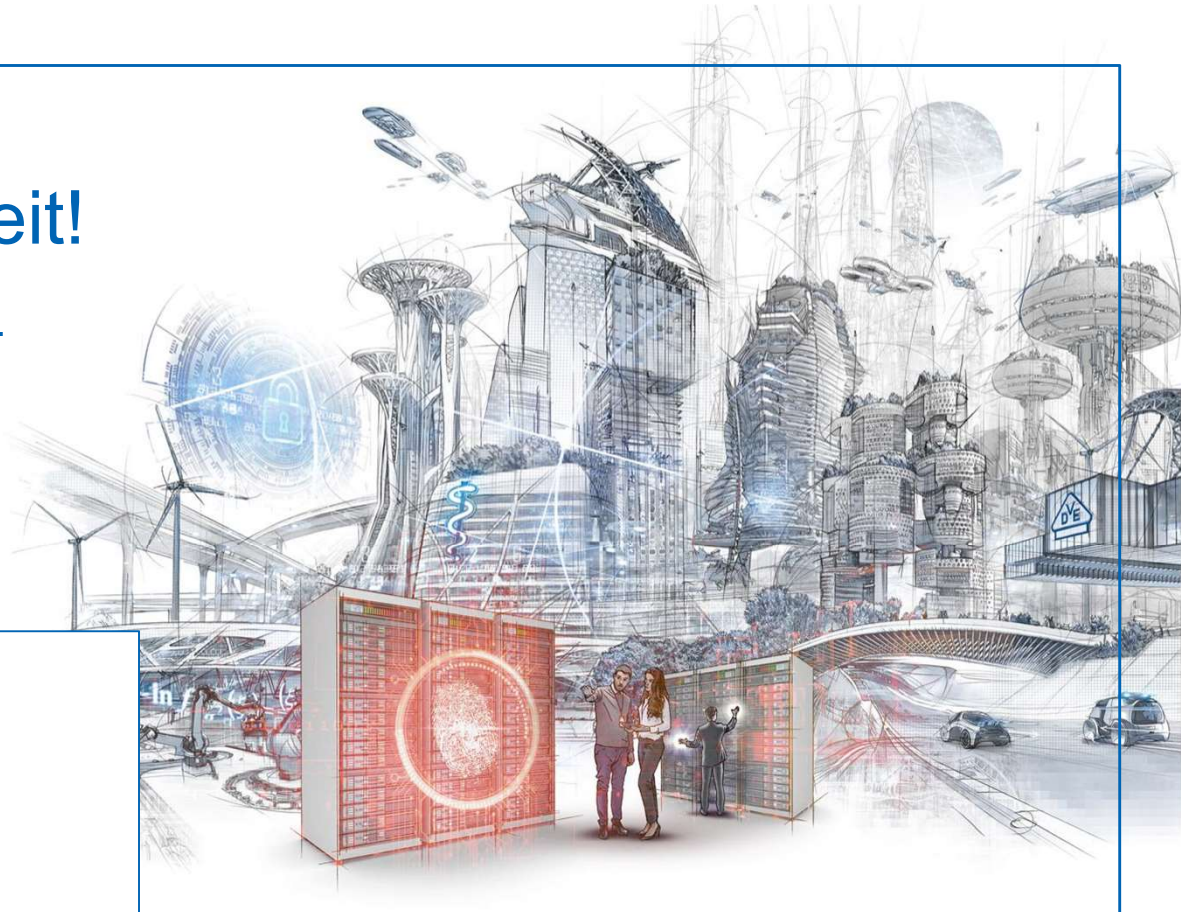
- **Parallel zu den rechtlichen Entwicklungen des EU Cybersecurity Act**, vgl. Art. 55 des Entwurfs: Ergänzende Informationen über die Cybersicherheit zertifizierter IKT-Produkte)
- § 9a BSIG-E: Etablierung eines **freiwilligen IT-Sicherheitskennzeichens**
- **Zweck:** Umsetzung des behördlichen Auftrags 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

Erwartete Auswirkungen auf Unternehmen 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**
- **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