

TeleTrust "IT-Sicherheitsrechtstag 2022"

Berlin, 21.09.2022

ITSiG-Tango

Wie sich das Verhältnis von KRITIS-Betreibern, Zulieferern, Herstellern und Aufsicht nach dem IT-Sicherheitsgesetz 2.0 ändert

RA Karsten U. Bartels LL.M.

HK2 Rechtsanwälte, Vorstand TeleTrust, Leiter AG Recht

Karsten U. Bartels LL.M.*



- Rechtsanwalt/ Partner bei HK2
- Geschäftsführer HK2 Comtection GmbH
- Stellv. Vorstandsvorsitzender Bundesverband IT-Sicherheit e. V. (TeleTrusT)
- Vorsitzender Arbeitsgemeinschaft IT-Recht im Deutschen Anwaltverein e.V.
- Lehrbeauftragter Hochschule Hof für Datenschutz-Compliance
- Zert. Datenschutzbeauftragter (TÜV)

*Rechtsinformatik



- IT-Recht/ Datenschutzrecht
- IT-Sicherheitsrecht
- IP-Recht
- Gesellschaftsrecht
- Wirtschaftsrecht

*HK2 wurde zu den besten
Wirtschaftskanzleien 2022
gewählt.*

brand eins/ thema, Heft 23/ 2022



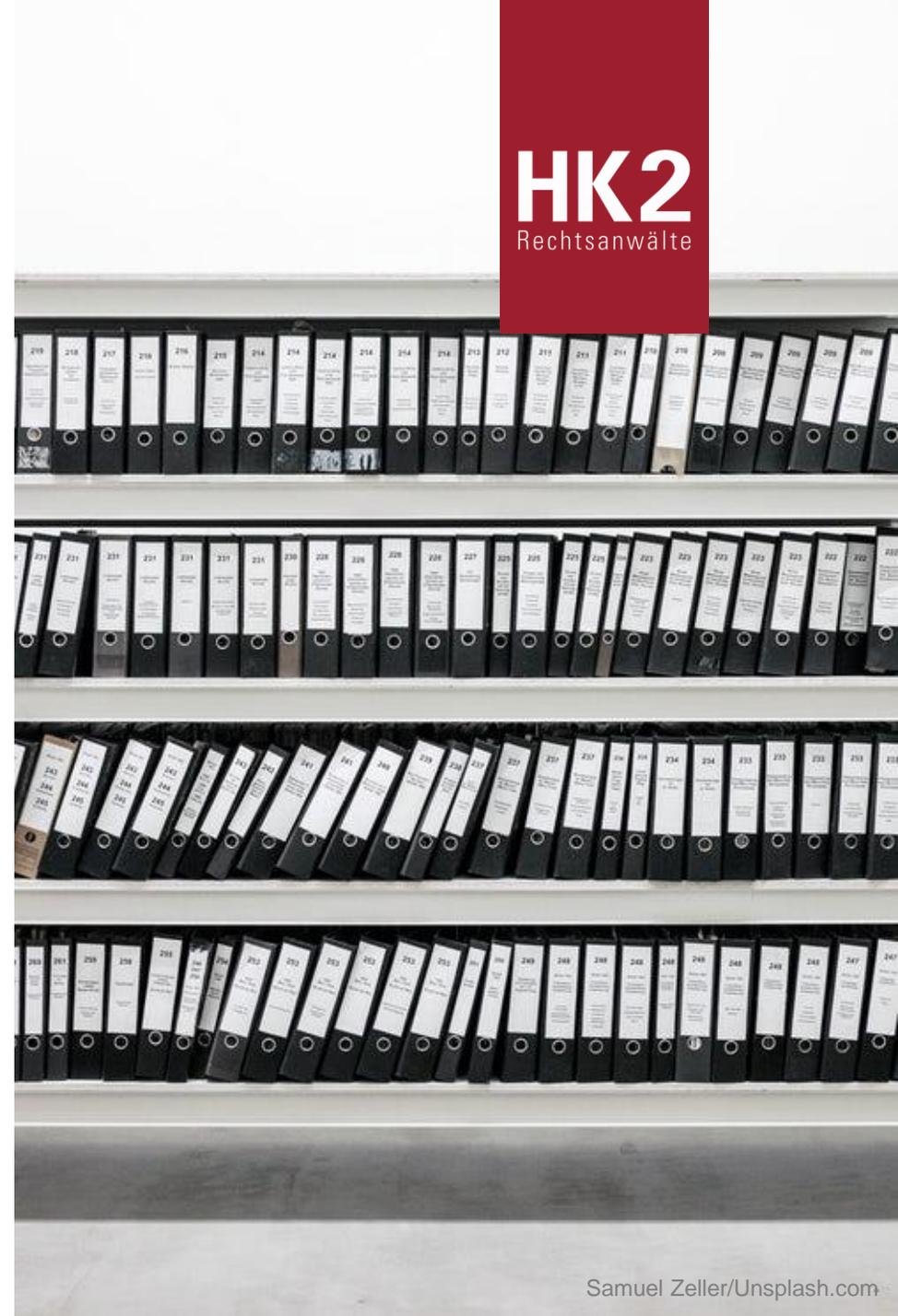
*HK2 TOP-Wirtschaftskanzlei
2022 für IT & TK und
Datenschutzrecht*

FOCUS 06/2022



HK2
Rechtsanwälte

Vereinbarungen zur IT-Sicherheit vor dem IT-Sicherheitsgesetz 2.0



Vereinbarungen zur IT-Sicherheit nach dem IT-Sicherheitsgesetz 2.0

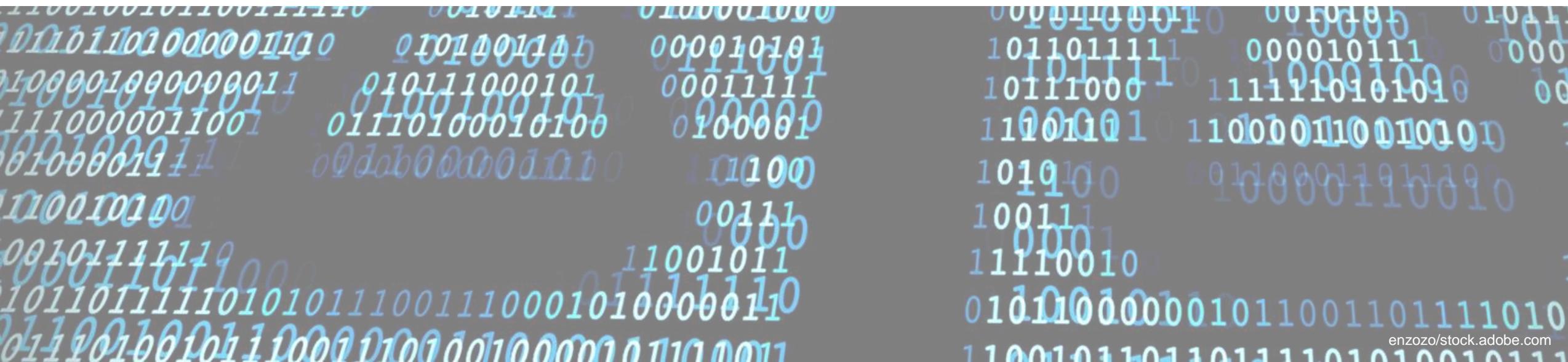


Am Anfang steht die Defintion

- Störungen und Beeinträchtigungen nach § 2 Abs. 13 BSIG: klar?
- Schwachstellen, Manipulationen (§ 9b Abs. 5) und Bedrohungen (§ 8a Abs. 1a S. 3): unklar!



Umgang mit Untersuchungen des BSI



Hersteller informationstechnischer Produkte und Systeme

§ 7a BSIG

- **Untersuchungsrecht** des BSI hinsichtlich auf dem Markt bereitgestellte oder zur Bereitstellung auf dem Markt vorgesehene IT-Produkte und –Systeme. Untersuchung durch Dritte möglich.
- **Auskunftspflicht** inkl. technischer Details („soweit erforderlich ... alle notwendigen Auskünfte ...“)
- **Informationsweitergabe** des BSI an Aufsichtsbehörde des Bundes oder an Ressort, wenn Behörde nicht vorhanden.
- BSI kann Erkenntnisse **weitergeben** und **veröffentlichen**, soweit erforderlich nach § 3 Abs. 1 S. 2 Nr. 1, 14, 14a, 17, 18 BSIG. Zuvor ist dem Hersteller Gelegenheit zur Stellungnahme zu geben.
- BSI kann **Öffentlichkeit** namentlich (Hersteller, Produkt) **informieren**, wenn Auskunft unterlassen wird und Gelegenheit zur Stellungnahme gegeben wurde.

Parteien und Produkte - de lege ferenda?

- KRITIS-Betreiber

Parteien und Produkte - de lege ferenda?

- KRITIS-Betreiber
 - KRITIS-Verordnung des BMI
nach § 10 Abs. 1 BSIG

Parteien und Produkte - de lege ferenda?

- KRITIS-Betreiber
- Unternehmen im besonderen öffentlichen Interesse

Parteien und Produkte - de lege ferenda?

- KRITIS-Betreiber
- Unternehmen im besonderen öffentlichen Interesse
 - Außenwirtschaftsverordnung
 - Rechtsverordnung des BMI (§ 10 Abs. 5 BStG)
 - Störfallverordnung

Parteien und Produkte - de lege ferenda?

- KRITIS-Betreiber
- Unternehmen im besonderen öffentlichen Interesse
- Hersteller kritischer Komponenten

Parteien und Produkte - de lege ferenda?

- KRITIS-Betreiber
- Unternehmen im besonderen öffentlichen Interesse
- Hersteller kritischer Komponenten
 - § 2 Abs. 13 BSIG ...

Hersteller kritischer Komponenten

- Kritische Komponenten im Sinne von § 2 Abs. 13 BSI-G sind IT-Produkte
 - die **in Kritischen Infrastrukturen eingesetzt** werden (Nr. 1),
 - bei denen **Störungen** der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit zu einem **Ausfall** oder zu einer **erheblichen Beeinträchtigung** der Funktionsfähigkeit Kritischer Infrastrukturen oder zu **Gefährdungen** für die öffentliche Sicherheit **führen können** (Nr. 2) und
 - die **gesetzlich als „kritische Komponente“** bestimmt oder eine gesetzlich definierte **„kritischen Funktion“ realisieren** (Nr. 3).

Untersagungsbefugnisse des BMI bei kritischen Komponenten

- Untersagung des weiteren **Einsatzes** der kritischen Komponente, § 9b Abs. 4 BSIG
- Untersagung des weiteren **Einsatz** kritischer Komponenten desselben **Typs** und desselben **Herstellers** unter Einräumung einer angemessenen Frist, § 9b Abs. 6 BSIG
- Untersagung **jeden Einsatzes** kritischer Komponenten eines Herstellers, § 9b Abs. 5, 7 BSIG

Leistungsbeschreibung

- Schwachstellen-Management
 - Erkennung
 - Bewertung
 - Behebung
- Beheben von IT Security Incidents

Qualitätssicherung

- Compliance-Klausel
 - Gesetz
 - Vertrag
 - Zertifizierungen
 - Normen/ Standards/ Richtlinien
 - B3S
- Warnungen des BSI
- Stand der Technik ...



Stand der Technik

- Definition
- Feststellungen zum SdT: Ist-Beschreibung, Fiktion, Vermutung
- Im Streit: ext. Bewertung
- Dokumentation
- Rechtsfolgenverknüpfung

Zulieferer-Anforderungen

- Selbsterklärung i. S. v. § 8f BSIG unabhängig vom Status „UBI“
- Garantieerklärung i. S. v. § 9b Abs. 3 BSIG, unabhängig davon, ob „kritische Komponenten“
- Unterbeauftragungsbeschränkung
- Überprüfung Versicherungsumfang



Anpassung, Kontrolle, Exit

- Change Request Management
- Change of Control
- Überleitungsunterstützung

IT-Sicherheit, Datenschutz und Geheimnisschutz



Anforderungen an Auftragnehmer

- IT-Sicherheitsanforderungen
- Datenschutzrechtliche Maßnahmen
 - AV-Vereinbarungen und Verträge zu joint controllership anpassen
- Geheimhaltungsverpflichtungen nach Maßgabe des GeschGehG (angemessene Geheimhaltungsmaßnahmen)

Vertragsstrafen ... und andere schwierige Schritte

Haftung und höhere Gewalt justieren



HK2
Rechtsanwälte

Voraussetzungen effektiver Verhandlungen zur IT-Sicherheit

Viel Erfolg auf dem Verhandlungsparkett!

Fragen?

HK2
Rechtsanwälte

Rechtsanwalt

Karsten U. Bartels LL.M.

Hausvogteiplatz 11 A
10117 Berlin

Telefon +49 (0)30 27 89 00-0
Telefax +49 (0)30 27 89 00-10
E-Mail bartels@hk2.eu

www.hk2.eu

[linkedin.com/in/karstenbartels](https://www.linkedin.com/in/karstenbartels)

www.hk2.eu