TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

"T.I.S.P. Community Meeting 2021"

Berlin, 03.-04.11.2021

IT-Sicherheitsgesetz 2.0

Auswirkungen auf KRITIS-Betreiber und -Zulieferer

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
- Lehrbeauftragter Hochschule Hof für Datenschutz-Compliance
- Zert. Datenschutzbeauftragter (TÜV)
- Stellv. Vorstandsvorsitzender Bundesverband IT-Sicherheit e. V. (TeleTrusT)
- Vorsitzender Arbeitsgemeinschaft IT-Recht im Deutschen Anwaltverein e.V.

*Rechtsinformatik

HK2
Rechtsanwälte

- IT-Recht
- Datenschutzrecht
- IT-Sicherheitsrecht
- IP-Recht

„HK2 wurde zu den besten Wirtschaftskanzleien 2021 gewählt“

brand eins/ thema, Heft 20/ 2021

HK2 TOP Wirtschaftskanzlei 2021 für IT und TK

FOCUS 36/2021

ITSiG 2.0 und Zulieferer

1. Zulieferer als Unternehmen im besonderen öffentlichen Interesse
   - Pflichten/ -Adressaten
   - Stand der Technik
2. Zulieferer als Hersteller
3. Herstellerhaftung
4. Auswirkungen auf KRITIS-/ Non-KRITIS-Verträge
5. Fragen *to-go*

loubna-benamer-jTMz4Nc6vRI-unsplash

HK2 Rechtsanwälte

Zulieferer als ***Unternehmen im besonderen öffentlichen Interesse***


Panumas nikhomkhai/Pexel.com

UBI (Var. 1)
Rüstungsunternehmen

im Sinne von § 2 Abs. 14 Nr. 1 BSIG i.V.m. § 60 Abs. 1 Nr. 1 AWV ist, wer:

„Güter im Sinne des Teils I Abschnitt A der Ausfuhrliste entwickelt, herstellt, modifiziert oder die tatsächliche Gewalt über solche Güter innehat“

→ Teil I A: Liste für Waffen, Munition und Rüstungsmaterial

Panumas nikhomkhai/Pexel.com

UBI (Var. 2)
IT-Sicherheitsunternehmen für Verschlusssachen

HK2 Rechtsanwälte

im Sinne von § 2 Abs. 14 Nr. 1 BSIG i.V.m. § 60 Abs. 1 Nr. 3 Außenwirtschaftsverordnung (AWV) ist, wer:

*„**Produkte mit IT-Sicherheitsfunktionen** zur Verarbeitung **staatlicher Verschlusssachen** oder für die IT-Sicherheitsfunktion wesentliche Komponenten **solcher Produkte***

a) herstellt oder

b) hergestellt hat und noch über die dabei zugrunde liegende Technik verfügt

und die Produkte des Unternehmens oder im Falle für die IT-Sicherheitsfunktion wesentlicher Komponenten das Gesamtprodukt vom Bundesamt für Sicherheit in der Informationstechnik zugelassen wurden“

UBI (Var. 3 + 4)
Groß- oder USP-Unternehmen

im Sinne von § 2 Abs. 14 Nr. 2 BSIG gehörig

- zu den **größten deutschen Unternehmen**
  - Bemessung nach inländischer Wertschöpfung
  - daher erhebliche volkswirtschaftliche Bedeutung

  oder
- wegen **Alleinstellungsmerkmal von wesentlicher Bedeutung als Zulieferer** für größte Unternehmen.

→ Kennzahlen zur Bestimmung in Rechtsverordnung des BMI, § 10 Abs. 5 BSIG

HK2 Rechtsanwälte

Vanessa Schmid/Unsplash.com

Für UBI nach § 2 Abs. 14 Nr. 1, 2 BSIG gilt:

§ 8f BSIG

- Abs. 1: **Selbsterklärung zur IT-Sicherheit** beim Bundesamt vorzulegen
  - Ziff. 1 welche **Zertifizierungen** im Bereich der IT-Sicherheit in den letzten zwei Jahren durchgeführt, welche Prüfgrundlage und welcher Geltungsbereich hierfür festgelegt wurden,
  - Ziff. 2 welche sonstigen **Sicherheitsaudits** oder **Prüfungen** im Bereich der IT-Sicherheit in den letzten zwei Jahren durchgeführt, welche Prüfgrundlage und welcher Geltungsbereich hierfür festgelegt wurden oder
  - Ziff. 3 wie sichergestellt wird, dass die für das Unternehmen **besonders schützenswerten informationstechnischen Systeme, Komponenten und Prozesse angemessen geschützt werden**, und **ob dabei der Stand der Technik eingehalten** wird.
- Abs. 5: **Pflicht zur Registrierung** und Einrichtung **Kontaktstelle**
- Abs. 7: Pflicht zur **Meldung von Störungen**
- Abs. 9: bei Verdacht eines Verstoßes gegen Abs. 5: BSI ggü. Wertschöpfung darlegen und Bestätigung eines WP beibringen, dass Unternehmen nach der RV kein UBI ist.

HK2 Rechtsanwälte

Für UBI nach § 2 Abs. 14 Nr. 1, 2 BSIG gilt:

§ 8f Abs. 3 BSIG (IT-Sicherheit in UBI)

„Das Bundesamt kann auf Grundlage der Selbsterklärung nach Absatz 1 ***Hinweise*** *zu angemessenen* ***organisatorischen und technischen Vorkehrungen*** *nach Absatz 1 Nummer 3 zur Einhaltung des* ***Stands der Technik*** *geben.“*

Meldepflicht für UBI nach § 2 Abs. 14 Nr. 1, 2 BSIG

HK2 Rechtsanwälte

§ 8f Abs. 7 BSIG: unverzüglich zu melden sind:

1. **Störungen** der Verfügbarkeit, der Integrität, der Authentizität und der Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die zu einem **Ausfall** oder zu einer **erheblichen Beeinträchtigung** der Erbringung der Wertschöpfung **geführt haben**,
2. **erhebliche Störungen** der Verfügbarkeit, der Integrität, der Authentizität und der Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die **zu einem Ausfall** oder zu einer **erheblichen Beeinträchtigung** der Erbringung der Wertschöpfung **führen können**.

HK2 Rechtsanwälte

Fristen für UBI nach § 2 Abs. 14 Nr. 1, 2 BSIG

- Für **Rüstung- oder IT-Sicherheitsunternehmen für Verschlusssachen** nach AWV (§ 2 Abs. 14 Nr. 1 BSIG) gelten neue Pflichten **ab 01.05.2023**, § 8f Abs. 4 S. 1 BSIG.
- Für **Groß- oder USP-Unternehmen** (§ 2 Abs. 14 Nr. 2 BSIG) gelten neue Pflichten frühestens zwei Jahre nach Inkrafttreten der erlassenen Rechtsverordnung, § 8f Abs. 4 S. 2 BSIG.

Grahame Jenkins/Unsplash.com

HK2 Rechtsanwälte

Störfall-UBI, Var. 5 + 6

- die Betreiber eines Betriebsbereichs der oberen Klasse im Sinne der Störfall-Verordnung in der jeweils geltenden Fassung sind
  oder
- nach § 1 Absatz 2 der Störfall-Verordnung diesen gleichgestellt sind.

Betriebsbereich oberer Klasse im Sinne der Störfall-Verordnung

HK2 Rechtsanwälte

- § 2 Abs. 14 Nr. 3 BSIG verweist auf die Störfall-Verordnung
- § 2 Nr. 2 12. BImSchV (Störfall-Verordnung): Betriebsbereich der oberen Klasse ist ein Betriebsbereich, in dem **gefährliche Stoffe** in **Mengen** vorhanden sind, die die in Spalte 5 der Stoffliste in Anhang I (S. 14 ff.) genannten Mengenschwellen **erreichen** oder **überschreiten.**
- Möglichkeit der Gleichbehandlung eines Betriebsbereiches unterer Klasse gemäß § 1 Abs. 2 der 12. BImSchV. Gleichbehandlung dann auch gemäß § 2 Abs. 14 Nr. 3 BSIG.

Für UBI nach § 2 Abs. 14 Nr. 3 BSIG gilt:

§ 8f BSIG

- Abs. 6
  - freiwillige Registrierung beim BSI
  - freiwillige Benennung einer Kontaktstelle, an die das BSI auch die Informationen nach § 8b Abs. 2 Nr. 4 sendet.
- Abs. 8: **Meldepflicht an BSI** (ab 01.11.2021)
  - **Störungen** der Verfügbarkeit, der Integrität, der Authentizität und der Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die zu einem **Störfall nach der Störfall-Verordnung** in der jeweils geltenden Fassung geführt **haben**,
  - **erhebliche Störungen** der Verfügbarkeit, der Integrität, der Authentizität und der Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die **zu einem Störfall** nach der Störfall-Verordnung in der jeweils geltenden Fassung **führen können**.
  - Meldung muss Angaben zu der Störung, zu den technischen Rahmenbedingungen, insbesondere zu der vermuteten oder tatsächlichen Ursache, der betroffenen IT und der Art der betroffenen Einrichtung oder Anlage enthalten.

HK2 Rechtsanwälte

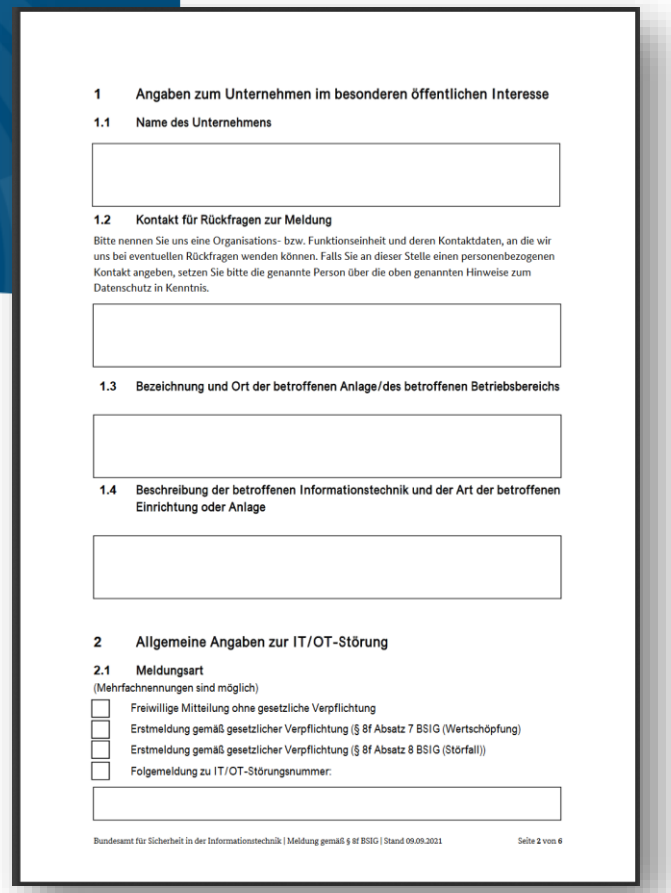
Für alle UBI nach § 8b Abs. 4a BSIG gilt:

„Während einer erheblichen Störung gemäß Absatz 4 Satz 1 Nummer 2, § 8f Absatz 7 Satz 1 Nummer 2 oder Absatz 8 Satz 1 Nummer 2 kann das Bundesamt im Einvernehmen mit der jeweils zuständigen Aufsichtsbehörde des Bundes ***von*** *den betroffenen Betreibern Kritischer Infrastrukturen oder* ***den Unternehmen im besonderen öffentlichen Interesse die Herausgabe*** *der zur Bewältigung der Störung* ***notwendigen Informationen einschließlich personenbezogener Daten verlangen****…“*

Unternehmen im besonderen öffentlichen Interesse

Mit dem IT-Sicherheitsgesetz 2.0 wurden Unternehmen im besonderen öffentlichen Interesse (UBI) eingeführt. Wer hierunter fällt und welche Rechte und Pflichten hiermit einhergehen, finden Sie in den FAQ. Für Störfall-UBI (UBI 3) gilt ab 1.11.2021 eine Meldepflicht. Details hierzu finden Sie ebenfalls in den FAQ.

Wenn Sie Fragen haben, die nicht durch die vorliegende FAQ beantwortet werden, wenden Sie sich gerne per E-Mail unter ubi-buero@bsi.bund.de an das UBI-Büro.



1 Angaben zum Unternehmen im besonderen öffentlichen Interesse

1.1 Name des Unternehmens

1.2 Kontakt für Rückfragen zur Meldung

Bitte nennen Sie uns eine Organisations- bzw. Funktionseinheit und deren Kontaktdaten, an die wir uns bei eventuellen Rückfragen wenden können. Falls Sie an dieser Stelle einen personenbezogenen Kontakt angeben, setzen Sie bitte die genannte Person über die oben genannten Hinweise zum Datenschutz in Kenntnis.

1.3 Bezeichnung und Ort der betroffenen Anlage/des betroffenen Betriebsbereichs

1.4 Beschreibung der betroffenen Informationstechnik und der Art der betroffenen Einrichtung oder Anlage

2 Allgemeine Angaben zur IT/OT-Störung

2.1 Meldungsart

(Mehrfachnennungen sind möglich)

- ☐ Freiwillige Mitteilung ohne gesetzliche Verpflichtung
- ☐ Erstmeldung gemäß gesetzlicher Verpflichtung (§ 8f Absatz 7 BSIG (Wertschöpfung)
- ☐ Erstmeldung gemäß gesetzlicher Verpflichtung (§ 8f Absatz 8 BSIG (Störfall))
- ☐ Folgemeldung zu IT/OT-Störungsnummer:

Bundesamt für Sicherheit in der Informationstechnik | Meldung gemäß § 8f BSIG | Stand 09.09.2021 Seite 2 von 6

Weitere Informationen

UBI Sicherheitsvorfälle melden

FAQ UBI Allgemeine Fragen

Störfall-UBI (UBI 3): FAQ zur Meldepflicht

HK2
Rechtsanwälte

Der Stand der Technik

§ 8a Abs. 1a BSIG-ENT (ITSiG 2.0 RefENT, Mai 2020)

HK2 Rechtsanwälte

„… Die eingesetzten Systeme zur Angriffserkennung ***haben dem jeweiligen Stand der Technik zu entsprechen****. Die* ***Einhaltung des Standes der Technik wird vermutet, wenn*** *die Systeme* ***der Technischen Richtlinie [Bezeichnung] des Bundesamtes*** *in der jeweils geltenden Fassung* ***entsprechen****.*

HK2 Rechtsanwälte

§ 3 Abs. 1 Ziff. 20 BSIG (Aufgaben des BSI)

*„**Beschreibung** und Veröffentlichung **eines Stands der Technik** bei sicherheitstechnischen Anforderungen an IT-Produkte unter Berücksichtigung bestehender Normen und Standards sowie Einbeziehung der betroffenen Wirtschaftsverbände.“*

Zulieferer als **Hersteller**

ESB Professional/Shutterstock.com

Hersteller informationstechnischer Produkte und Systeme (Var. 1)

HK2 Rechtsanwälte

§ 7a BSIG

- Abs. 1: **Untersuchungsrecht** des BSI hinsichtlich auf dem Markt bereitgestellte oder zur Bereitstellung auf dem Markt vorgesehene IT-Produkte und –Systeme. Untersuchung durch Dritte möglich.
- Abs. 2: **Auskunftspflicht** inkl. technischer Details („soweit erforderlich … alle notwendigen Auskünfte …“)
- Abs. 3 **Informationsweitergabe** des BSI an Aufsichtsbehörde des Bundes oder an Ressort, wenn Behörde nicht vorhanden.
- Abs. 4: 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.
- Abs. 5: BSI kann **Öffentlichkeit** namentlich (Hersteller, Produkt) **informieren**, wenn Auskunft unterlassen wird und Gelegenheit zur Stellungnahme gegeben wurde.

HK2 Rechtsanwälte

Was sind IT-Produkte?

§ 2 Ziff. 9a BSIG

IT-Produkte im Sinne dieses Gesetzes sind Software, Hardware sowie alle einzelnen oder miteinander verbundenen Komponenten, die Informationen informationstechnisch verarbeiten.

Weitergabe von Erkenntnissen, wenn erforderlich nach § 3 Abs. 1 S. 2 Nr. 1, 14, 14a, 17, 18 BSIG

HK2 Rechtsanwälte

- *Nr. 1: Abwehr von Gefahren für die Sicherheit der Informationstechnik des Bundes;*
- *Nr. 14: Beratung, **Information und Warnung** der Stellen des Bundes, der Länder sowie **der Hersteller, Vertreiber und Anwender** in Fragen der Sicherheit in der Informationstechnik, insbesondere unter Berücksichtigung der möglichen Folgen fehlender oder unzureichender Sicherheitsvorkehrungen;*
- *Nr. 14a: Verbraucherschutz und **Verbraucherinformation** im Bereich der Sicherheit in der Informationstechnik, insbesondere **durch Beratung und Warnung** von Verbrauchern in Fragen der Sicherheit in der Informationstechnik und unter Berücksichtigung der möglichen Folgen fehlender oder unzureichender Sicherheitsvorkehrungen;*
- *Nr. 17: **Aufgaben** nach den §§ 8a bis 8c und 8f **als zentrale Stelle für** die Sicherheit in der Informationstechnik **Kritischer Infrastrukturen**, **digitaler Dienste** und **der Unternehmen im besonderen öffentlichen Interesse**;*
- *Nr. 18: Unterstützung bei der Wiederherstellung der Sicherheit oder Funktionsfähigkeit informationstechnischer Systeme in herausgehobenen Fällen nach § 5a; [→ Aufgaben/ Befugnisse der nat. behörden für Cybersicherheitszertifizierung]*

HK2 Rechtsanwälte

Hersteller kritischer Komponenten (Var. 2)

- Kritische Komponenten im Sinne von § 2 Ziff. 13 BSIG 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).

Einsatz Kritischer Komponenten durch KRITIS-Betreiber

HK2 Rechtsanwälte

§ 9b Abs. 3 BSIG Untersagung des Einsatzes kritischer Komponenten

- S. 1: Einsatz *kritischer Komponenten* nur zulässig, wenn Hersteller eine Erklärung über seine Vertrauenswürdigkeit (**Garantieerklärung**) gegenüber dem KRITIS-Betreiber abgeben hat.

- S. 3: Garantieerklärung enthält Angaben dazu, **wie** der Hersteller **sicherstellt**, dass die kritische Komponente **nicht über technische Eigenschaften verfügt**, die spezifisch geeignet sind, **missbräuchlich**, insbesondere zum Zwecke von **Sabotage**, **Spionage** oder **Terrorismus** auf die **Sicherheit**, **Vertraulichkeit**, **Integrität**, **Verfügbarkeit** oder **Funktionsfähigkeit** der Kritischen Infrastruktur einwirken zu können.

  „Diese Aussage muss sich auf die Komponente selbst und ihr Zusammenspiel mit anderen Komponenten beziehen… Dabei muss der Hersteller seine Garantieerklärung in Bezug auf sein Endprodukt einschließlich aller ihm zugelieferten Teile abgeben, das heißt auch in Bezug auf die Lieferkette.“ (BT-Drs. 19/28844, S. 44)

- S. 4: BMI legt Einzelheiten der Mindestanforderungen an die Garantieerklärung durch Allgemeinverfügung (Bundesanzeiger) fest.

Untersagungsbefugnisse des BMI

- 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 **jedens Einsatzes** kritischer Komponenten eines Herstellers, § 9b Abs. 5, 7 BSIG

HK2
Rechtsanwälte

Gesetzliche Anforderungen an Einsatz kritischer Komponenten führen zu **faktischen Obliegenheiten** und **vertraglichen Verpflichtungen des Herstellers**.

HK2
Rechtsanwälte

Herstellerhaftung nach ITSiG

enzozo/stock.adobe.com

Antwort der Bundesregierung auf Kleine Anfrage Drucksache 19/27487 v. 10.03.2021, S. 11

HK2 Rechtsanwälte

Erkennt die Bundesregierung, auch mit Blick auf den aktuellen Fall, Probleme bei der Herstellerhaftung?

Wenn ja, wie will sie diesen konkret gesetzgeberisch begegnen, und welche Maßnahmen enthält das „IT-Sicherheitsgesetz 2.0“ (ITSiG2.0) hierzu?

Wenn nein, warum nicht?

Antwort der Bundesregierung auf Kleine Anfrage Drucksache 19/27487 v. 10.03.2021, S. 11

HK2 Rechtsanwälte

Antwort:

… Aufgrund der Vollharmonisierung dieses Rechtsgebiets sind gesetzgeberische Reformen nur auf europäischer Ebene möglich…

Eine punktuelle Überarbeitung der Produkthaftungsrichtlinie ist insoweit im Zuge des Revisionsprozesses zu prüfen, für den die EU-Kom-mission einen Vorschlag in diesem Jahr angekündigt hat

… das IT-Sicherheitsgesetz 2.0 als nationale Regelungsvorschrift [ist] im Übrigen nicht der richtige Standort für derartige gesetzliche Regelungen.

HK2
Rechtsanwälte

Auswirkungen des ITSiG 2.0 auf **Verträge**

Anpassungsbedarf KRITIS ./. Zuliefer

- ITSec Level Agreements/ IT-Security Service and Management Agreements
- Leistungsverträge, EVB-ITs
- Ausschreibungen

- zudem
  - Abgleich mit einschlägigem B3S
  - Geschäftsgeheimnis-Schutzkonzepte
  - Datenschutzvereinbarungen/ -konzepte

IT-Security Service and Management Agreement

1. Ziel, Anwendbarkeit, Verknüpfung mit weiten Verträgen, Rangfolge der Regelungen
2. Definitionen
3. **Technische und organisatorische IT-Sicherheitsmaßnahmen**
4. **IT-Security Change Management**
5. Vergütung
6. Unterbeauftragungsbeschränkungen
7. Umgang mit Audits, Testaten und Zertifikaten
8. Entscheider und Vertretungsregelungen
9. Kommunikation
10. Benachrichtigungspflichten
11. Mitwirkungspflichten
12. Eskalationsregime
13. Beweislastregeln
14. Rechtsfolgenregime
15. Sonstiges
16. Anlagen
    - TOM Spezifikationen
    - Vorlagen Reporting, Benachrichtigungen
    - Konzepte des Anbieters (Datenschutz, IT-Sicherheit)

Auswahl anzupassender Regelungen 1/2

- Hauptleistung am Maßstab des ITSiG 2.0 beschreiben und messen
- Compliance-Klausel zur Anpassung an ändernde Rechtslage
- Vergütung anpassen
- Benachrichtigungspflicht bei Störungen ggü. Betreiber (Spiegelbild gesetzlicher Meldepflicht)

HK2 Rechtsanwälte

Auswahl anzupassender Regelungen 2/2

- Haftungsverteilung anpassen
- Neukalkulation von Haftungshöchstgrenzen
- Anpassung pauschalierten Schadenersatzes
- Gründe außerordentlicher Kündigungsrechte anpassen
- Regelungen zum Geheimnisschutz gem. GeschGehG überprüfen
- Stand-der-Technik-Klauseln anpassen

Verpflichtungen zum Stand der Technik

- Konkrete Verpflichtung auf den Stand der Technik
- Umgang mit Veröffentlichungen des BSI
- Festlegung der Schutzmaßnahmen
  - Maßnahmenbeschreibung
  - Verknüpfung mit IT-Sicherheitszielen
- Methode
  - Nachweis zur Praxiserprobung
  - Nachweis zum Grad der Fortschrittlichkeit
  - Ggf. Standards/ Normungen und Veröffentlichungen von Fachverbänden/ Experten als Maßstab
- Dokumentation
  - Detailtiefe
  - Struktur
- Prüfung und Überprüfung
- Rechtsfolgen
- Umgang mit Angemessenheitserwägungen/ planmäßigem Unterschreiten des SdT

Zudem

- IT-Sicherheitskonzept
- IT-Sicherheitsmaßnahmen
- Dokumentation
- Auditregelungen
- SLA
- Datenschutzkonzept
- …

HK2 Rechtsanwälte

jj-ying-WmnsGyaFnCQ-unsplash

louis-hansel-7RtM37cLJ3c-unsplash

HK2 Rechtsanwälte

Schaffung vs. Begrenzung konkreter vertraglicher Ansprüche gegen Zulieferer

Selbsterklärung zur IT-Sicherheit (UBI)

HK2 Rechtsanwälte

→ Vertragliche Verpflichtung auf:

- **Zertifizierung/en** im Bereich der IT-Sicherheit und Datenschutz
- sonstige **Sicherheitsaudits** oder **Prüfungen** im Bereich der IT-Sicherheit und
- **IT-Sicherheitskonzept** und Umsetzungs-/ Wirksamkeitsnachweis („Sicherstellung“) hinsichtlich der IT-Systeme, -Komponenten und -Prozesse und Dokumentation und wie dabei der **Stand der Technik** eingehalten wird.

Auskunftsrecht gegen und Untersuchung des Hersteller/s *Kritischer Komponenten*

→ Vertragliche Pflicht des Herstellers zur unverzüglichen, umfassenden Benachrichtigung des Betreibers bei behördlichen Verfahren nach § 7a BSIG gegen Hersteller

- Auskunft
- Untersuchung
- bekannte Veröffentlichungen
- Stellungnahmen des Herstellers

- Zudem
  - Verteidigungsklausel
  - Eskalations-Regeln

Garantieerklärung des Herstellers *Kritischer Komponenten*

HK2 Rechtsanwälte

→ **Vertragliche Verknüpfung der Garantieerklärung mit**

- Weiteren Informationspflichten ggü. Mindestanforderungen nach § 9b Abs. 3 S. 2 BSIG und Allgemeinverfügung.
- Nachweis durch Offenlegung ggü. Betreiber oder fachkundigem Dritten
- Vertragsstrafen
- Schadenersatz

Rechtsfolgen für Fälle i.S.v. § 9b Abs. 5 BSIG (Ausschluss der Vertrauenswürdigkeit)

HK2 Rechtsanwälte

→ **Vertragliche Verpflichtungen und Rechtsfolgenverknüpfung**

1. **Pflichtenverstoß gegen die Garantieerklärung**
2. Angabe von **unwahren Tatsachenbehauptungen** in der Garantieerklärung
3. **Mangelnde Unterstützung** von Sicherheitsüberprüfungen und Penetrationsanalysen an seinem Produkt und in der Produktionsumgebung („erforderlicher Umfang in angemessener Weise“?)
4. Schwachstellen oder Manipulationen werden nicht unverzüglich, nachdem er davon Kenntnis erlangt, **beseitigt** und dem Betreiber der Kritischen Infrastruktur **gemeldet**.
5. Die kritische Komponente auf Grund von **Mängeln** ein erhöhtes Gefährdungspotenzial aufweist oder aufgewiesen hat, missbräuchlich auf die Sicherheit, Vertraulichkeit, Integrität, Verfügbarkeit oder Funktionsfähigkeit der Kritischen Infrastruktur einwirken zu können.
6. Die kritische Komponente über **technische Eigenschaften** verfügt oder verfügt hat, die spezifisch geeignet sind oder waren, missbräuchlich auf die Sicherheit, Vertraulichkeit, Integrität, Verfügbarkeit oder Funktionsfähigkeit der Kritischen Infrastruktur einwirken zu können.

Wirkung auf Non-Kritis-Verträge

Phil Lenoir/Shutterstock.com

HK2 Rechtsanwälte

Zu guter Letzt

Wissen Sie, welche IT-Sicherheitsverträge mit welchen konkreten Inhalten derzeit für und gegen Ihr Unternehmen gelten? Kennen Sie sie, soweit Ihr Bereich betroffen ist?

In welchen Vertragsverhandlungen zur IT-Sicherheit befinden Sie sich derzeit?

Wurden die geltenden Verträge zur IT-Sicherheit im Team mit den Abteilungen IT, IT-Sicherheit, IT-Recht und DSB erstellt oder geprüft?

Wie bewerten Sie, ob und wie Ihre Verträge die Anforderungen des ITSiG 2.0 im Sinne Ihrer Interessen umsetzen?

Wer gibt die interne Freigabe zur Zeichnung eines Vertrags mit IT-Sicherheitsbezügen?

HK2
Rechtsanwälte

hk2.eu/newsletter

HK2
Rechtsanwälte

Kontakt

www.hk2.eu

www.comtection.de

linkedin.com/in/karstenbartels

twitter.com/KarstenUBartels