TeleTrusT "IT-Sicherheitsrechtstag 2021"

Berlin, 24.09.2021

Allgemeine Einführung: IT-Sicherheitsgesetz 2.0

Mareike Gehrmann

Taylor Wessing, Rechtsanwältin und Fachanwältin für IT-Recht

Inhalt

TaylorWessing

Aktuelle Gefährdungslage

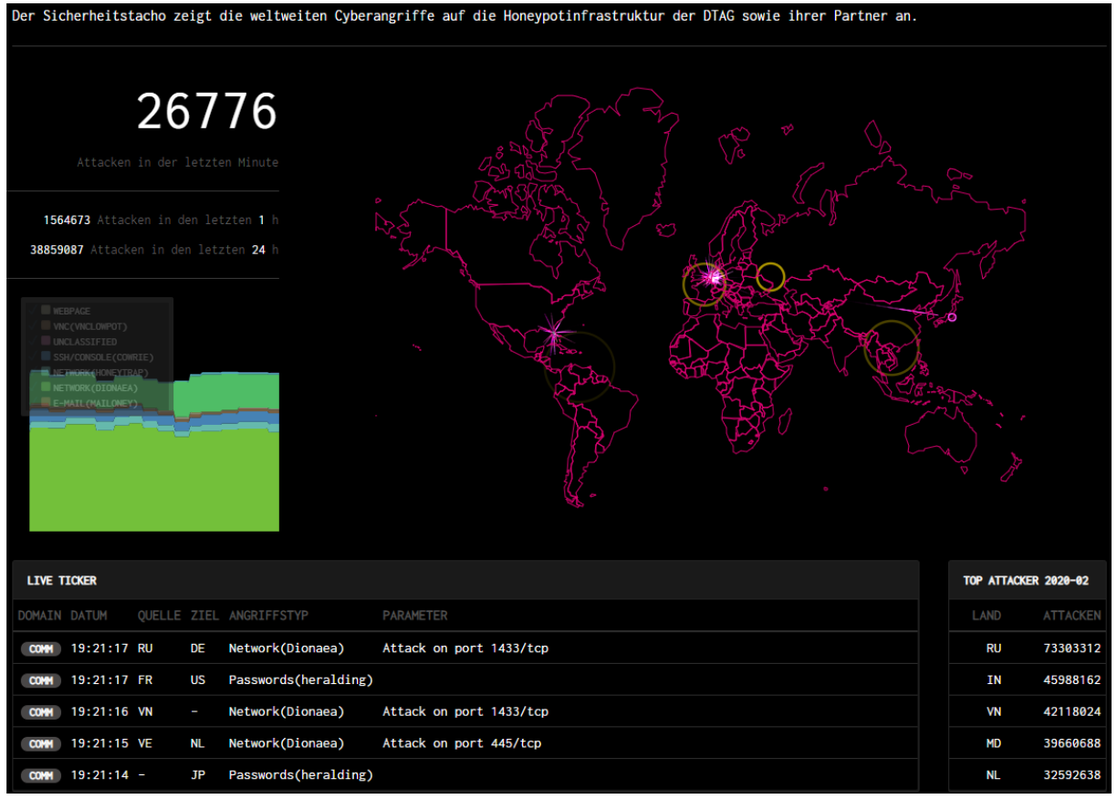
Gefährdungslage für Unternehmen

Beispiel: Sicherheitstacho der DTAG

- Weltweite Cyberangriffe auf die „Honeypot“-Infrastruktur der DTAG
- Zirka 25.000 Angriffe pro Minute

Unternehmen sind ständiges Ziel von Hackerangriffen

- Bei einer Studie des Security-Anbieters Proofpoint gaben 67 Prozent aller befragten Unternehmen in Deutschland, Österreich und der Schweiz an, Opfer eines Cyberangriffs geworden zu sein.*
- Es wurden branchenübergreifend 200 Security-Verantwortliche befragt. Phishing wurde als größtes Problem gesehen.
- Versicherungen: Entwicklung von Produkten für Unternehmen (und Verbraucher)



Quelle: https://sicherheitstacho.eu/start/main

*Quelle: https://www.proofpoint.com/de/resources/white-papers/it-sicherheitsstudie-dach

DSGVO-Bußgeldverfahren wegen mangelnder Cyber Security

Einige Beispiele u.a.:

Marriott Inc.

Im Fall der Marriott Inc. hatten Hacker bei der Hotelkette Starwood von 2016 bis 2018 Zugriff auf die personenbezogenen Daten von mehr als 339 Mio. Kunden. Dazu gehörten auch Zahlungsinformationen. Marriott Inc. kaufte die Hotelkette auf, jedoch fiel das Datenleck erst 2018 auf. Das Bußgeld belief sich auf über 110 Mio. EUR. Marriott hat beim Unternehmenskauf keine Prüfung der Cyber Security des Unternehmens vorgenommen.

British Airways

Hacker leiteten 2018 den Besucherverkehr der Webseite von British Airways auf eine betrügerische Webseite um. Die personenbezogenen Daten von 550 Mio. Kunden konnten abgeschöpft werden. Zunächst wurde ein Bußgeld in Höhe von 180 Mio. EUR verhangen, welches im Nachhinein auf 20 Mio. EUR herabgesenkt wurde. British Airways hatte keine hinreichenden technischen Schutzmaßnahmen ergriffen, um Hackerangriffen vorzubeugen.

1&1 GmbH

Durch das unzureichende Authentifizierungsverfahren im Kunden-Callcenter gelang es einer nichtberechtigten Person Daten eines Kunden abzugreifen und ihn anschließend strafrechtlich relevant zu stalken. Es wurde ein Bußgeld in Höhe von 9,55 Mio. EUR verhangen, welches durch das LG Bonn auf 900.000 EUR reduziert wurde (Urt. v. 11.11.2020 Az. 29 OWi 1/20).

Zugriffsbeschränkung Bsp.: Gesundheitsdaten

Europaweit wurden mehrere Bußgelder gegen Unternehmen im Gesundheitssektor – vor allem Krankenhäuser – erlassen, da der Zugriff auf die besonders schützenswerten Gesundheitsdaten nicht hinreichend reguliert wurde. Somit konnte etwa Personal uneingeschränkt auf alle Gesundheitsdaten der Patienten zugreifen. Das höchste Bußgeld wurde in Schweden gegen das Capio St. Göran Krankenhaus in Höhe von 2,9 Mio. EUR verhangen. Es besteht auch die Pflicht Daten vor unbefugten, internen Zugriffen zu schützen.

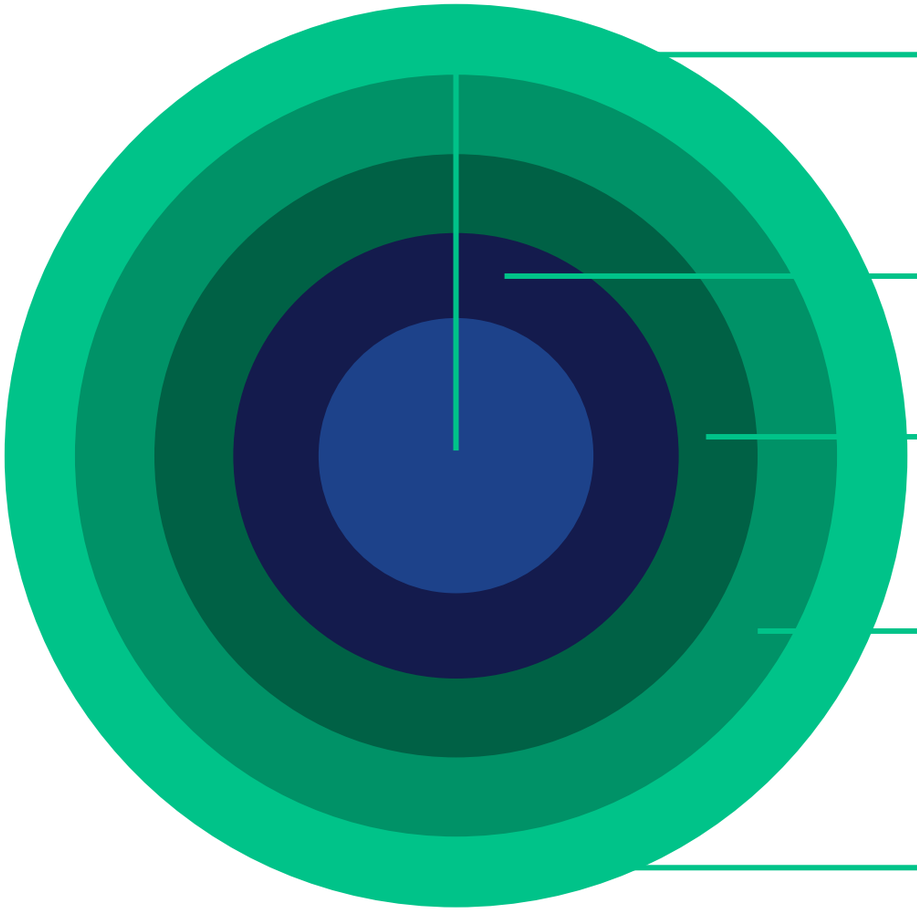
TaylorWessing

Rechtslage

Rechtslage seit 2015 – Prävention

IT-Sicherheitsstandards (ISO 27001, BSI Grundschutz etc.)

Für Unternehmen ergibt sich aus einer Vielzahl von Rechtsnormen – neben den allgemeinen zivilrechtlichen Vorgaben – die Pflicht, hinreichende **Schutzmaßnahmen** zu **implementieren** und **Cyber-Vorfälle zu melden**.



Regulatorische Anforderungen, Int. Standards

IT-SiG / BSI-KritisV

Sondergesetze (u.a. § 13 Abs. 4 und 7 TMG / § 109 Abs. 2 TKG)

DSGVO (u.a. Art. 25, 28, 32, 33, 34 DSGVO)

Allg. (zivilrechtliche) Haftung / Produkthaftung

Übersicht: Regulierungen und Vorhaben

1. Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz 2.0)
2. Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union und zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS 2 RL)
   - Ablösung und Weiterentwicklung der 2016 in Kraft getretenen NIS-RL
3. Cybersicherheitsstrategie der EU für die digitale Dekade
4. Cybersicherheitsstrategie für Deutschland 2021
   - Ablösung und Weiterentwicklung der Cyber-Sicherheitsstrategie 2016
5. Zweite Änderungsverordnung der Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz" (BSI-KritisV)
   - Tritt am 01.01.2022 in Kraft
   - Keine Umsetzung des IT-SiG 2.0, sondern Anpassung im Rahmen der Evaluierung gem. § 9 BSI-KritisV: Keine Regelungen zur Bestimmung von Unternehmen im besonderen öffentlichen Interesse oder zu Schwellenwerten für den Sektor „Siedlungsabfallentsorgung“

TaylorWessing

Update IT-SiG 2.0

IT-Sicherheitsgesetz 2.0 (IT-SiG 2.0)

- Der lange Weg zum IT-SiG 2.0
  - 27.03.2019 – Erster Entwurf
  - 05.05.2020 – Zweiter Entwurf
  - 19.11.2020 – Dritter Entwurf
  - 16.12.2021 – Kabinettsfassung
  - 01.03.2021 – Anhörung im Ausschuss für Inneres und Heimat
  - 19.04.2021 – Änderungsantrag von CDU/CSU und SPD
  - 20.04.2021 – Antrag der Fraktionen der CDU/CSU und SPD auf eine Entschließung des 4. Ausschusses des Deutschen Bundestages – Ausschuss für Inneres Heimat (am 21.04.2021 auch von FDP / AfD Fraktion)
  - 23.04.2021 – Abstimmung im Bundestag und Annahme des Gesetzesentwurfs
  - 07.05.2021 – Billigung durch den Bundesrat
  - 28.05.2021 – Inkrafttreten
- Änderung von BSI-Gesetz (BSIG) und anderer bereichsspezifischer Gesetze zur IT-Sicherheit

Erweiterung des Adressatenkreises (1)

- Betreiber kritischer Infrastrukturen (KRITIS): Erweiterung um den Sektor **Siedlungsabfallentsorgung**
- Mehr KRITIS-Betreiber durch BSI-KritisV 2.0
  - Tiefere Schwellenwerte (z.B. bei IT-Hosting/Housing/Exchanges, Stromerzeugung) und geänderte Schwellenwerte
  - Neue KRITIS-Anlagen in bestehenden Sektoren (z.B. Ausweitung des Anlagenbegriffes insbesondere auf „Software und IT-Dienste, die für die Erbringung einer kritischen Dienstleistung notwendig sind“)
    - ▶ Regierung schätzt, dass über 270 weitere Unternehmen als KRITIS-Betreiber einzustufen sind, zusätzlich zu den bereits zirka 1.600 bestehenden KRITIS-Betreibern
    - ▶ Unternehmen im besonderen öffentlichen Interesse und der Sektor „Siedlungsabfallentsorgung“ sind noch nicht berücksichtigt
- Achtung: Spezialgesetze neben IT-SiG 2.0

➔ Beispiel: Krankenhäuser, § 75c SGB V

Erweiterung des Adressatenkreises (2)

– „**Unternehmen im besonderen öffentlichen Interesse**“ (§ 2 Abs. 14 Satz 1 Nr. 2 BSIG) sind nicht unmittelbar kritische Infrastrukturen, werden aber als solche behandelt. Sie unterliegen einem abgeschwächten Pflichtenkatalog.

Dazu gehören Unternehmen, die:

1. Güter gem. § 60 Absatz 1 Nr. 1 und 3 der Außenwirtschaftsverordnung in der jeweils geltenden Fassung herstellen oder entwickeln (Bsp.: Rüstungshersteller, Hersteller von IT-Produkten für die Verarbeitung staatlicher Verschlusssachen),
2. nach ihrer inländischen Wertschöpfung zu den größten Unternehmen in Deutschland gehören und daher von erheblicher **volkswirtschaftlicher Bedeutung** für die Bundesrepublik Deutschland (BRD) sind oder die für solche Unternehmen als **Zulieferer** wegen ihrer Alleinstellungsmerkmale von wesentlicher Bedeutung sind oder
3. Betreiber eines Betriebsbereichs der oberen Klasse im Sinne der Störfall-Verordnung in der jeweils geltenden Fassung sind oder gem. § 1 Absatz 2 der Störfall-Verordnung diesen gleichgestellt sind.

– Unternehmen, die weniger als 50 Personen beschäftigen und deren Jahresumsatz 10 Mio. Euro (Kleinst- und kleine Unternehmen) sind ausgeschlossen (wie bei KRITIS-Betreibern und Anbietern digitaler Dienste)

Erweiterung des Adressatenkreises (3)

– Nr. 2 „Wertschöpfungskriterium“: Zur Bestimmung von Unternehmen i.S.v. § 2 Abs. 14 Satz 1 Nr. 2 BSIG wird das BMI ermächtigt, durch **Rechtsverordnung** abstrakt-generelle Kriterien festzulegen, durch die eine Bestimmung der Verpflichteten möglich ist. Die Berechnung der wirtschaftlichen Kennzahlen zur Bestimmung der volkswirtschaftlichen Bedeutung der Unternehmen und auch die erfassten Unternehmen sollen sich dabei am **Gutachten der Monopolkommission** nach § 44 Abs. 1 GWB (sog. Hauptgutachten) orientieren. Auszug aus dem Gutachten der Monopolkommission von 2020 (Seite 80 ff.):

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

Rang	Trend[2]	Unternehmen[3]	Wertschöpfung[4] in Mio. Euro	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

Neue Pflichten (1)

KRITIS-Betreiber

- Bislang: Implementierung von Cyber Security Maßnahmen, die dem Stand der Technik entsprechen; regelmäßiger Nachweis alle zwei Jahre (§ 8a Abs. 1 und 3 BSIG); Meldung erheblicher Störungen (§ 8b Abs. 4 BSIG)
- Wesentliche Neuerungen:
  - Einsatz von Systemen zur **Angriffserkennung** ab dem 01.05.2023 (§ 8a Abs. 1a BSIG)
    - ► BSI stellt zur Unterstützung der Betreiber eine Malware Information Sharing Plattform (MISP) bereit, damit Informationen, die sich zum Generieren von Erkennungsmustern von Cyber-Angriffen verwenden lassen, ausgetauscht werden und dadurch Systeme zur Angriffserkennung aktuell gehalten werden können
  - **Registrierung** beim BSI, zusätzlich zur Einrichtung einer jederzeit erreichbaren Kontaktstelle für die Kommunikation mit dem BSI (§ 8b Abs. 3 BSIG)
  - **Datenherausgabepflicht**: BSI kann „die Herausgabe der zur Bewältigung der Störung notwendigen Informationen einschließlich personenbezogener Daten verlangen“ (§ 8b Abs. 4a BSIG)

Neue Pflichten (2)

KRITIS-Betreiber

– Wesentliche Neuerungen:

- **Pflicht zur Anzeige** des geplanten Einsatzes sog. **Kritischer Komponenten** gegenüber dem BMI (§ 9b Abs. 1 BSIG)
  - ▶ Beifügung einer Garantieerklärung des Herstellers über dessen Vertrauenswürdigkeit (§ 9b Abs. 3 S. 1 und 2 BSIG) und Aufrechterhaltung dieser Garantieerklärung
  - ▶ Garantieerklärung erstreckt sich auf gesamte Lieferkette des Herstellers
  - ▶ Festlegung der Mindestanforderungen an die Garantieerklärung durch eine Allgemeinverfügung des BMI
  - ▶ Untersagungsbefugnis des BMI bis zum Ablauf von zwei Monaten nach Anzeige bei Beeinträchtigung von öffentlicher Ordnung oder Sicherheit
  - ▶ Nachträgliche Untersagungsbefugnis wenn sich die Komponente bereits im Einsatz befindet
- **Neue Informations- und Meldepflichten**
- **Freiwilliges IT-Sicherheitskennzeichen (Verbrauchersiegel)**

Pflichten für UNÖFI

Unternehmen im besonderen öffentlichen Interesse

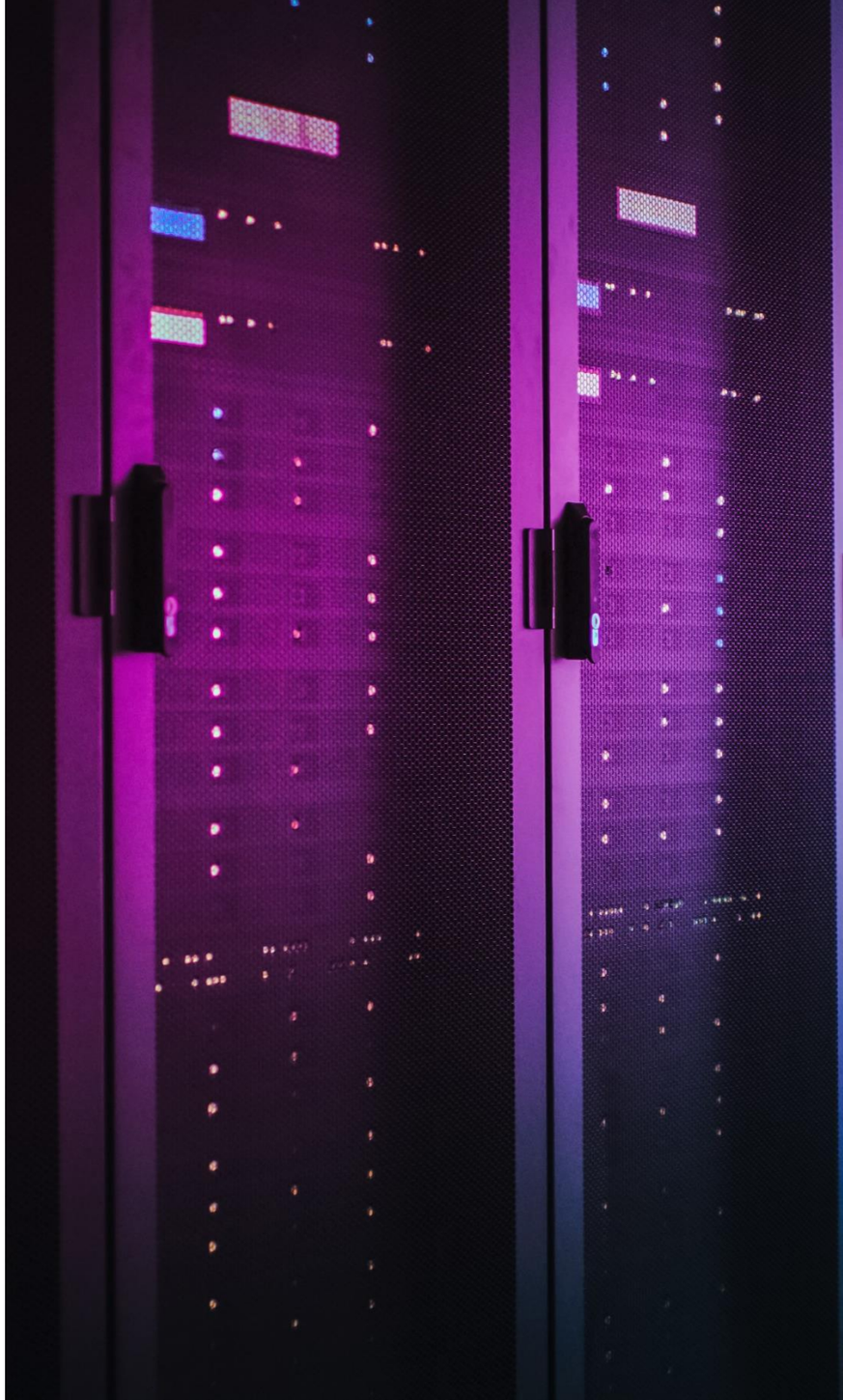
– Wesentliche Pflichten

- **Registrierung** mit der Vorlage der ersten Selbsterklärung beim BSI (§ 8f Abs. 5 Satz 1 BSIG) beim BSI
- **Benennung** einer werktags von 8 Uhr und 17 Uhr **erreichbaren Stelle**
- UNÖFI nach § 2 Abs. 14 Nr. 1 oder 2 BSIG: Abgeschwächter Pflichtenkatalog sieht die Pflicht zur Vorlage einer **Selbsterklärung über die IT-Sicherheit** vor (§ 8f Abs. 1 BSIG), die alle zwei Jahre in aktualisierter Form vorzulegen ist
  - ► Unzureichende Cyber Security Maßnahmen stellen keine Pflichtverletzung dar, bei Hinweisen des BSI besteht keine Pflicht zur Umsetzung dieser
  - ► Unternehmen gem. § 2 Abs. 14 Nr. 1 BSIG: ab 01.05.2023; Unternehmen gem. § 2 Abs. 14 Nr. 2 BSIG: frühestens zwei Jahre nach Inkrafttreten der (noch zu erstellenden RechtsVO) gem. § 10 Abs. 5 BSIG
- **Meldepflichten**
- **Datenherausgabepflicht**

Weitere Änderungen (1)

Anbieter digitaler Dienste

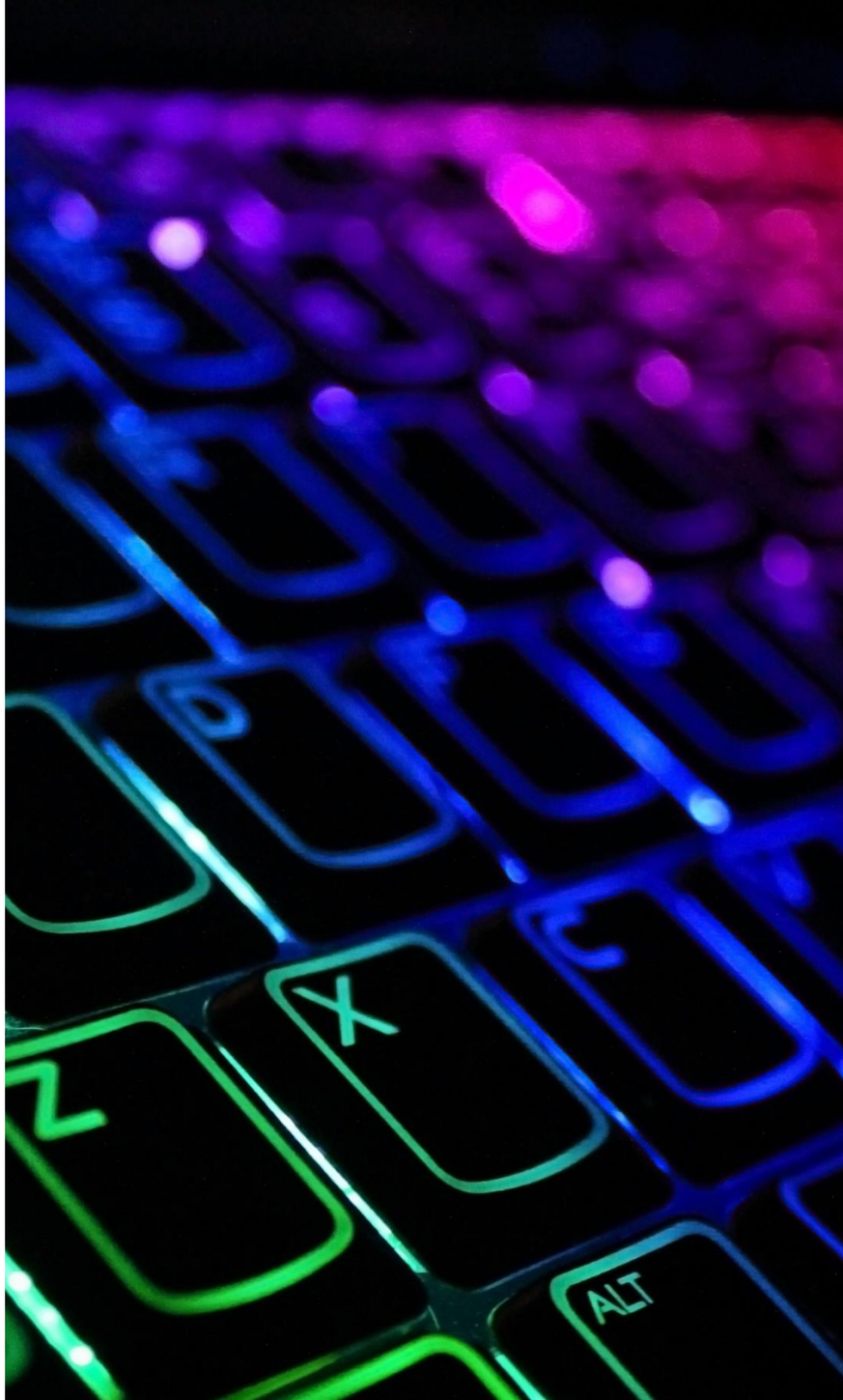
- Neben KRITIS-Betreiber und UNÖFI = Primäre Adressaten des IT-SiG
- Anbieter von Online-Marktplätzen, Online-Suchmaschinen, Cloud-Computing
- Wesentliche Neuerungen:
  - Punktuelle Änderungen
  - Verschärfung des Bußgeldrahmens
  - Anordnungsbefugnis des BSI
- **Wesentlicher Unterschied zu KRITIS-Betreibern:**
  Während **KRITIS-Betreiber** im Hinblick auf ihre Cyber Security Maßnahmen auch für eine qualitativ oder zeitlich unzureichende Umsetzung haften (KRITIS-Betreiber dienen **unmittelbar dem Funktionieren des Gemeinwesens**) sieht § 14 Abs. 2 Nr. 8 BSIG dies für **Anbieter digitaler Dienste** nur vor, wenn geeignete und verhältnismäßige technische und organisatorische Maßnahmen gar **nicht getroffen** werden.



Weitere Änderungen (2)

Hersteller von IT-Produkten

- Einsatz von kritischen Komponenten wird an Informations- und Mitwirkungspflichten der Hersteller geknüpft (§ 9b BSIG)
  - Beispiel: Unterstützung bei der Sicherheitsüberprüfung der Komponenten
- Untersagung des Einsatzes ist an die Vertrauenswürdigkeit des Herstellers gekoppelt (Untersagung = erheblicher Reputationsschaden)
- Abgabe einer Garantieerklärung (§ 9b Abs. 3 BSIG)
- Komponente darf nicht über technische Eigenschaften verfügen, die spezifisch geeignet sind, missbräuchlich, insbesondere zum Zwecke von Sabotage, Spionage oder Terrorismus auf die Sicherheit, Vertraulichkeit, Verfügbarkeit oder Funktionsfähigkeit der KRITIS einzuwirken
- Unverzügliche Beseitigung von Schwachstellen von IT-Produkten und Meldung an KRITIS-Betreiber



Bußgelder

- **Erweiterung des Bußgeldkatalogs**

- **Sprunghafte Erhöhung der Bußgelder**
  - Bislang: bis zu 100.000 Euro
  - Jetzt: je nach Fall (i) bis zu 2 Mio. Euro, (ii) bis zu 1 Mio. Euro, (iii) bis zu 500.000 Euro oder (iv) bis zu 100.000 Euro
    - Durch Verweis auf § 30 Abs. 2 Satz 3 OWiG kann sich die Bußgeldhöhe sogar noch auf bis zu **20 Mio. Euro verzehnfachen**

Mehr Befugnisse für das BSI

Wesentliche Änderungen

- Erweiterungen von Prüf- und Kontrollbefugnissen des BSI zum Schutz der IT der Bundesverwaltung u.a. durch Festlegung von Mindeststandards
- Schaffung von Befugnissen zur Detektion von Schadprogrammen zum Schutz der Regierungsnetze
- Befugnis zur Abfrage von Bestandsdaten bei Anbietern von Telekommunikations-diensten, um Betroffene über Sicherheitslücken und Angriffe zu informieren
- Rechtsgrundlage für das BSI, Sicherheitslücken an den Schnittstellen informationstechnischer Systeme zu öffentlichen TK-Netzen zu detektieren sowie Einsatz von Systemen und Verfahren zur Analyse von Schadprogrammen und Angriffsmethoden
- Schaffung einer Anordnungsbefugnis des BSI gegenüber Telekommunikations- und Telemedienanbietern zur Abwehr spezifischer Gefahren für die Informationssicherheit
- Beschreibung und Veröffentlichung eines Stands der Technik bei sicherheitstechnischen Anforderungen an IT-Produkte
- Zuständigkeit für den „digitalen Verbraucherschutz“

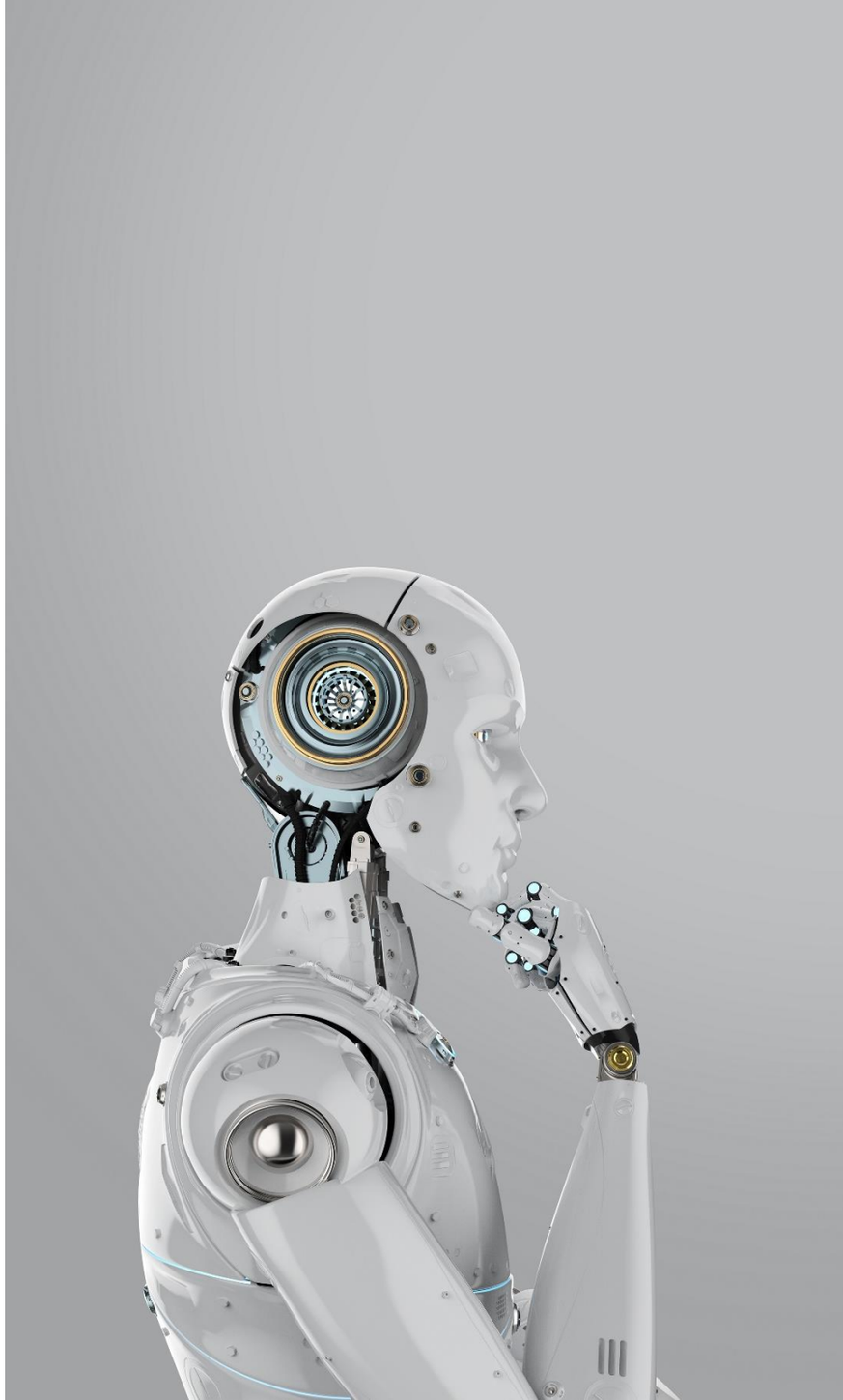
TaylorWessing

Kritik und To Do`s

Kritik

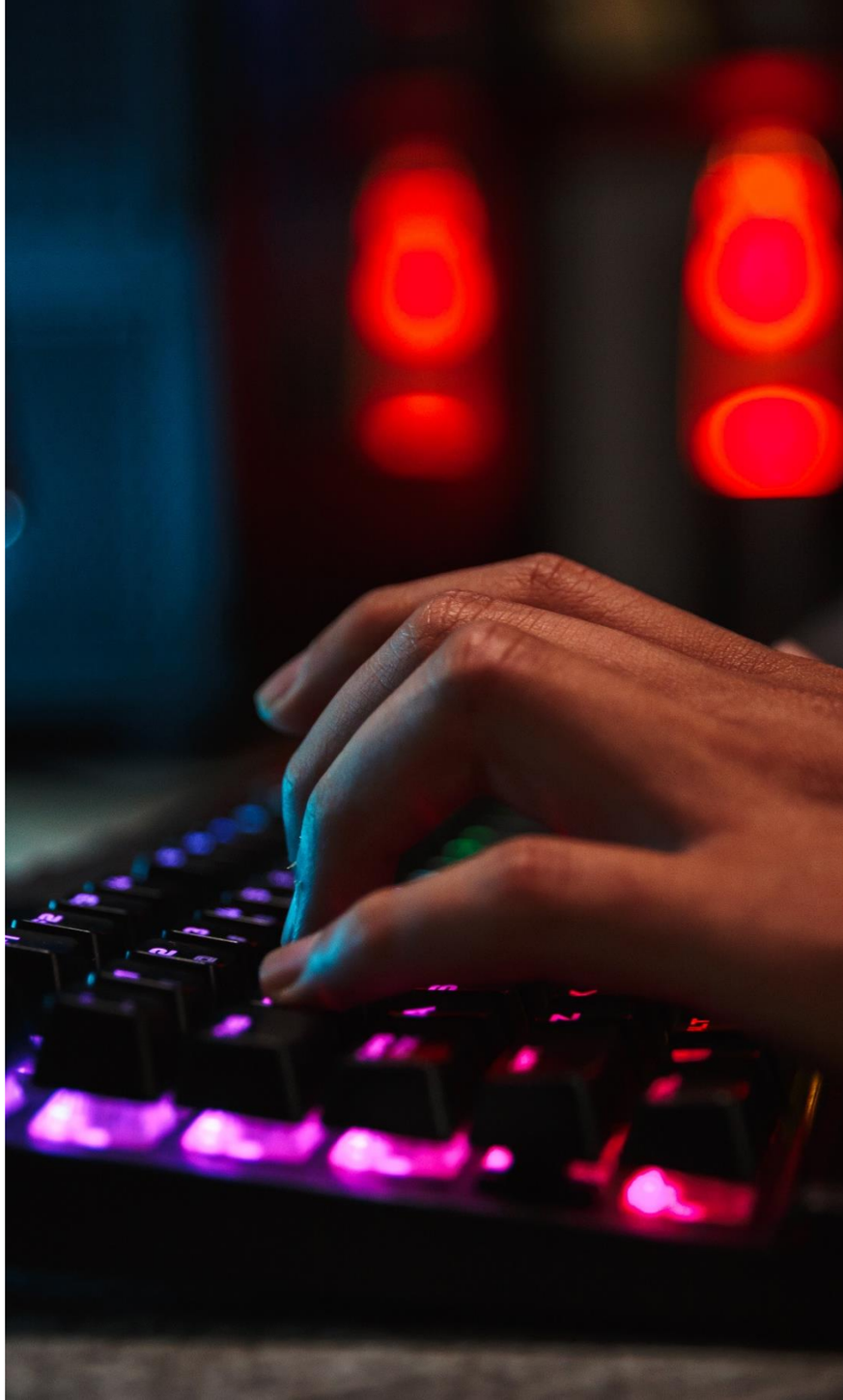
Insbesondere:

- Kritik an Verhältnismäßigkeit der Bußgelder (ohne Berücksichtigung des Jahresumsatzes)
- Mangelnde Rechtssicherheit: Wesentliche Festlegungen durch Allgemeinverfügung oder Rechtsverordnung
  - Beispiel: Bestimmung der UNÖFI
- Grundrechtliche und staatsorganisationsrechtliche Bedenken
- Kritik an der Befugniserweiterung des BSI
- BSI bleibt nachgeordnete Behörde vom BMI
- „Nach dem Gesetz ist vor dem Gesetz“ – Brauchen wir immer so lange?



To Do´s – Was ist zu tun?

- **Bestehende KRITIS-Betreiber**
  - Neue KRITIS-Anlagen prüfen, Umsetzung von Cyber Security Maßnahmen
  - Geänderte Schwellenwerte prüfen
  - Umsetzung neuer Meldepflichten
- **Neue KRITIS-Betreiber**
  - Identifizierung als KRITIS-Betreiber
  - Registrierung als KRITIS-Betreiber beim BSI
  - Umsetzung von Cyber Security Maßnahmen und Meldepflichten
- **KRITIS, insbesondere Telekommunikation**
  - Identifizierung Kritischer Komponenten
  - Kritische Komponenten melden und freigeben
- **Unternehmen im besonderen öffentlichen Interesse**
  - Registrierung
  - Umsetzung von Cyber Security Maßnahmen und Meldepflichten



TaylorWessing

Taylor Wessing

Ihre Ansprechpartnerin

Als Fachanwältin für IT-Recht leitet Mareike Christine Gehrmann ihre Mandanten durch den Wandel der Digitalisierung. Unternehmen und Behörden schätzen ihren Rat. Mit ausgewiesener Expertise aus zahlreichen Digitalisierungsprojekten berät sie ihre Mandanten zu Datenschutz, Cybersecurity und zum IT-Vertragsrecht. Agile Programmierung, SaaS, IT-Sourcing, Lizenzmanagement und Open Source gehören zu ihrem täglichen Geschäft.

Sie ist Expertin im lösungsorientierten Arbeiten mit Mittelständlern und Global Playern, vor allem in den Branchen Versicherung, Gesundheit und Personaldienstleistung. Ferner arbeitet sie grenzüberschreitend mit dem niederländischen Team von Taylor Wessing zusammen und berät vor allem niederländische Unternehmen beim Eintritt in den deutschen Markt.

Mareike Christine Gehrmann publiziert, hält Vorträge und ist Mitglied im Expertennetzwerk "IT-Compliance, IT-Recht und IT-Security" der Computerwoche. Seit dem Wintersemester 2021/2022 ist sie Lehrbeauftragte an der Hochschule Niederrhein für „Verwaltungs- und IT-Recht“ im Studiengang „BCSM“.

Seniorität:

- 2012 Zulassung zur Anwaltschaft; 8 Jahre anwaltliche Berufserfahrung
- Seit 2017 Salary Partner bei Taylor Wessing

Sprachen

- Deutsch, Englisch

Nominiert als eine der besten TMT-Expertinnen in Deutschland, Women in Business Law Expert Guide 2021

Nominiert als eine der besten Privacy & Datenschutz-Expertinnen in Deutschland, Women in Business Law Expert Guide 2021

Ausgezeichnet als eine der besten TMT-Expertinnen in Deutschland, Women in Business Law Expert Guide 2020

Nominiert für den „Europe Women Business Award“ in der Kategorie „Best in Privacy & Data Protection“, 2019

Nominiert für den „Finance Monthly Magazine Global Award“ in der Kategorie Telecommunications – Lawyer of the Year – Germany, 2019

Mareike Christine Gehrmann

Salary Partner
Düsseldorf

+49 211 8387-189
m.gehrmann@taylorwessing.com

Beratungsschwerpunkte

- Datenschutz
- Informationstechnologie/ Telekommunikation
- Litigation & Dispute Resolution

Unser Service für Sie

Coronavirus // Antworten zu rechtlichen Implikationen

Das Coronavirus (2019-nCoV) stellt neben Medizin und Politik auch die Wirtschaft vor neue Herausforderungen. Bei Taylor Wessing beschäftigen wir uns intensiv mit den rechtlichen Implikationen der Pandemie.

Auf der Seite Coronavirus // Antworten zu rechtlichen Implikationen möchten wir Sie zu den rechtlichen Implikationen für Ihren Geschäftsbetrieb auf dem Laufenden halten, um die in dieser Situation notwendigen Schritte nicht zu versäumen und künftige Streitigkeiten soweit wie möglich zu vermeiden.

Pulse - Das Coronavirus Update von Taylor Wessing

Bleiben Sie auf dem Laufenden mit unserem wöchentlichen Newsletter **Pulse – das Coronavirus Update**. Klicken Sie bitte hier für die Anmeldung.

Corona Task Force

Bei individuellen Fragen zur Thematik steht Ihnen unsere Corona Task Force unter corona.task@taylorwessing.com und +49 211 8387 216 jederzeit zur Verfügung.

PlugIn

Die Wirtschaft digitalisiert sich in rasender Geschwindigkeit. Unter dem Begriff ‚Digitale Transformation' setzt sich jede Branche mit den neuen, technischen Möglichkeiten auseinander. Es entstehen Produkte, Dienstleistungen und Prozesse, die bislang denkbar, aber so nicht umsetzbar waren. Passen unsere aktuellen, rechtlichen Grundlagen dazu und gewährleisten einen verbindlichen Rahmen – oder überholt die Digitalisierung gerade das Recht? Auf unserer Plattform PlugIn schreiben unsere Experten monatlich aus erster Hand über das Recht der digitalen Zukunft.

Podcast – Law aufs Ohr

Der Taylor Wessing-Podcast LAW AUFS OHR informiert über Zukunftstechnologien aus Sicht von Anwälten, die sich täglich mit dem Recht der digitalen Zukunft beschäftigen. Der Podcast bietet Weitsicht und Einsichten, spricht sowohl Rechtskundige als auch Nicht-Juristen an und schlägt eine Brücke zwischen Paragrafen und Alltag. Er bleibt nicht bei den juristischen Implikationen der digitalen Transformation stehen, sondern versucht ihre Tragweite für Unternehmen, Verbraucher und Rechtsanwälte zu erfassen. Das Recht der digitalen Zukunft – hier besprechen wir es.

Europa > Mittlerer Osten > Asien

taylorwessing.com