Bird & Bird

Risikomanagement und Haftung für Sicherheitspannen nach DSGVO und ITSiG

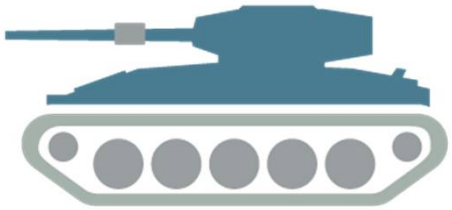
CODE 2018

11. Juli 2018, CODE Jahrestagung

Dr. Alexander Duisberg, Bird & Bird LLP

Übersicht

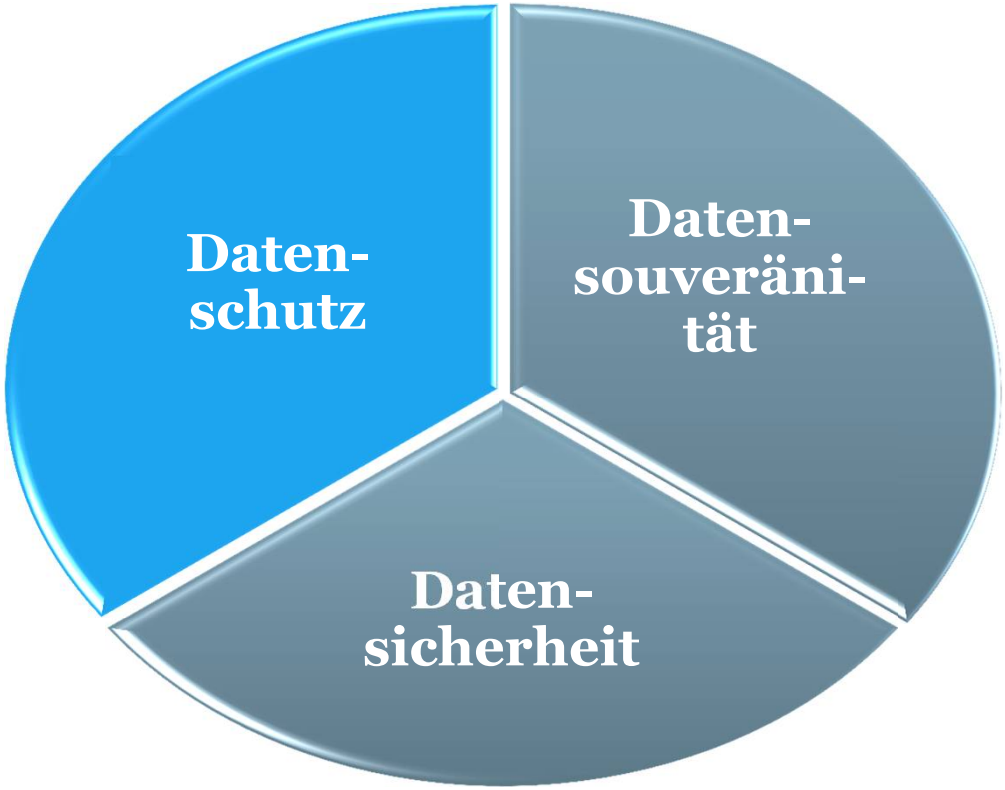
- Datenschutz und Datensicherheit – das neue Wertgefüge der Digitalisierung
- Frühwarnsysteme und Überwachungspflichten – Haftung von Vorstand und Aufsichtsrat
- IT Sicherheitsgesetz und NIS Richtlinie – praktische Handhabe für Unternehmen im Verteidigungssektor
- Betriebs- und Geschäftsgeheimnisse in der Digitalisierung
- Sicherheitspannen – Anforderungen und praktische Erfahrungen
- Fazit



Bird & Bird

Datenschutz und Datensicherheit – das neue Wertgefüge der Digitalisierung

Drei Felder der Betrachtung



Bird & Bird

Einleitung (1)

- Seit 25. Mai 2018 in Kraft
- Direkt anwendbar in jedem Mitgliedstaat (MS)
- Ersetzt Datenschutzrichtlinie 95/46/EC und nationale DS-Gesetze
- Ziel: Harmonisierung des Rechtsrahmens
- Aber: nationale Abweichungen möglich, z. B.
  - Rechtmäßigkeit der Verarbeitung zur Erfüllung einer rechtlichen Verpflichtung (Art. 6 (1) c und e, (2))
  - Löschung von Daten (Art. 17 (1) e)
  - Datenschutz-Folgenabschätzung (Art. 35 (10))
  - DSB Anforderungen (Art. 37 (4))
  - Beschäftigtendatenschutz (Art. 88 (1))

Einleitung (2)

Sachlicher Anwendungsbereich (Art. 2 DSGVO)

- Automatisierte Verarbeitung von Daten
- Nichtautomatisierte Verarbeitung von Daten, die in einem Dateisystem gespeichert sind/werden sollen

Räumlicher Anwendungsbereich (Art. 3 DSGVO)

- Verarbeitungstätigkeit einer Niederlassung
  - In der EU
  - Außerhalb der EU (!), falls die Betroffenen in der EU sind und diesen
    - Waren und Dienste angeboten werden oder
    - Deren Verhalten beobachtet wird

Bußgelder – Zwei Stufen

Art. 83 (4):

Bis zu €10 Mio. oder 2% des weltweiten Umsatzes für Verstöße, z.B.:

- Führung der Verzeichnisse von Verarbeitungstätigkeiten
- Implementierung von TOMs
- Meldung von Verstößen
- Benennung eines DSB
- Verarbeitung nur nach Weisung des Verantwortlichen (Auftragsverarbeiter)

Art. 83 (5):

Bis zu €20 Mio. oder 4% des weltweiten Umsatzes für Verstöße, z.B.:

- Grundsätze der Verarbeitung, einschließlich Bedingungen an die Einwilligung
- Anforderungen an internationalen Datentransfer
- Betroffenenrechte
- Nichteinhaltung von behördlichen Anweisungen

Big Data – was ermöglicht die DSGVO?

"Datenschutz darf Big Data Management nicht verhindern"
(Angela Merkel, IT Gipfel 2016)

Datenminimierung?
- Überkommenes Prinzip
- Relevant für Zweckbindung

Zweckbindung und Zweckgestaltung?
- Begrenzte Spielräume (Art. 6 Abs. 4 DSGVO)
- Big Data geht weiter

Nach der Reform ist vor der Reform?
- D = Vorreiter für Rahmenbedingungen Digitalisierung?
- Plattform Industrie 4.0, Industrial Data Space wichtige Treiber

Bird & Bird

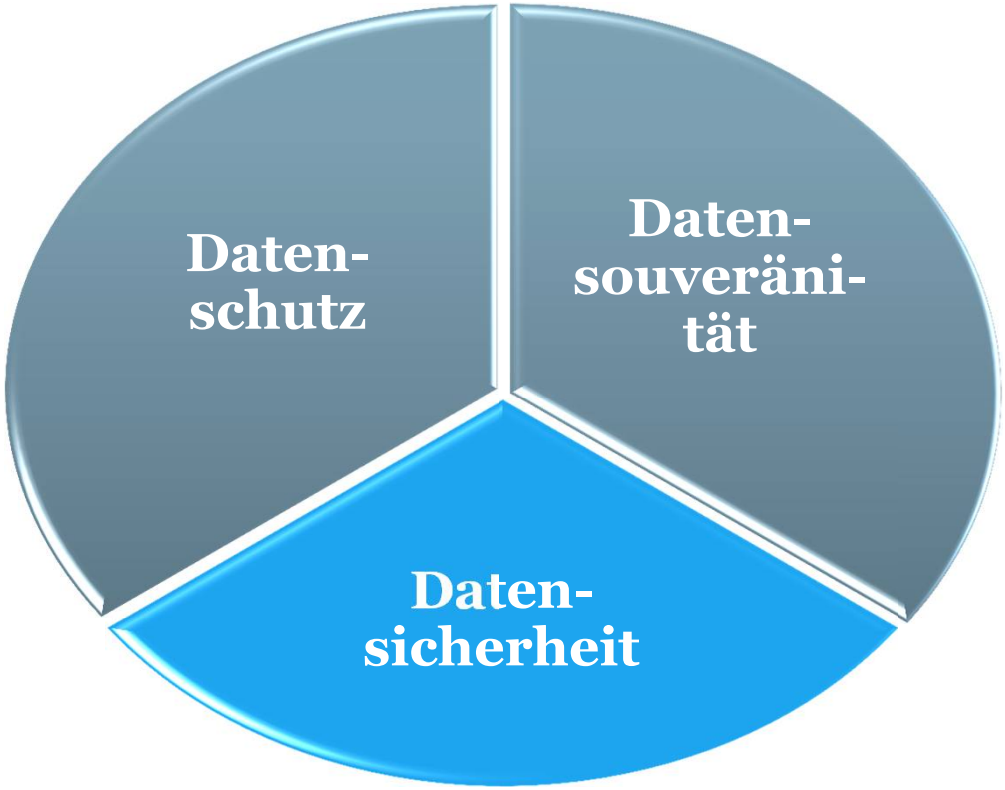
Anonymisiert oder Pseudonymisiert?

Big Data – normative Kraft des Faktischen?

- Anonymisierung
  - Personenbezug irreversibel entfernt
  - Risiko der De-Anonymisierung
  - Technologisch: Randomisieren (z.B. Zusatzgeräusche, Verfremdung, etc.) oder Generalisierung (z.B. Aggregation und K-Anonymität, L-Diversität/T-Nähe)
  - WP 29 Opinion zur Anonymisierung (10. April 2014)
- Pseudonymisierung (Art. 4 para. 5 GDPR)
  - Maßnahme der Risikominderung
  - DSGVO setzt Anreize
  - Enger Zusammenhang mit Verschlüsselung (Art. 6 Abs. 4 DSGVO)

Konkretisierung: Regulierer

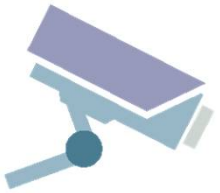
Drei Felder der Betrachtung



Bird & Bird

Frühwarnsysteme und Überwachungs-pflichten – Haftung von Vorstand und Aufsichtsrat

Sicherheit ist Vorstandsthema



Vorstands- und GF-Haftung (§91 Abs. 2 AktG)

- *"Vorstand hat .. insbesondere ein Überwachungssystem einzurichten, damit den Fortbestand der Gesellschaft gefährdende Entwicklungen früh erkannt werden."*
- **Frühwarnsysteme und Cyber-Resilienz unmittelbar verknüpft!**
- Verstöße begründen Organhaftung

Überwachungspflicht des Aufsichtsrats (§ 107 Abs. 3 AktG)

- Überwachung der Überwachungs- und Kontrollsysteme
- Persönliche Sorgfaltspflichten (§ 116 AktG)
- Schadensersatzpflichten

Cybersicherheit ➡ Spitze der Unternehmensführung

Bird & Bird

IT Sicherheitsgesetz und NIS-Richtlinie – praktische Handhabe für Unternehmen im Verteidigungssektor

IT SiG (2015) – Leitbild für die NIS RiLi

- Stärkung der IT Sicherheit und Verhinderung von Ausfällen kritischer Infrastrukturen
- Normadressaten: KRITIS-Betreiber
- Nähere Ausführung in mehreren Rechtsverordnungen (RVO)
  - RVO **03. Mai 2016:** erste Schritte zur Spezifizierung der KRITIS
  - RVO **30. Juni 2017:** Katalog klar definierter KRITIS, z. B.

eine Stelle im Sinne des § 2 Nummer 11 des Messstellenbetriebsgesetzes in der jeweils geltenden Fassung.

j) Gasförderanlage

eine Anlage zur Förderung von Erdgas aus einer Bohrung.

k) Gasspeicher

ein Gasspeicher im Sinne des § 3 Nummer 31 des Energiewirtschaftsgesetzes in der jeweils geltenden Fassung.

l) Fernleitungsnetz

ein Netz im Sinne des § 3 Nummer 19 des Energiewirtschaftsgesetzes in der jeweils geltenden Fassung.

m) Gasverteilernetz

ein Verteilernetz im Sinne des § 3 Nummer 37 des Energiewirtschaftsgesetzes in der jeweils geltenden Fas-

eine Anlage oder ein System zur Verbindung voneinander unabhängiger Tankstellen mittels zentraler Komponenten. Eine zentrale Komponente dient der zentralen Versorgung der Tankstellen eines Tankstellennetzes mit Kraftstoff.

u) Heizwerk

eine Anlage zur Erzeugung von Wärme zur Belieferung von Endkunden im Sinne der Verordnung über Allgemeine Bedingungen für die Versorgung mit Fernwärme in der jeweils geltenden Fassung.

v) Heizkraftwerk

eine Anlage zur Erzeugung von elektrischer Energie und Nutzwärme nach § 2 Nummer 14 des Kraft-Wärme-Kopplungsgesetzes in der jeweils gel-

Bird & Bird

Wer ist KRITIS Betreiber?

Branchenbezogene Kategorien

- Wasser- und Trinkwasser-Versorger
- Energieversorger, -Lieferant, -Netzwerkbetreiber für
  - Strom
  - Öl
  - Gas
- Gesundheitssektor
- Betreiber von Digitalen Infrastrukturen oder Digital Diensten (DDL)
- Banken und Finanzdienstleister (teilweise)
- Transport
  - Luftverkehr
  - Schiffahrt
  - Bahn

Bird & Bird

Übergreifende Ziele der NIS-Richtlinie

- Mitgliedstaaten (MS) setzen nationale NIS Strategie um
- Koordination zwischen den MS
- CSIRTs-Netzwerk in allen MS (= Computer Security Incident Response Team)
- Zusammenarbeit zwischen privatem und öffentlichem Sektor
- Mindestanforderungen an Cyber-Sicherheit
- Meldepflichten für KRITIS Betreiber und Betreiber von Digitaldiensten
- MS bestimmen nationale Behörden, die als (ausschließliche) Anlaufstelle und für das CSIRT zuständig sind ➡ Rolle des BSI weiter gestärkt

  Relevanz für Verteidigungssektor?

Bird & Bird

Digitale Dienstleister (DDL)

- DDL klar definiert: Betreiber von Online Marktplätzen, Online Suchmaschinenbetreiber und Cloud-Dienstleister
- Relevant für ca. 500-1.500 Cloud-Betreiber in D
- MS müssen keine Liste vorhalten
- DDL müssen gewichtige Vorfälle der zuständigen Behörde / dem BSI melden
- Ort der Hauptniederlassung maßgeblich
- Benannter Vertreter für DDL, die von außerhalb EU Markt bedienen
- BSI als Kontrollinstanz bzgl. Einhaltung

Anwendbar auf Cloud-basierte Cyber-Sicherheitsdienste

Bird & Bird

Betriebs- und Geschäftsgeheimnisse in der Digitalisierung

Fragmentierte Rechtslandschaft (1)

Gesetz gegen den Unlauteren Wettbewerb (§ 17 UWG)

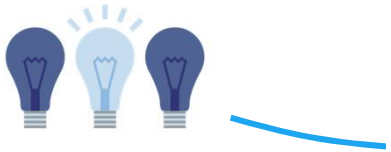
- Schützt Betriebs- und Geschäftsgeheimnissen
- Gegen unberechtigten Zugriff und Weitergabe
- Einstweiliger Rechtsschutz
- Zivilrechtliche Haftung und Straftatbestände

Trade Secrets Richtlinie (EU 2016/943) – Umsetzung in Vorbereitung

- Schutzgegenstand: Informationen von wirtschaftlichem Wert, weil geheim
- Geheimnisträger muss gebotene Maßnahmen zur Geheimhaltung getroffen haben
- Zivilrechtliche Ansprüche gegen unberechtigtes Offenbaren etc.
- Straftatbestände (3-5 Jahre max.) inkl. bei Begehung aus dem Ausland

Bird & Bird

Fragmentierte Rechtslandschaft (2)



Nutzen von Vertraulichkeitsvereinbarungen (NDA)?

- Vertragsinstrument zum Schutz vertraulicher Informationen
- Gängige Vertragsstandards
- Typische Ausnahmen (unabhängig bekannte Informationen, etc.)
- Rechtsdurchsetzung
  - Vertragsstrafen
  - Gerichtliche Durchsetzung

Technischer Schutz von Geschäftsgeheimnissen

- Verschlüsselung und andere technische Maßnahmen
- Konflikte mit Ausfuhrkontrollrecht
- Industrial Data Space könnte helfen

Geheimnisschutz der Metadaten!

Bird & Bird

Sicherheitsüberprüfungsgesetz (SÜG) und Geheimschutzhandbuch

Überprüfung von Personen mit sicherheitsempfindlicher Tätigkeit

- Vertraulichkeitsstufen STRENG GEHEIM, GEHEIM, VS-VERTRAULICH, VS-NUR FD DIENSTGEBRAUCH
- Relevant für "verteidigungswichtige Einrichtungen"
- Bedarf grds. Zustimmung der betroffenen Person
- Modifizierte Auskunftsrechte der betroffenen Person
- Ggf. auch Meldepflichten und Reisebeschränkungen

Sicherheitsüberprüfung auch für nicht-öffentliche Stellen

- Breite Relevanz für IT Lieferanten
- Strafvorschriften für Datenmissbrauch etc. (§3)

Geheimschutzhandbuch (BMWi 2004) – zentral für den Geheimschutz

- BMWi mit zentraler Zuständigkeit für Unternehmen
- Legt Maßnahmen fest, informiert über spezifische Risikolagen etc.
- Geheimschutz obliegt Unternehmen; zentrale Rolle des Sicherheitsbevollmächtigen

Bird & Bird

Sicherheitspannen – Anforderungen und praktische Erfahrungen

Sicherheitspannen – die Zeit läuft (Art. 33 DGSVO)

Risikobasierter Ansatz (Art. 33 DSGVO)

- (-) wenn kein Risiko Betroffene (= Beweislastumkehr)

Verantwortlicher

- **Unverzüglich und möglichst binnen 72 Stunden nach Bekanntwerden**
- Meldung an die Aufsichtsbehörde und mindestens
  - Namen / Kontaktdaten des DSB
  - Beschreibung des Datenverstoßes, wahrscheinlicher Folgen, getroffener Maßnahmen

Auftragsverarbeiter

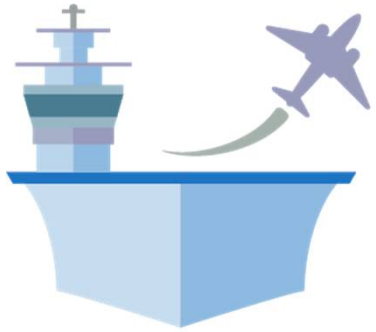
- Unverzügliche Meldung an Verantwortlichen
- Vertragliche Abreden

Benachrichtigung der Betroffenen Personen bei hohem Risiko

- Klare und verständliche Sprache
- Ausnahmeregelungen prüfen (Art. 34 Abs. 3 DSGVO)

Bird & Bird

Sicherheitspannen – nicht auf die Krise warten!



Ressourcenplanung

- Aufgabe für oberes oder Top-Management
- Handlungsplan aufsetzen
- Haftung bei Versäumnissen (2% Bußgeldrahmen)

Datenpannen feststellen

- Kategorisieren, kritische Fälle eingrenzen
- Informationsaufbereitung

Mitteilungspflichten (Behörden und Betroffene)

- Timing und Logistik
- Umfang der Information

Internationale Dimension

- "Document retention" und "litigation hold" (USA)!

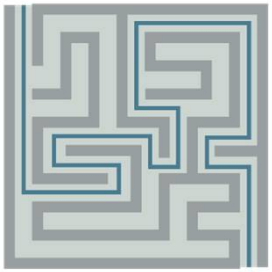
Bird & Bird

Mitteilung von IT-Störungen (ITSiG) (1)

Grundpflichten der KRITIS Betreiber

- Kontaktstelle benennen (schon zuvor)
- "Stand der Technik" umsetzen
  - Unternehmen im Bereich IT, TK, Energie, Wasser und Ernährung haben / hatten 2 Jahre Zeit ab Veröffentlichung RVO (3. Mai 2016), ihre IT nach Stand der Technik abzusichern
- Nachweis gegenüber BSI alle 2 Jahre (§ 8a Abs. 3 BSIG)

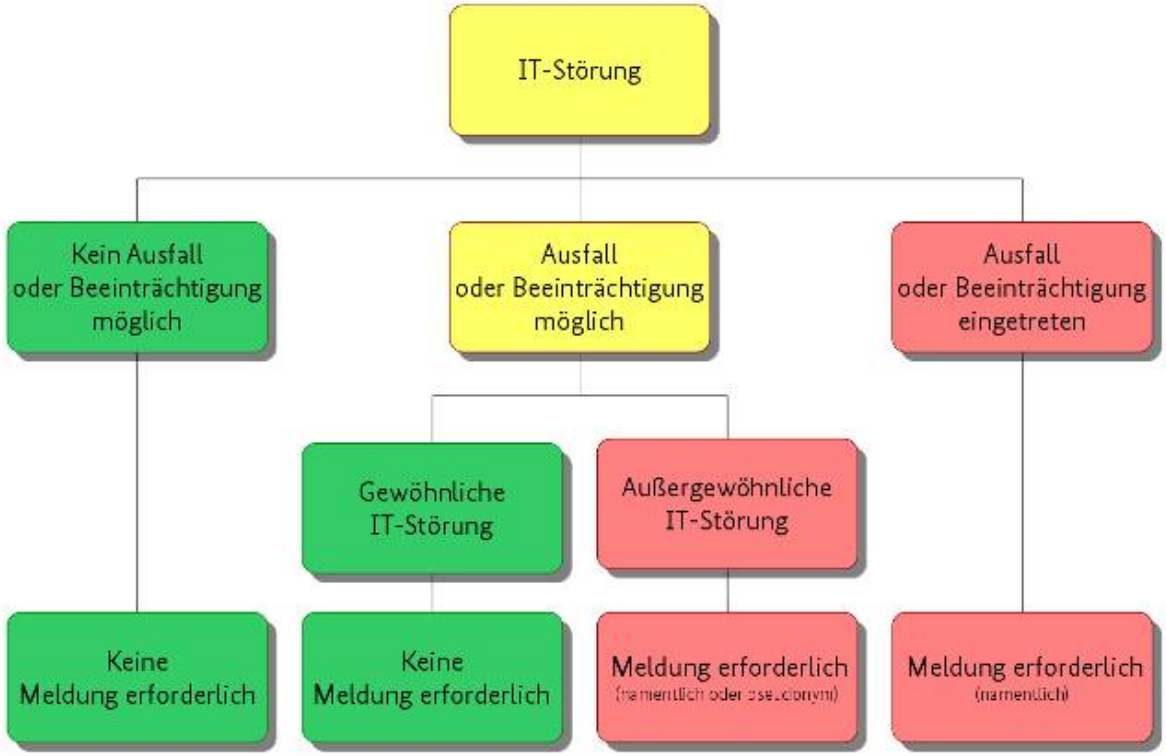
Mitteilung von IT Störungen



- Meldeformulare, Anleitung zur Mitteilung von Störungen schickt BSI (per Post) bei Benennung der Kontaktstelle
- Etablierte und vertrauenswürdige Meldekanäle
- Feststellung meldewürdiger Störung – 3 Fälle
  - Prüfdiagramm des BDSI

Bird & Bird

Mitteilung von IT-Störungen (ITSiG) (2)



Ausfall vs. Beeinträchtigung?

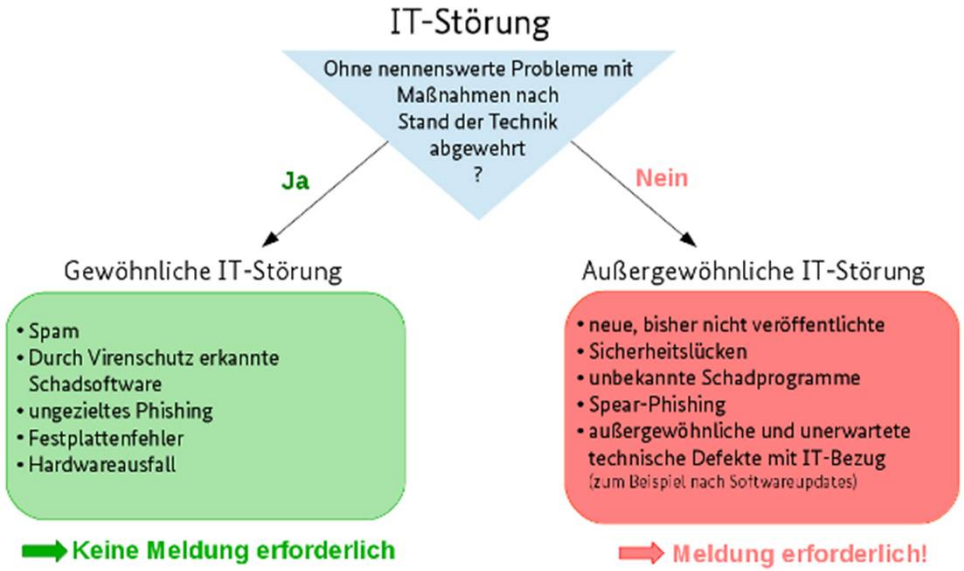
- Ausfall: Banküberweisung dauert 3 Tage, etc.
- Beeinträchtigung: Kraftwerk liefert 210 MW statt 420 MW, etc.
- Grundsätzlich: weiter Anwendungsbereich
- Im Zweifel: Meldepflicht

Abbildungsquelle: *Bundesamt für Sicherheit in der Informationstechnik*

Bird & Bird

Mitteilung von IT-Störungen (ITSiG) (4)

Gewöhnliche oder außergewöhnliche Störung?



Wenn außergewöhnlich: Fakultative Meldung an Allianz für Cyber-Sicherheit

Abbildungsquelle: *Bundesamt für Sicherheit in der Informationstechnik*

Bird & Bird

Fazit

Fazit

- Sicherheit – Haftungsfrage des Management
- DSGVO – Krisenplan und Meldepflichten
- IT SiG und NIS RiLi erheblich
- Handlungsbedarfe sind jetzt

Sicherheit und rechtliche Beratung eng verbunden!

Bird & Bird

Über Bird & Bird

- Eine der führenden internationalen Kanzleien
- 28 Büros und über 1.200 Anwält weltweit
- Herausragend in Tech & Comms
- Internationale Zusammenarbeit mit hochspezialisierten Tech-Kanzleien in Europa, Türkei, Naher Osten, Asien und USA

Aarhus, Abu Dhabi, Beijing, Bratislava, Brussels, Budapest, Copenhagen, Dubai, Duesseldorf, Frankfurt, The Hague, Hamburg, Helsinki, Hong Kong, London, Luxembourg, Lyon, Madrid, Milan, Munich, Paris, Prague, Rome, Shanghai, Singapore, Stockholm, Sydney und Warsaw

Leaders in what's new

"Well-staffed and dedicated team providing a broad range of services across IT, media and telecommunications. Experienced in handling cross-border mandates and advising clients from the financial services and life sciences sectors. Also represents clients in contentious matters."

Chambers Europe 2017

Bird & Bird

" Alexander Duisberg ist "ein scharf-sinniger, reaktiver und effizienter Praktiker", der für seine Fähigkeiten in IT-Outsourcing-Projekten gelobt wird."

Who's Who Legal 2017

" Er bearbeitet sowohl strittige als auch nicht strittige Angelegenheiten; er ist bekannt für seine fundierte Branchen-erfahrung und sein Wissen über digitale Transformationen."

Who's Who Legal 2018

"Absoluter Experte"

JUVE 2017

Vielen Dank!

Dr. Alexander Duisberg

alexander.duisberg@twobirds.com

twobirds.com