IT-Sicherheitsrisiken: Haftung und Versicherung

Dr. Axel Frhr. v. d. Bussche, LL.M. (LSE)
Rechtsanwalt, Fachanwalt für Informationstechnologierecht
Taylor Wessing

Hackerangriff auf Belgiens Außenministerium

Hacker haben Server des belgischen Außenministeriums infiltriert. Sie sollen es dabei auf Material im Zusammenhang mit der Ukraine-Krise abgesehen haben.

10.05.2014 – http://www.heise.de/newsticker/meldung/Hackerangri...

Cyberspionage: USA klagen chinesische Militärhacker an

Nach Jahren der Beschwerden gehen die USA erstmals ernsthaft gegen mutmaßliche Internetangriffe aus China vor: Das Justizministerium klagt fünf Mitglieder der Volksbefreiungsarmee mit dem Vorwurf der Cyberspionage an.

19.05.2014 – http://www.heise.de/newsticker/meldung/Cyberspiona...

145 Millionen Kunden von eBay-Hack betroffen

ebay

WICHTIG

Unbekannte haben einen großen Teil der Kundendatenbank der Online-Handelsplattform kopiert. Während der Druck auf eBay steigt, gibt es erste Hinweise, dass die gestohlenen Daten schon missbraucht werden.

22.05.2014 – http://www.heise.de/security/meldung/145-Millionen...

AVM-Routerleck: Telekom warnt über 12.000 Fritzbox-Nutzer

Eine signierte Mail soll jene Kunden wachrütteln, die ihre Fritzbox noch immer in einer besonders fatalen Konfiguration betreiben: mit veralteter Firmware und aktivem Fernzugriff.

29.04.2014 – http://www.heise.de/security/meldung/AVM-Routerlec...

SSL-GAU Heartbleed: Verhaftung nach Hack der kanadischen Steuerbehörde

In Zusammenhang mit dem Hack der kanadischen Steuerbehörde wurde der 19-jährige Stephen A. S. verhaftet. Ihm drohen 20 Jahre Haft.

17.04.2014 – http://www.heise.de/security/meldung/SSL-GAU-Heart...

Agenda

01 > IT-Compliance als Rechtsbegriff

02 > IT-Compliance als unternehmerische Pflicht

03 > Mögliche Rechtsfolgen / Haftung

04 > Einrichtung einer Compliance Organisation

05 > Einrichtung eines IT-Risikomanagementsystems

06 > Management des Cyber-Ernstfalls

07 > Risikotransfer durch Versicherungsschutz

08 > Versicherungsumfang (Beispiel)

01 > IT-Compliance als Rechtsbegriff

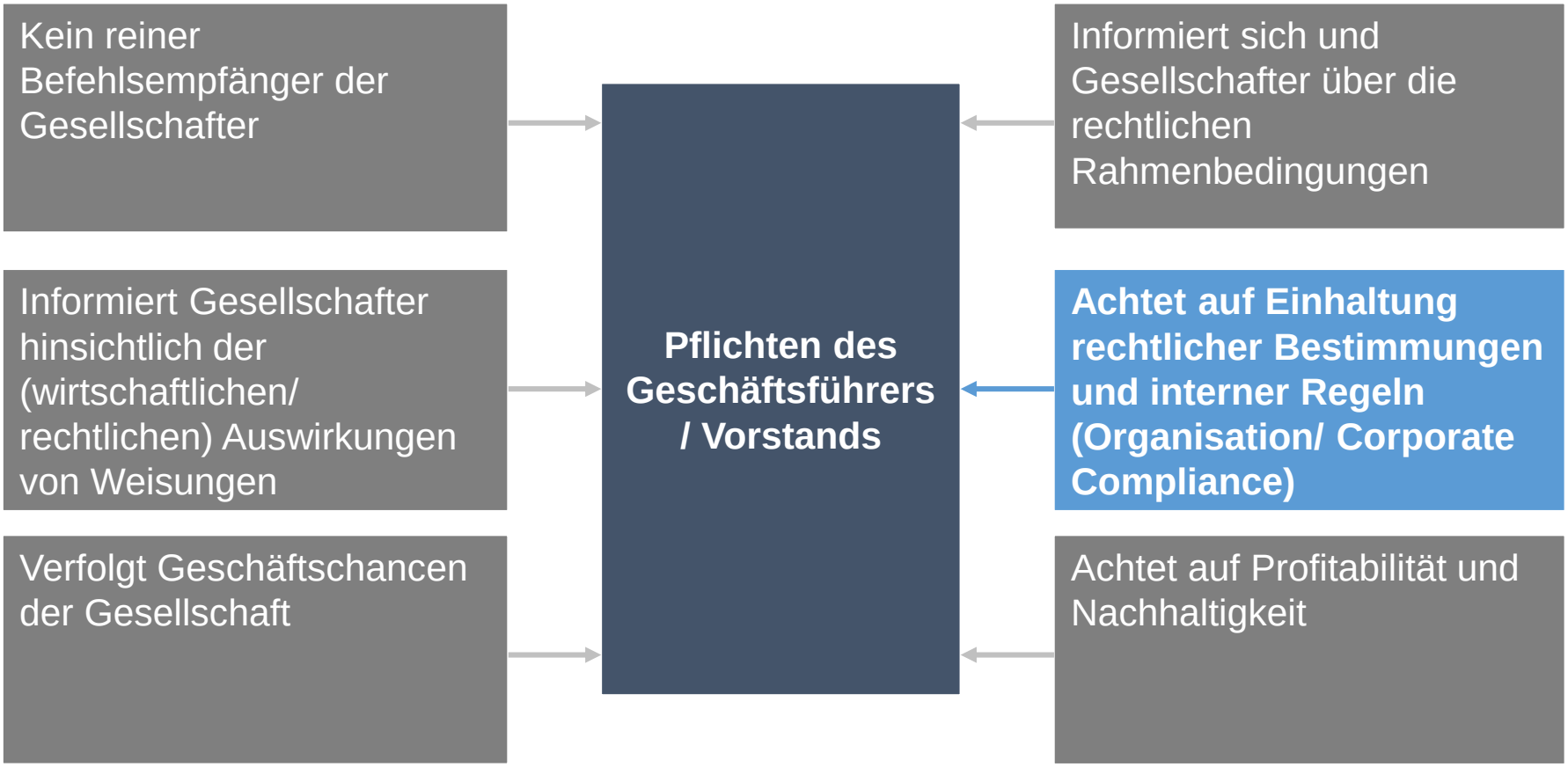
- **Definition "IT-Compliance":**
  "Einhaltung bestimmter Sicherheitsstandards, die die Verfügbarkeit, Unversehrtheit oder Vertraulichkeit von Informationen betreffen, durch Sicherheitsvorkehrungen
  1. in informationstechnischen Systemen, Komponenten oder Prozessen oder
  2. bei der Anwendung von informationstechnischen Systemen, Komponenten oder Prozessen." **(§ 2 Abs. 2 Gesetz über das Bundesamt für Sicherheit in der Informationstechnik)**

IT-Security	Datenschutz
Verfügbarkeit:	Schutz des Zugang zu Daten / IT-Systemen,
Unversehrtheit:	Schutz vor inhaltlicher Manipulation,
Vertraulichkeit:	Schutz vor unbefugter Kenntnisnahme,
Zurechenbarkeit:	Schutz vor gefälschter Identität / Herkunft,
Informationelle Selbstbestimmung:	Schutz von personenbezogenen Daten,
Qualitätsprüfung:	regelm. Überprüfung der sachgerechten Umsetzung der Sicherheitsmaßnahmen.

> IT-Compliance bedeutet Risikovermeidung

© Dr. Axel Frhr. v. d. Bussche

- **Corporate Compliance im System der Managementpflichten**



© Dr. Axel Frhr. v. d. Bussche

02 > IT-Compliance als unternehmerische Pflicht

Gesellschaftsrecht § 91 Abs. 2 AktG Analog für Geschäftsführer der GmbH	> "Der Vorstand hat geeignete Maßnahmen zu treffen, insbesondere ein Überwachungssystem einzurichten, damit den Fortbestand der Gesellschaft gefährdende Entwicklungen früh erkannt werden." > IT Compliance als Bestandteil des Risikomanagements
Handelsrecht §§ 239 Abs. 4 S. 2, 261 HGB	> Jeder Kaufmann hat bei der Führung seiner Handelsbücher und der Aufbewahrung seiner Unterlagen in elektronischer Form die Sicherung der IT-Systeme zu gewährleisten.
Bürgerliches Recht	> Deliktsrecht: Organisationsverschulden bei unzureichender IT-Sicherheit > Vertragsrecht: Pflicht zur IT-Compliance kann sich vertraglich ergeben
Datenschutz Verpflichtung zur Sicherung der IT-Systeme	> § 9 BDSG „Acht Gebote der Datensicherheit“ > § 109 TKG, § 13 Abs. 4 TMG > § 78a SGB X > Insb. Umgang mit Kunden- und Angestelltendaten

© Dr. Axel Frhr. v. d. Bussche

- 25.07.2015: **IT-Sicherheitsgesetz** tritt in Kraft als Teil der **"Digitalen Agenda"**: = Maßnahmenbündel der Bundesregierung zur Gewährleistung der „Cyber-Sicherheit“

IT- Sicherheitsgesetz

Ziel	Inhalt
Verbesserung der Sicherheit informations-technischer Systeme in Deutschland durch:	- Mindestanforderungen an sog. "Kritische Infrastrukturen" (Energie, IT, Telekommunikation, Banken, Versicherungen, Verkehr etc.): *"angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme"* - Stärkung der Stellung von BSI und BKA - Berichts- und Meldepflichten (Cyber-Angriffe) gegenüber BSI

IT- Sicherheitsgesetz

Kritik: bestehende Unsicherheit, welche Unternehmen letztlich in der zu erlassenden Rechtsverordnung als "Betreiber kritischer Infrastrukturen" klassifiziert werden

Kritik: häufige Verwendung unbestimmter Rechtsbegriffe, z.B. "angemessene Maßnahmen", "erhebliche Störung" etc.

Kritik insbesondere von Datenschützern:

Gesetz verpflichtet Unternehmen zu umfassenden Datenspeicherungen, ohne konkrete Vorgaben zum datenschutzkonformen Umgang mit personenbezogenen Daten zu treffen

(z.B. Berechtigung von Telekommunikationsdiensteanbietern, Bestands- und Verkehrsdaten von Teilnehmern und Nutzern zu erheben und zu verwenden, um Störungen an Telekommunikationsanlagen zu erkennen oder zu beseitigen)

03 > Mögliche Rechtsfolgen bei Verstößen / Haftung

Ordnungswidrigkeit § 130 Abs. 1 i.V.m. § 30 OWiG	**> Haftung der Geschäftsleitung** für vorsätzliches oder fahrlässiges Unterlassen der Aufsichtsmaßnahmen, die erforderlich sind, um Zuwiderhandlungen gegen Pflichten zu verhindern, die die Geschäftsleitung treffen und deren Verletzung mit Strafe oder Geldbuße bedroht ist. **> Haftung des Unternehmens** für Ordnungswidrigkeit, § 30 OWiG **> Geldstrafe bis 10 Million €**
Schadensersatz-ansprüche	> Gegenüber Unternehmen (z. B. Siemens Finanzvorstand) > Gegenüber Geschäftsleitung > Gegenüber zuständigen Mitarbeitern (z.B. Leiter IT, IT-Sicherheitsbeauftragter)
Sonstige mögliche Folgen	> **Imageverlust; Vertrauensverlust bei Kunden** > Verweigerung des Bestätigungsvermerks durch Wirtschaftsprüfer > Ratingprobleme (Basel II) > Verlust des Versicherungsschutzes > Abmahnung wegen Wettbewerbsverstoß > Informationspflicht bei besonderen Daten nach § 42a BDSG > Bußgeld durch die Aufsichtsbehörden bei Datenlecks

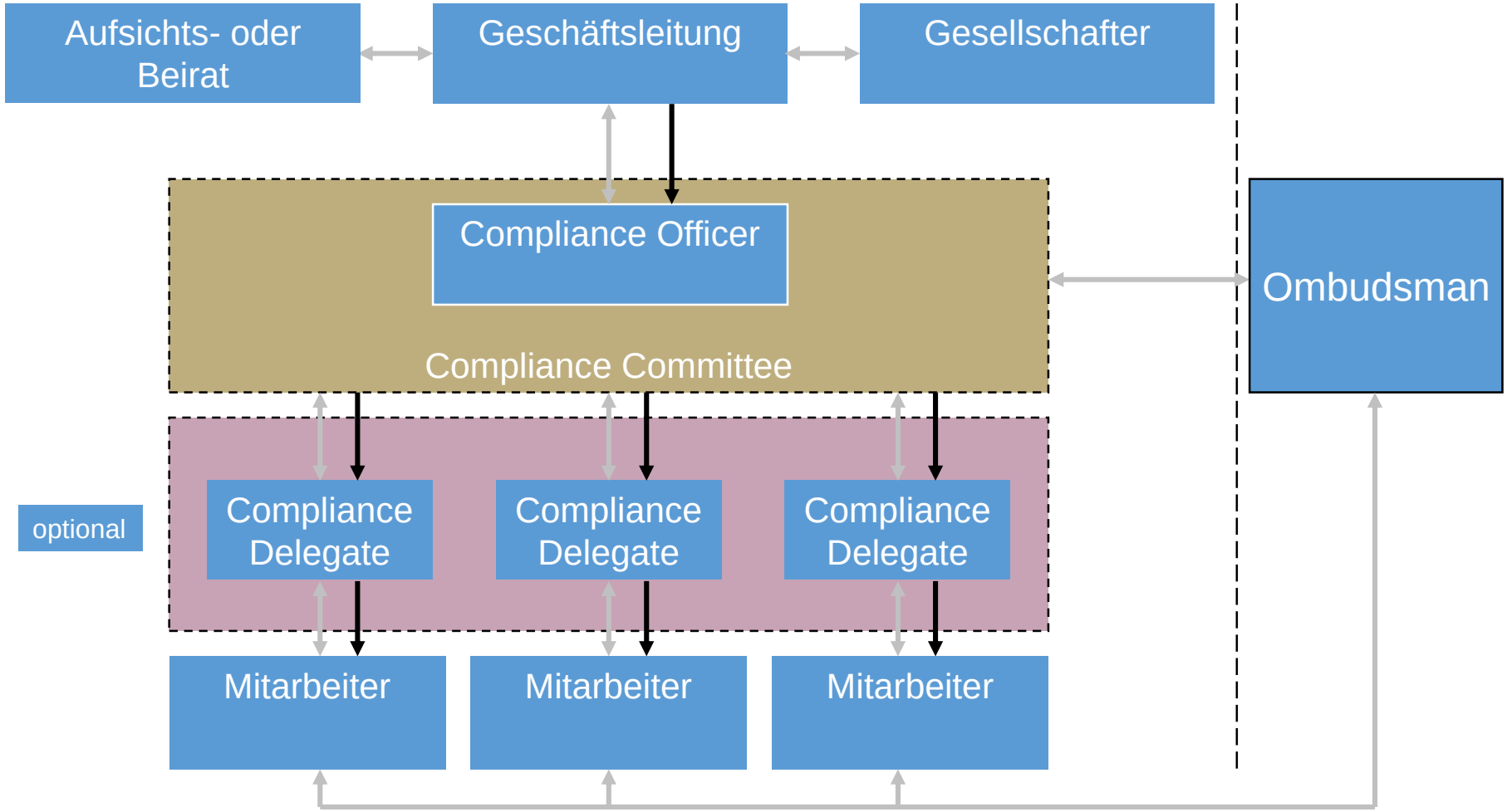
© Dr. Axel Frhr. v. d. Bussche

2 Mose 18, 22-23 in der Fassung der Einheitsübersetzung:

Ex 18,22	[Sie sollen dem Volk jederzeit als Richter zur Verfügung stehen. Alle wichtigen Fälle sollen sie vor dich bringen, die leichteren sollen sie selber entscheiden.] Entlaste dich und lass auch andere Verantwortung tragen!
Ex 18,23	Wenn du das tust, [sofern Gott zustimmt,] bleibst du der Aufgabe gewachsen und die Leute hier können alle zufrieden heimgehen.

© Dr. Axel Frhr. v. d. Bussche

04 > Einrichtung einer Compliance Organisation



© Dr. Axel Frhr. v. d. Bussche

05 > Einrichtung eines IT-Risikomanagementsystems

Bestandsaufnahme

> Wo wird IT eingesetzt?
> Welche IT wird eingesetzt?
> Risikoanalyse
> Bestehender Versicherungsschutz

Risikomanagementsystem

> Festlegung der zu ergreifenden Sicherheitsmaßnahmen
> Berücksichtigung der wichtigen operativen Risiken
> Technische Maßnahmen
> Organisatorische Maßnahmen
> Berücksichtigung IT-immanenter rechtlicher Risiken
  – Lizenzmanagement
  – Datenschutz
  – Outsourcing

> Sorgfalts- und Leistungsnachweis, somit Reduzierung des Haftungsrisikos durch ISO 27001 – Zertifizierung möglich

© Dr. Axel Frhr. v. d. Bussche

- **Ablaufplan mit Zuständigkeiten**

  - Eingriff erkennen
  - Data Breach Coach des Versicherers (z.B. ACE, Hiscox) einschalten
  - Schadenfall dem Versicherer anzeigen
  - Eingriff beenden (Schadensbegrenzung/-beseitigung, vgl. § 42a BDSG)
  - Sachverhalt erfassen
  - Maßnahmenplan erstellen
  - Incident Response Team einsetzen
  - Maßnahmenplan abarbeiten
  - neue Risikobewertung / Präventionsmaßnahmen verbessern

© Dr. Axel Frhr. v. d. Bussche

- D&O-Versicherungsschutz
- Eigen- und Drittschäden über Cyber-Police:
  - noch kein Standardprodukt am deutschen Markt!
  - Anbieter sind insb. ACE, Allianz, AXA, CHUBB, HDI, Hiscox, Zurich

© Dr. Axel Frhr. v. d. Bussche

08 > Versicherungsumfang (Beispiel)

Baustein A: Versicherte Gefahren, die zu Eigenschäden führen

- Verlust, Zerstörung oder Beschädigung von Daten und Programmen durch Verlust, Zerstörung oder Beschädigung der Hardware
- Nachteilige Veränderung oder Verlust von Daten/Programmen durch:
  - Mut- oder böswillige Handlungen durch AN oder Dritte (Malicious Act)
  - Programme oder Programmteile mit Schadfunktion (Malicious Codes), insb. Computerviren und -würmer, Trojaner, Logische Bomben, Denial of Service (DoS) durch gezielte Überlastung des Infrastruktursystems
  - Menschliches Versagen / Fehlbedienung
  - Ausfall oder Störung der Hardware
  - Überspannung, Spannungsabfall
  - Diebstahl / Verlust oder unzulässige Veröffentlichung von Daten

© Dr. Axel Frhr. v. d. Bussche

08 > Versicherungsumfang (Beispiel)

Baustein A: Versicherte Schäden = Eigenschäden

- Software- und Datenwiederherstellung
- Mehrkosten / Beschleunigungskosten (erhöhte Betriebskosten)
- Betriebsunterbrechungskosten (optional)
- Ausfallkosten externe Dienstleister (Cloud: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Software as a Service (SaaS))
- Kosten für Sachverständige, Berater (Forensik), Rechtsanwälte, WP
- Kosten für erhöhten Werbeaufwand
- Kosten für Regress beim Schädiger (soweit identifiziert)
- Leistungen bei erpresserischer Bedrohung (optional)
- Vertragsstrafen (optional)

© Dr. Axel Frhr. v. d. Bussche

08 > Versicherungsumfang (Beispiel)

Baustein B: Versicherte Gefahren, die Haftpflicht auslösen

- Beleidigung / Verleumdung / üble Nachrede
- Diebstahl geistigen Eigentums
- Verletzung von Datenschutz und Vertraulichkeit
- Unbefugte Nutzung eines fremden Computersystems oder unbeabsichtigte Übertragung eines Computervirus auf das System eines Dritten

© Dr. Axel Frhr. v. d. Bussche

08 > Versicherungsumfang (Beispiel)

Baustein B: Versicherte Schäden = 1. Fremdschäden

Freistellung wegen begründeter privatrechtlicher Haftung gegenüber Dritten aus:

- Datenschutzrecht, §§ 7, 8 BDSG
- Vertrag
- unerlaubter Handlung
- Urheberrecht

bzw. Abwehr unbegründeter Haftpflichtansprüche Dritter

© Dr. Axel Frhr. v. d. Bussche

08 > Versicherungsumfang (Beispiel)

Baustein B: Versicherte Schäden = 2. Krisenmanagement

- Benachrichtigungskosten (Benachrichtigung der Kunden, Einrichtung Call Center, Multimediaverbreitung, Anzeige an Datenschutzbehörde)
  - § 42a BDSG: bei bestimmten personenbezogenen Daten
  - § 109a TKG: bei Telekommunikationsdienstleistern
- Kosten für Nachforschungen (Monitoring, Forensik, Berater etc.)
- Kosten für Verhandlungen mit Aufsichtsbehörden zur Vermeidung von Bußgeld, § 43 III BDSG (Rechtsanwalt, Krisenmanager etc.)
- Kosten für Presseberatung
- Kosten für Kreditüberwachungsdienste
- Kosten der Feststellung von Schadensersatzansprüchen gegen Dienstleister (Rechtsanwalt)

08 > Versicherungsumfang (Beispiel)

Häufig versicherte Zusatzleistung: Incident Response Team

- **Kostenlose Telefon-Hotline (24/7)** zum **Data Breach Coach** = Rechtsanwaltskanzlei, die in vorgegebenem Umfang kostenfrei zum Data Breach-Vorfall berät

- Beratungsumfang: unmittelbare Beratung bei der Strukturierung des Managements des Cyber-Ernstfalls und bei der Auswahl, Beauftragung und Koordinierung der erforderlichen Sachverständigen / Berater (**Incident Response Team**)

- Wahrung der Rechtsanwalts-Schweigepflicht

- Unabhängigkeit von der Schadenbearbeitung des Versicherungsfalls beim Versicherer

© Dr. Axel Frhr. v. d. Bussche

Vielen Dank für Ihre Aufmerksamkeit.

Dr. Axel Frhr. v. d. Bussche, LL.M. (L.S.E.)
Rechtsanwalt, Hamburg
Fachanwalt für Informationstechnologierecht

Kontakt
T: +49 (0) 40 36 80 30
E: a.bussche@taylorwessing.com

Taylor Wessing
Hanseatic Trade Center
Am Sandtorkai 41
20457 Hamburg

www.taylorwessing.com

Taylor Wessing
Benrather Str. 15
40213 Düsseldorf

Dr. Gunbritt Kammerer-Galahn
Rechtsanwältin, Düsseldorf
Fachanwältin für Versicherungsrecht

Kontakt
T: +49 (0) 211 83 87 0
E: g.kammerer-galahn@taylorwessing.com

© Dr. Axel Frhr. v. d. Bussche

- Veröffentlichungen zum Datenschutzrecht von Dr. Axel Frhr. von dem Bussche, LL.M. (L.S.E.)

Copyright notice
Icons used in this presentation were made by Freepik from www.flaticon.com and are licensed under CC BY 3.0

Unsere Standorte:

Beijing *
Unit 2307&08, West Tower,
Twin Towers
B-12 Jianguomenwai Avenue
Chaoyang District
Beijing 100022
T. +86 (10)6567 5886

Berlin
Ebertstraße 15
10117 Berlin
T. +49 (0)30 88 56 36 0

Bratislava
TaylorWessing e|n|w|c
Panenská 6
81103 Bratislava
T. +421(0)2 5263 2804

Brno *
TaylorWessing e|n|w|c
Dominikánské náměstí 4/5
602 00 Brno
T. +420 543 420 401

Brussels
Trône House
4 Rue du Trône
1000 Brussels
T. +32 (0)2 289 6060

Budapest
TaylorWessing e|n|w|c
Dorottya u. 1. III. em.
1051 Budapest
T. +36 (0)1 327 04 07

Cambridge
24 Hills Road
Cambridge, CB2 1JP
T. +44 (0)1223 446400

Dubai
26th Floor, Rolex Tower,
Sheikh Zayed Road,
P.O. Box 33675
Dubai, United Arab Emirates
T. +971 (0)4 309 1000

Düsseldorf
Benrather Straße 15
40213 Düsseldorf
T. +49 (0)211 83 87 0

Frankfurt
Senckenberganlage 20-22
60325 Frankfurt a.M.
T. +49 (0)69 971 30 0

Hamburg
Hanseatic Trade Center
Am Sandtorkai 41
20457 Hamburg
T. +49 (0)4 0 36 80 30

Jakarta **
Hanafia Ponggawa & Partners
Wisma 46 Kota BNI, 32nd & 41st
Floor. Jl. Jend Sudirman
Kav 1 Jakarta 10220
T. +62 21 5746 545

Kiev
TaylorWessing e|n|w|c
Illinsky Business Center
vul. Illinska 8
04070 Kiev
T. +38 (0)44 369 32 44

Klagenfurt *
TaylorWessing e|n|w|c
Alter Platz 1
9020 Klagenfurt
T. +43 (0)463 51 52 27

London
5 New Street Square
London EC4A 3TW
T. +44 (0)20 7300 7000

Munich
Isartorplatz 8
80331 Munich
T. +49 (0)89 2 10 38 0

Paris
69 avenue Franklin D. Roosevelt
75008 Paris
T. +33 (0)1 72 74 03 33

Prague
TaylorWessing e|n|w|c
U Prasné brány 1
CZ-110 00 Praha 1
T. +420 224 81 92 16

Shanghai *
Unit 1509, United Plaza
No. 1468, Nanjing West Road
Shanghai 200040
T. +86 (0)21 6247 7247

Singapore
RHTLaw Taylor Wessing LLP
Six Battery Road
#09-01, #10-01
Singapore 049909
T. +65 6381 6868

Seoul **
DR & AJU LLC
Donghoon Tower
317 Teheran-Ro
Gangnam-gu
Korea

Vienna
TaylorWessing e|n|w|c
Schwarzenbergplatz 7
1030 Vienna
T. +43 (0)1 716 55

Warsaw
TaylorWessing e|n|w|c
ul. Mokotowska 1
00-640 Warsaw
T. +48 (0)22 584 97 40

© Dr. Axel Frhr. v. d. Bussche