WILHELM
RECHTSANWÄLTE

Bankensymposium Digitalisierung & Recht, 21. Mai 2019, Bonn

Cyber-Security aus haftungsrechtlicher Sicht

RA Christian Drave, LL.M.

IHR REFERENT

Christian Drave ist spezialisiert auf Industrieversicherung und Haftung.

Im Fokus seiner Beratung und Prozessvertretung stehen Fragen internationalen Versicherungsschutzes (u.a. im Zusammenhang mit internationalen Versicherungs-programmen). Einen Schwerpunkt seiner Beratung legt er auf die Koordination von Haftpflichtansprüchen und Versicherungsschutz in (häufig grenzüberschreitenden) Produkthaftpflicht- und Rückruffällen.

Christian Drave berät, referiert und publiziert regelmäßig zu versicherungsrechtlichen Spezialfragen, insbesondere im Bereich Cyberrisiken. Er hält einen „Master of Insurance Law“ (LL.M.) und ist Fachanwalt für Transport- und Speditionsrecht sowie gelernter Schifffahrtskaufmann.

Kontakt:

+49 (0) 211.68 77 46-43

christian.drave@wilhelm-rae.de

Empfohlen im Versicherungsrecht („Professionell, lösungsorientiert und bei Verhandlungen sehr überzeugend“)

Legal 500 Deutschland 2017

AGENDA

1. Haftungsrisiko Kundenschädigung
2. Haftungsrisiko Datenverlust
3. Sorgfaltsanforderungen im Zusammenhang mit Cyberrisiken
4. Möglichkeiten der Haftungsminimierung und des Risikotransfers?
5. Cyberrisiken und Managerhaftung
6. Fazit

1. HAFTUNGSRISIKO KUNDENSCHÄDIGUNG

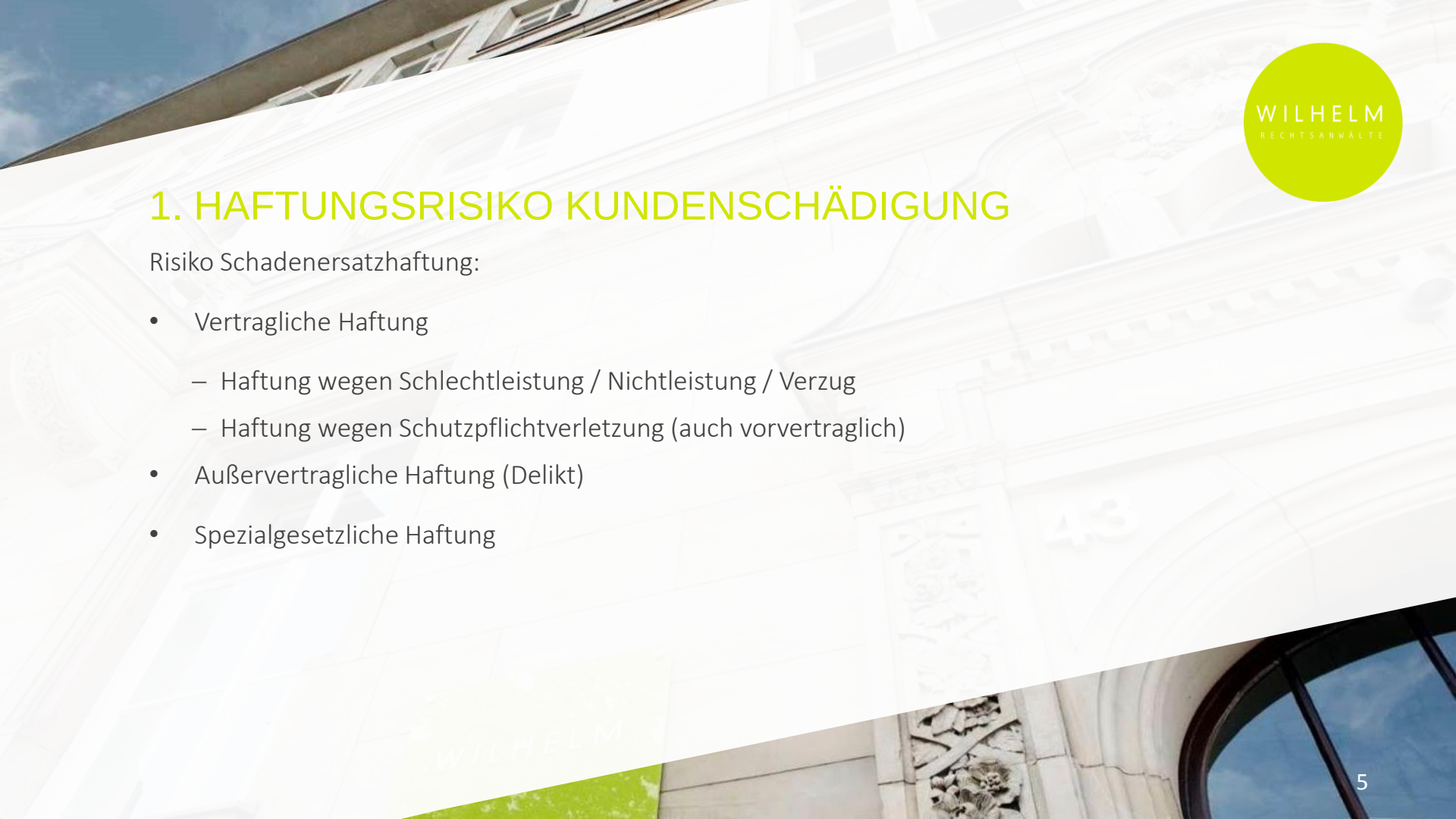
Szenario:

Durch eine Phishing-Attacke erlangen Hacker Zugriff auf Passwörter mehrerer Großkunden eines Finanzdienstleisters. Die Angreifer nutzen die Daten zur Abzweigung hoher Summen von den Konten der Kunden.

1. HAFTUNGSRISIKO KUNDENSCHÄDIGUNG

Risiko Schadenersatzhaftung:

- Vertragliche Haftung
  - Haftung wegen Schlechtleistung / Nichtleistung / Verzug
  - Haftung wegen Schutzpflichtverletzung (auch vorvertraglich)
- Außervertragliche Haftung (Delikt)
- Spezialgesetzliche Haftung



2. HAFTUNGSRISIKO DATENVERLUST

Szenario:

Eine Bank mit Privatkundengeschäft wird Opfer eines Hackerangriffs. Die Hacker erlangen zwar keinen Zugriff auf die Finanztransaktionen, aber auf die Kundendaten (u.a. Namen, Adressen, Kontostände).

Neben dem Vertrauensverlust der Kunden drohen der Bank finanzielle Konsequenzen.

ZDNet / Sicherheit / Cyberkriminalität

Großbank HSBC räumt Hacker-Angriff ein

Unbekannte greifen offenbar per Brute-Force-Angriff auf Online-Konten zu. Sie erbeuten persönliche Daten, jedoch offenbar kein Geld. HSBC verbessert als Folge die Authentifizierung für seine Online-Konten.

von Stefan Beiersmann am 7. November 2018 , 07:33 Uhr

Die Großbank HSBC meldet einen Sicherheitsvorfall. Unbekannte haben offenbar auf eine nicht näher genannte Zahl von Konten des Geldinstituts zugegriffen. Das geht aus Unterlagen hervor, die HSBC bei den zuständigen Behörden im US-

2. HAFTUNGSRISIKO DATENVERLUST

Schadenersatzansprüche bei Datenverlust?

Ausgangspunkt: EU-Datenschutz-Grundverordnung (DSGVO)

- geltendes Recht seit 25. Mai 2018
- unmittelbar und vorrangig vor nationalem Datenschutzrecht (BDSG)
- regelt ein strenges, einheitliches europäisches Datenschutzrecht
- regelt umfassende Pflichten
- schafft Risiken für Unternehmen
    - Schadenersatzansprüche Betroffener (Art. 82 DSGVO)
    - Geldbußen (Art. 83 DSGVO)

2. HAFTUNGSRISIKO DATENVERLUST

Art. 82 Abs. 1 DSGVO

„Jede Person, der wegen eines Verstoßes gegen diese Verordnung ein materieller oder immaterieller Schaden entstanden ist, hat Anspruch auf Schadenersatz gegen den Verantwortlichen oder gegen den Auftragsverarbeiter.“

Erwägungsgrund 146 DSGVO

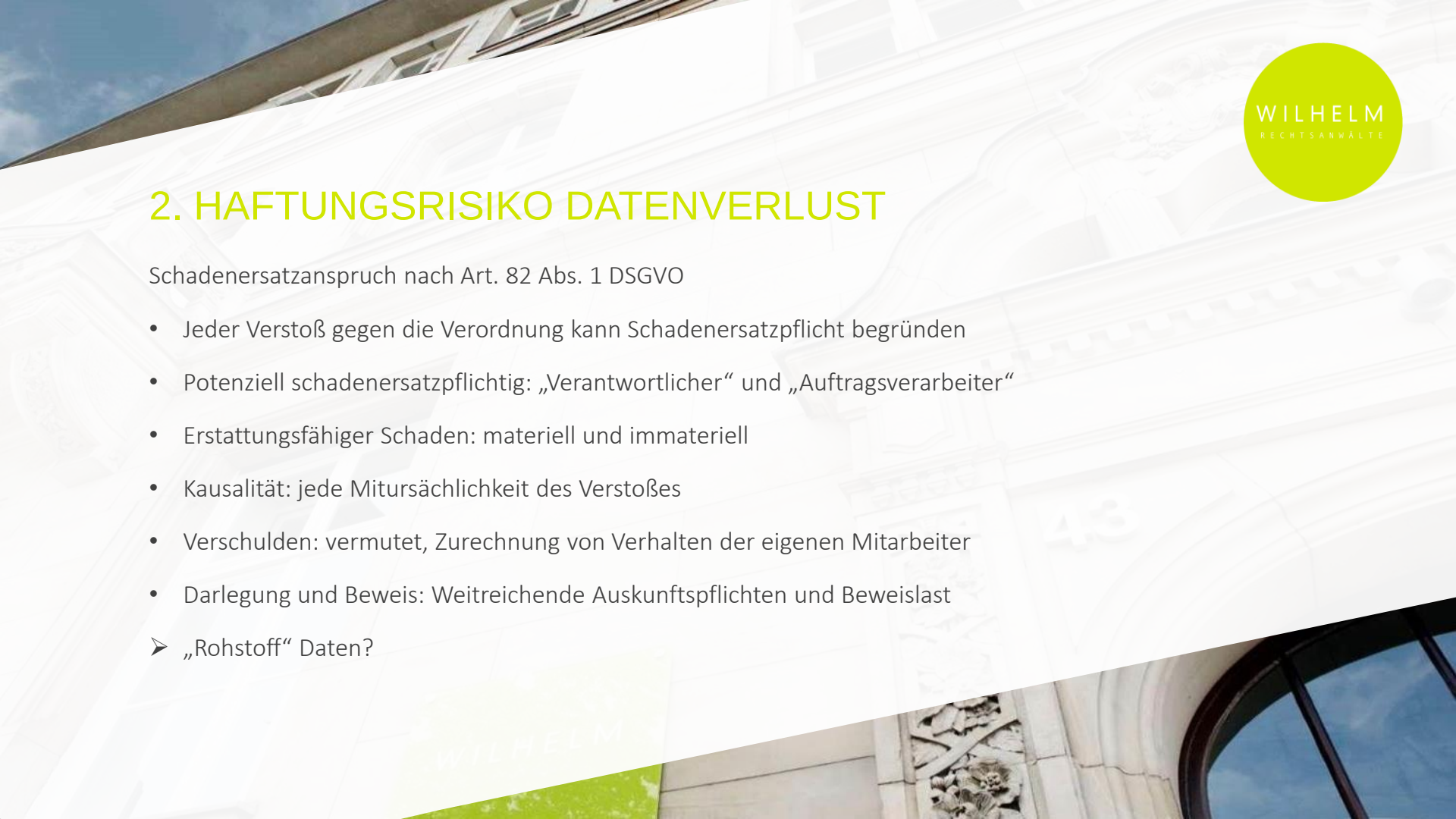
„Die betroffenen Personen sollten einen vollständigen und wirksamen Schadenersatz für den erlittenen Schaden erhalten“

2. HAFTUNGSRISIKO DATENVERLUST

Schadenersatzanspruch nach Art. 82 Abs. 1 DSGVO

- Jeder Verstoß gegen die Verordnung kann Schadenersatzpflicht begründen
- Potenziell schadenersatzpflichtig: „Verantwortlicher“ und „Auftragsverarbeiter“
- Erstattungsfähiger Schaden: materiell und immateriell
- Kausalität: jede Mitursächlichkeit des Verstoßes
- Verschulden: vermutet, Zurechnung von Verhalten der eigenen Mitarbeiter
- Darlegung und Beweis: Weitreichende Auskunftspflichten und Beweislast

➢ „Rohstoff“ Daten?



3. SORGFALTSANFORDERUNGEN

Art 32 DSGVO

"Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. (...)

3. SORGFALTSANFORDERUNGEN

- Im Einzelfall zu bestimmen
- Art. 32 DSGVO
- MaRisk, § 25a Abs. 1 S. 3 Nrn. 3 und 5 KWG
- Konkretisierung: z.B. über Bankaufsichtlichen Anforderungen an die IT (BAIT) sowie BSI-Empfehlungen oder DIN- / ISO-Standards (z.B. ISO Norm 27001)
- Konkretisierung über Aufsichtspraxis und Rechtsprechung
- Dialog mit Versicherern

4. HAFTUNGSMINIMIERUNG UND RISIKOTRANSFER

- Cyber-Risikomanagement und -Compliance
- Technische und organisatorische Cybersicherheit
- Vertragliche Regelungen
- Risikotransfer: Versicherung?
- Dokumentation

5. CYBERRISIKEN UND MANAGERHAFTUNG

- Haftungsrisiken für Unternehmensleiter
- Deckung schafft Haftung?

➢ Cyber Security als Leitungsaufgabe

6. FAZIT

- Cyberrisiken schaffen relevante Haftungsrisiken für Unternehmen und Unternehmensleiter
- Risiken und Sorgfaltsanforderungen sind individuell zu prüfen und Maßnahmen zu treffen → Risikomanagement
- Cyber Security ist Leitungsaufgabe

VIELEN DANK FÜR IHRE AUFMERKSAMKEIT

Weitere Informationen erhalten Sie auch auf unserer Website:

www.wilhelm-rae.de

Für Ihre Fragen und Anregungen stehen wir Ihnen gerne in einem persönlichen Gespräch zur Verfügung:

Wilhelm
Partnerschaft von Rechtsanwälten mbB

Düsseldorf:

Reichsstraße 43
40217 Düsseldorf

Telefon: + 49 - (0) 211.68 77 46 - 0
Telefax: + 49 - (0) 211.68 77 46 - 20

info@wilhelm-rae.de

Berlin:

Mommsenstraße 45
10629 Berlin

Telefon: + 49 - (0) 30.81 72 732 - 0
Telefax: + 49 - (0) 30.81 72 732 - 20

Sitz: Düsseldorf
AG Essen: PR 1597