Cyberrisiken – Haftungsszenarien für betroffene Unternehmen

11. Düsseldorfer Versicherungsrechtstag
12. Oktober 2018

Dr. Oliver Sieg, Rechtsanwalt, Partner

Übersicht

Noerr

Einleitung: Aktualität des Themas „Cyberangriffe“

„Uber muss wegen verschwiegener Datenlecks Rekordstrafe zahlen“

Handelsblatt vom 27.09.2018

„Attacke legt Internetseite des Energiekonzerns RWE lahm“

Zeit Online vom 25.09.2018

„Russische Top-Spione hacken offenbar Welt-Anti-Doping-Agentur“

Welt vom 15.09.2018

„Milliarden-Schaden für Firmen – Cyberangriffe werden zur alltäglichen Gefahr“

n-tv vom 13.09.2018

„Onlinekriminalität – Kliniken im Visier von Hackern“

Tagesschau vom 09.09.2018

Einleitung: Unterschiedliche Ausprägungen von Cyberangriffen

Reputationsangriff

z.B. Fake News

Datenmanipulation

Fälschung / Veränderung / Löschen

Datendiebstahl

- Geschäftsgeheimnisse (Know-how; Produkte; Prozesse)
- Personenbezogene Daten von
  - Mitarbeitern
  - Geschäftspartnern (Kunden)
  - Dritten

Missbrauch von IT-Anlagen

Betrug

z.B. Fake President

Erpressung

→ Stören von IT-Anlagen, Kommunikationswegen, Produktionsabläufen und -mitteln

Sabotage

→ Stören von IT-Anlagen, Kommunikationswegen, Produktionsabläufen und -mitteln

Spionage

→ Hauptziel
→ Vorbereitung anderer Straftaten

Noerr

/ Einleitung: Gefährdungslage durch Cyberangriffe

Wirtschaft

- **Digitalisierung** der Wirtschaft
  - Industrie 4.0; IoT; Blockchain
- Bericht zur Lage der IT-Sicherheit in Deutschland 2017 des **BSI**:
  - Anstieg der Zahl von Cyberangriffen
  - Hohes Schadenspotential im Bereich Kritischer Infrastrukturen (**KRITIS**)
- Ca. 25% aller Cyber-Schadensfälle im Finanzdienstleistungssektor – gerade hier werden laut **BaFin-Präsident Hufeld** oft keine qualitativ ausreichenden Sicherheitsmaßnahmen vorgehalten

Öffentlicher Bereich / Verwaltung

- 28.02.2018: “Hacker drangen in deutsches Regierungsnetz ein” (spiegel.de)
- Manipulation von Wahlen
- Staats-Terrorismus; Cyber War

Gesellschaft / Privatsphäre

- „Smart Home“; Smart Phones
- Vermehrte Erhebung und Verwendung personenbezogener Daten im unternehmerischen Verkehr
- Identitätsdiebstahl

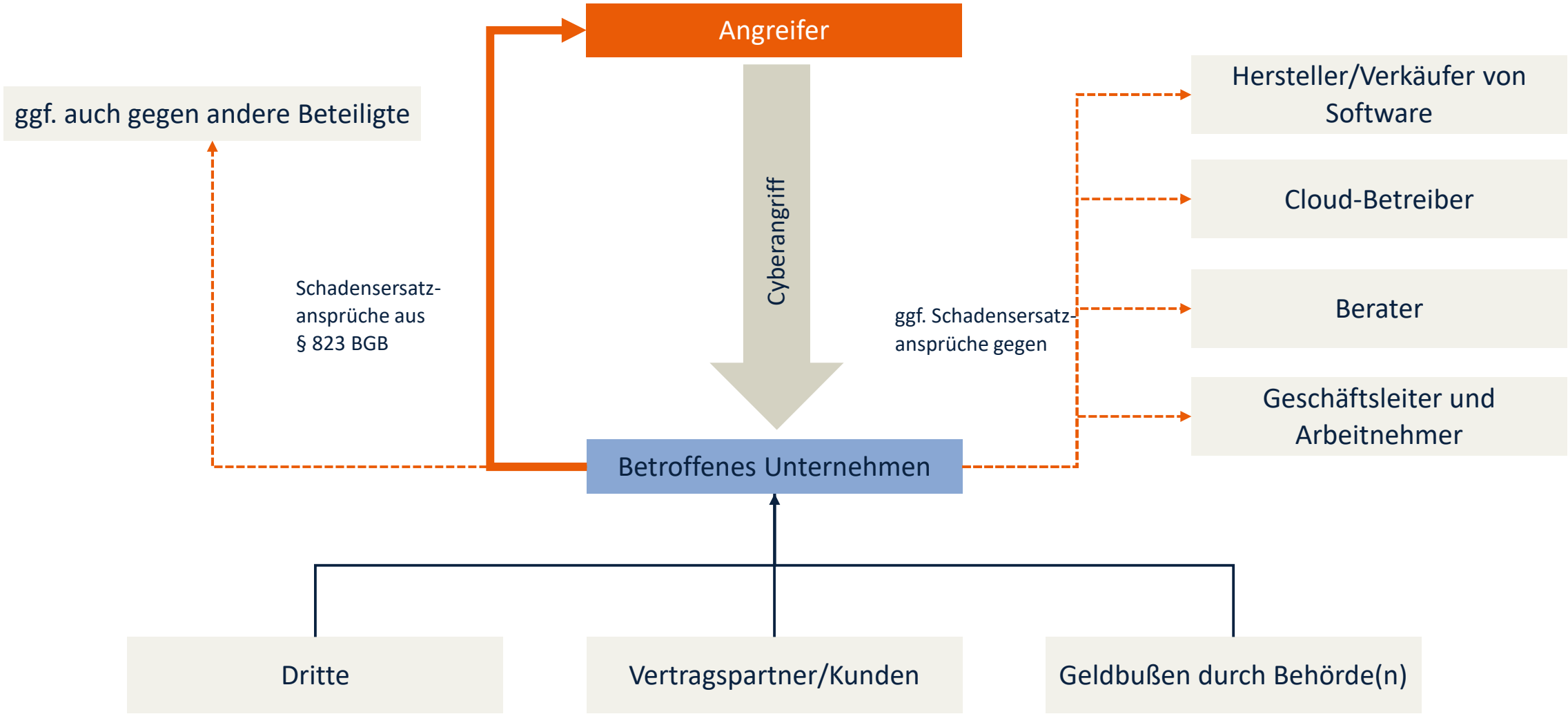
Noerr

Reaktionen auf einen Cyberangriff

- Umsetzen eines Notfallplans
- Forensische Maßnahmen (ggf. unter Hinzuziehung externer Sachverständiger)
  - Ermittlung der Ursache(n)/Verantwortlichen und der Betroffenen
  - Feststellung des Schadensumfangs
  - Auch aus anwaltlicher Perspektive
- Notfallmaßnahmen: Wiederherstellung Daten/ IT-System und Dokumentation des Schadensfalls
- Informationspflichten bei Verletzung des Schutzes personenbezogener Daten gemäß Art. 33, 34 DS-GVO
- Besondere Meldepflichten, vgl. § 8b Abs. 4 BSIG, § 109 Abs. 5 TKG, § 11 Abs. 1 lit. c) EnWG
- Ad-hoc-Publizitätspflicht bei Cyberangriffen? Art. 16 MAR
- Strafrecht und Ermittlungsverfahren – Zusammenarbeit mit Ermittlungsbehörden
- Einschaltung des Cyber-Versicherers?
- Berücksichtigung der grenzüberschreitenden Dimension

Noerr

/ Haftungsszenarien



Noerr

Ansprüche des betroffenen Unternehmens

Ansprüche gegen den Angreifer

§ 823 Abs. 1 BGB: Schutz von Leben, Körper, Gesundheit Freiheit, Eigentum

- Eigentumsverletzung nur, wenn
  - Daten auf körperlichen Gegenständen (Datenträgern, Festplatten) gespeichert sind und
  - auf die Sachsubstanz dieser Gegenstände eingewirkt (Beschädigung Zerstörung) wird
- Ggf. Eingriff in Recht am eingerichteten und ausgeübten Gewerbebetrieb (Betriebsbezogenheit)
- Umstritten: Schutz von Datenbeständen über ein „Recht am eigenen Datenbestand“ als „sonstiges Recht“ möglich und notwendig?

§ 823 Abs. 2 BGB i.V.m. Schutzgesetz

- Normen des StGB
  - § 202a StGB – Ausspähen von Daten
  - § 202b StGB – Abfangen von Daten unter Anwendung technischer Hilfsmittel
  - § 202d StGB – Datenhehlerei
  - § 303a StGB – Datenveränderung
  - § 303b StGB – Computersabotage
- § 17 Abs. 2 Nr. 1 a) UWG (unbefugtes Verschaffen/Sichern von Geschäfts- und Betriebsgeheimnissen unter Anwendung technischer Mittel zum Zwecke der Schädigung des Unternehmensinhabers)

Ansprüche nach Maßgabe ausländischen Rechts

Relevanz einstweiligen Rechtsschutzes und Zusammenarbeit mit Strafermittlungs-behörden

Realität: Herausforderungen bei der praktischen Durchsetzbarkeit

Noerr

Ansprüche des betroffenen Unternehmens

Ansprüche gegen andere Beteiligte

§ 823 Abs. 2 BGB i. V. m. § 202c StGB

- Vorbereiten des Ausspähens und Abfangens von Daten etwa durch Weitergabe interner Zugangspasswörter an Dritte

Bei Phishing Schadensersatzanspruch gegen den „Geldkurier“ aus § 823 Abs. 2 BGB i. V. m. § 261 StGB (Geldwäsche)

- So z.B. das Urteil des LG Köln vom 05.12.2007 (9 S 195/07, MMR 2008, 259)
- Nach einem Urteil des KG vom 15.10.2009 (8 U 26/09, MMR 2010, 128) handelt es sich nur bei § 261 Abs. 2 StGB um ein Schutzgesetz i. S. v. § 823 Abs. 2 BGB, nicht aber bei § 261 Abs. 1 StGB

Noerr

Ansprüche des betroffenen Unternehmens

Ansprüche gegen Softwarehersteller oder -verkäufer

Vertragliche Haftung

- Voraussetzung: Software war fehlerhaft
- Maßstab: konkrete vertragliche Ausgestaltung

Mängelgewähr-leistungsrechte

- gegen den Verkäufer nur, wenn Fehler/Sicherheitslücke bereits bei Gefahrübergang vorhanden

Umstritten: Schadensersatzanspruch gemäß §§ 280 Abs. 1, 241 Abs. 2 BGB wegen der Verletzung einer leistungsbezogenen Nebenpflicht aus § 242 BGB zur „Pflege der Produkte“, d.h. zur Sicherung des bezweckten Leistungserfolges?

- Jedenfalls nur gegen den Hersteller der Software, nicht gegen einen (personenverschiedenen) Verkäufer
- Vertragsverhältnis mit dem Softwarehersteller (Verkäufer)
  - Schadensersatzanspruch jedenfalls dann, wenn ein zusätzliches Entgelt für die Wartung entrichtet wird (LG Köln, Urteil v. 16.10.1997 – 83 O 26-97, NJW-RR 1999, 1285)
  - a. A.: Haftung nur, wenn Wartungspflicht ausdrücklich vereinbart

Deliktische Produzentenhaftung des Herstellers aus § 823 Abs. 1 BGB wegen Verletzung von Produktbeobachtungspflichten?

- Produktbeobachtungspflicht besteht auch **nach** Inverkehrbringen eines Produkts (sog. Marktbeobachtung)
- Pflicht zur Gefahrenabwehr i. R. einer Verkehrssicherungspflicht umfasst „prinzipiell auch solche Gefährdungen, die sich erst aus dem vorsätzlichen Eingreifen eines Dritten ergeben“ (vgl. BGH, Urteil vom 19.12.1989 - VI ZR 182/89, NJW 1990, 1236)
- **Problem**: I.R.d. Produktbeobachtungspflicht nur Pflicht zur Warnung oder auch zur Bereitstellung eines Updates?

Noerr

Ansprüche des betroffenen Unternehmens

Ansprüche gegen externe Cloud-Betreiber

Cloud Computing

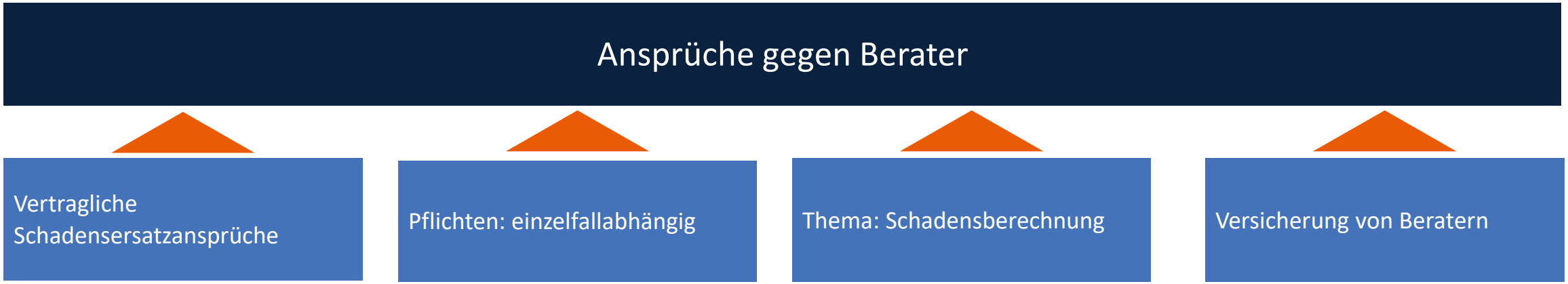
- Angebot/Bereitstellung vielschichtiger und umfassender Soft- und Hardwareleistungen in Form eines abstrakten Dienstes über ein Netzwerk
- Auslagerung von Daten, Dokumenten, Anwendungen etc. auf externe Server (sog. Cloud)

Haftungsgrundlagen

- **Problem**: Rechtliche Einordnung eines Cloud Computing Vertrages, da individuelle Ausgestaltung zu berücksichtigen
- Typengemischter Vertrag (miet-, werk- und dienstvertragliche Elemente)
- Auf welche Anspruchsgrundlage ein Schadensersatzanspruch gestützt werden kann, hängt davon ab, welches vertragliche Element durch den Cyberangriff betroffen ist
- Deliktische Haftung aus § 823 Abs. 1 BGB wegen Verletzung von Verkehrssicherungspflichten?

Noerr

Ansprüche des betroffenen Unternehmens



Ansprüche des betroffenen Unternehmens

Ansprüche gegen Arbeitnehmer

Grds. eingeschränkte Haftung nur bei betrieblich veranlasster Tätigkeit (sog. innerbetrieblicher Schadensausgleich)

- Eine Tätigkeit ist dann betrieblich veranlasst, wenn sie dem Arbeitnehmer arbeitsvertraglich übertragen worden ist oder sie im Interesse des Arbeitsgebers für den Betrieb ausgeführt wird (BAG, Urt. v. 18.04.2002 – 8 AZR 348/01, NJW 2003, 377)
- LAG Sachsen, Urt. v. 13.06.2017, 3 Sa 556/16 (Fake President)
- Vorsätzlich verursachte Schäden hat der Arbeitnehmer vollumfänglich zu tragen

Bei mutwilligem Handeln, das nicht betrieblich veranlasst ist, haftet der Innentäter wie ein außenstehender Angreifer nach den bereits dargestellten deliktsrechtlichen Grundsätzen

Noerr

Ansprüche des betroffenen Unternehmens

Ansprüche gegen Geschäftsleiter

Allgemeine Grundsätze der Organhaftung

Bestandssicherungspflicht aus § 91 Abs. 2 AktG i.V.m. § 93 Abs. 2 Satz 1 AktG?

- Pflicht zur Implementierung eines **Überwachungs- und Früherkennungssystems**; Einrichtung eines IT-Sicherheitssystems (Informieren über drohende Risiken und Ergreifung von Gegenmaßnahmen)
- Die Überwachungspflicht bezieht sich insoweit sowohl auf die **Gefährdungslage** als auch auf die zur **Gefahrenabwehr** ergriffenen Maßnahmen (d.h. der IT-Sicherheitsstandard ist regelmäßig zu überprüfen)
- Der Umfang der zu ergreifenden **IT-Sicherheitsmaßnahmen** richtet sich nach der Sensibilität der Unternehmensdaten, den denkbaren Schadensszenarien und den möglichen Schäden und Kosten, die aus einem Cybervorfall resultieren würden
- hierbei Orientierung an Branchenstandards und „Stand der Technik“
- Besondere aufsichtsrechtliche Vorgaben, z.B. VAIT, BAIT

Pflicht zum Abschluss einer Cyber-Versicherung?

D&O-Versicherung

IT-Sicherheit ist Chefsache

Noerr

Haftungsrisiken des betroffenen Unternehmens

Ansprüche von Vertragspartnern/Kunden

Vertragliche Mängelrechte

- Bei Eingriff in den Produktionsablauf durch Cyberangriff, soweit Produktion IT-gesteuert ist und der Angriff zu einem mangelbehafteten Endprodukt führt – Relevanz der konkreten vertraglichen Ausgestaltung

Schadensersatzanspruch wegen Verletzung der Pflicht zur Rücksichtnahme auf die Rechtsgüter des Vertragspartners gemäß §§ 280 Abs. 1, 241 Abs. 2 BGB bei Datenverlust oder -diebstahl infolge eines Cyberangriffs

Schadensersatz wegen Verzögerung der Leistung gemäß §§ 280 Abs. 1, 2, 286 BGB

- z.B. bei Betriebsunterbrechung, die zu einem Lieferverzug führt

Verschulden

- Fahrlässigkeitsvorwurf schon bei nicht regelmäßiger Aktualisierung von Sicherheitssoftware?
- Zurechnung des Verschuldens eines Dienstleisters gemäß § 278 BGB z.B. beim Outsourcing von IT?

Konflikt zwischen Ansprüchen und Haftungsrisiken des betroffenen Unternehmens

Noerr

Haftungsrisiken des betroffenen Unternehmens

Deliktische Ansprüche von Vertragspartnern/Kunden und von Dritten

Spezielle Haftungsnormen wie § 44 Abs. 1 Satz 4 TKG (Schadensersatz bei Verstoß gegen das TKG)

§ 823 Abs. 1 BGB i. V. m. Art. 1 und Art. 2 GG wegen einer Verletzung des Allgemeinen Persönlichkeitsrechts

§ 823 Abs. 1 BGB

- Ggf. gesetzliche Produzentenhaftung gegenüber dem Endabnehmer eines fehlerhaften Produkts, wenn der Cyberangriff zu dieser Fehlerhaftigkeit geführt hat
- Ggf. Verletzung von IT-Sicherheitspflichten?

§ 823 Abs. 2 BGB i. V. m. DS-GVO

Vorschriften der DS-GVO dürften weitestgehend als Schutzgesetze einzuordnen sein, denn Art. 1 DS-GVO lautet:

(1) *„Diese Verordnung enthält Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Verkehr solcher Daten.“*

(2) *„Diese Verordnung schützt die Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere deren Recht auf Schutz personenbezogener Daten.“*

Noerr

Haftungsrisiken des betroffenen Unternehmens

Schadensersatz nach der DS-GVO

Artikel 82 Abs. 1 DS-GVO:
*„ 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.“*

Artikel 82 Abs. 2 Satz 1 DS-GVO:
„Jeder an einer Verarbeitung beteiligte Verantwortliche haftet für den Schaden, der durch eine nicht dieser Verordnung entsprechende Verarbeitung verursacht wurde.“

- Verstoß gegen die Verordnung z. B. bei Verstößen gegen
  - die allgemeinen Grundsätze für die Verarbeitung personenbezogener Daten in Art. 5 DS-GVO
  - **aber auch**: Verstöße gegen delegierte Rechtsakte sowie nationale Rechtsvorschriften der Mitgliedstaaten zur Präzisierung der DS-GVO
- Nachweis mangelnden Verschuldens ist durch den Verantwortlichen/Auftragsverarbeiter zu erbringen, Abs. 3
- Schaden anzunehmen insbesondere, *„wenn die Verarbeitung zu einer Diskriminierung, einem Identitätsdiebstahl oder -betrug, einem finanziellen Verlust, einer Rufschädigung, einem Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden personenbezogenen Daten, der unbefugten Aufhebung der Pseudonymisierung oder anderen erheblichen wirtschaftlichen oder gesellschaftlichen Nachteilen führen kann […].“* (75. Erwägungsgrund DS-GVO)

Noerr

Haftungsrisiken des betroffenen Unternehmens

Verhängung von Geldbußen

Bußgelder nach Art. 83 DS-GVO, verhängt durch die Aufsichtsbehörde

- Verstoß gegen Datensicherheitsanforderungen
- Z.B. Verstoß gegen die Vorgaben hinsichtlich der Sicherheit der Verarbeitung aus Art. 32 DS-GVO (Einhaltung eines dem Risiko angemessenen Schutzniveaus)
  - Geldbußen von bis zu 10 Mio. EUR oder von bis zu 2 % des weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs, je nachdem, welcher der Beträge höher ist (Art. 83 Abs. 4 a) DS-GVO)
- Verstoß gegen die Grundsätze für die Verarbeitung personenbezogener Daten (Art. 5 DS-GVO), etwa gegen den Grundsatz der Datenminimierung aus Abs. 1 c)
  - Geldbußen von bis zu 20 Mio. EUR oder von bis zu 4 % des weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs, je nachdem, welcher der Beträge höher ist (Art. 83 Abs. 5 a) DS-GVO)
- Verstoß gegen Dokumentations- oder Meldepflichten
  - Dokumentationspflichten aus Art. 33 Abs. 5 DS-GVO und Meldepflichten aus Art. 33 und 34 DS-GVO
  - Umfang der Geldbuße richtet sich hier nach Art. 83 Abs. 4 a) DS-GVO
- Bußgeld gemäß § 14 BSIG z. B. wegen Verletzung einer Meldepflicht aus § 8b Abs. 4 BSIG für Betreiber Kritischer Infrastrukturen

Bußgeld gemäß § 14 BSIG z. B. wegen Verletzung einer Meldepflicht aus § 8b Abs. 4 BSIG für Betreiber Kritischer Infrastrukturen

Noerr

Fazit und Ausblick

- Derzeit umfassende Gefährdungslage für Wirtschaft, Gesellschaft und den öffentlichen Bereich/Verwaltung
- Vielfältige Haftungsrisiken für betroffene Unternehmen
- Digitalisierung und Vernetzung von Arbeitsprozessen steigert die Gefahr von Cyberangriffen
- Weitere Entwicklung hinsichtlich Gefahrenquellen und Haftung abhängig von diversen Faktoren:
  - Weitere Zunahme von IT-Outsourcing?
    Mögliche Folge: Steigende Relevanz von Haftungsfreizeichnungsklauseln
  - Cybersecurity Act auf EU-Ebene
  - Mögliche Einführung neuer Straftatbestände (z. B. Strafbarkeit des „digitalen Hausfriedensbruches“)
  - Zunehmende Relevanz der Geschäftsführerhaftung bei Cyberschadensfällen
    Mögliche Folge: Relevanz von IT-spezifischen Themen für D&O-Versicherungen
- Bedeutung eines funktionierenden Notfallmanagements – Prevent, Detect, Respond

Noerr

Dr. Oliver Sieg
Rechtsanwalt
Partner

+49 211 49986220
oliver.sieg@noerr.com

Oliver Sieg ist seit 1995 als Rechtsanwalt zugelassen. Er ist Co-Leiter der Litigation-Praxis bei Noerr.

Im Vordergrund der Praxis von Oliver Sieg steht die Prozessführung vor erstinstanzlichen und Berufungsgerichten, insbesondere in komplexen, auch grenzüberschreitenden Auseinandersetzungen. Er ist erfahren in der Führung von Schiedsgerichtsverfahren, vorwiegend nach DIS- oder ICC-Regeln sowie ad hoc, auch als Schiedsrichter.
Laut JUVE gehört Oliver Sieg zu den führenden Namen in „gesellschaftsrechtlichen Streitigkeiten“ sowie in „D&O-Beratung und Prozessen“.

Oliver Sieg ist unter anderem Mitglied des Fach- und Gesetzgebungsausschusses Versicherungsrecht des Deutschen Anwaltvereins, Vorsitzender des Vorprüfungsausschusses Versicherungsrecht der Rechtsanwaltskammer Düsseldorf und Beiratsmitglied der Forschungsstelle Versicherungsrecht der Universität Münster.

Kompetenzen

- Prozessführung
- Nationale und internationale Schiedsverfahren
- Manager-, Berufs- und Bankenhaftpflicht
- Gesellschaftsrechtliche Auseinandersetzungen
- Versicherungs- und Rückversicherungsrecht
- Vertragsrechtliche Streitigkeiten (Lieferbeziehungen, Dienstleistungen, Finanzierungen)
- Cyber-Haftung