

Cyberversicherung im Transportbereich

DGTR / DAV Webinare Transportrecht, 29.10.2020

Dr. Henning Schaloske, Partner



Allianz Risk Barometer 2020: Cyber steigt zum weltweiten Top-Risiko für Unternehmen auf

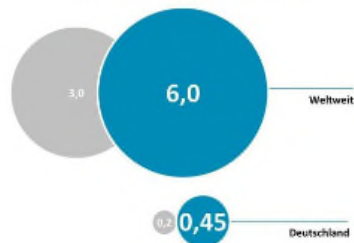
Pressemitteilung | 14. Januar 2020 | München

Cybercrime bedroht auch die Logistik

28.06.2017 | Redakteur: [M. A. Benedikt Hofmann](#)

Transport- und Logistikanbieter stehen im Fadenkreuz von hoch spezialisierten Hackern. Doch dem Strategieberatungsunternehmen Oliver Wyman zufolge können Unternehmen mit überzeugendem Risikomanagement von der Cybergefahr profitieren.

Direkte Kosten von Cyberangriffen weltweit und in 2017 vs. 2020, in Milliarden Euro¹



Die Transport- und Logistikbranche gerät immer stärker ins Visier von Cyberkriminellen. Mit der zunehmenden Digitalisierung der Prozesse bei Verladern, Spediteuren, Transportunternehmen und Infrastrukturbetreibern wachsen die Gefahren von

¹ Einschätzung basierend auf dem Bericht 'Direct Costs of Cyberattacks' von Oliver Wyman, veröffentlicht am 12. Juni 2017. Quelle: Oliver Wyman Analytics

Cyber Incidents



Ransomware



**Network
Interruption**



**Data
Breaches**



**Social
Engineering**



CYBERCRIME



**SUPPLY
CHAIN RISK**



**PHYSICAL
RECORDS**



**PHYSICAL
REALM**

Fig 1 Cyber Claims received by AIG EMEA (2018) – By reported incident



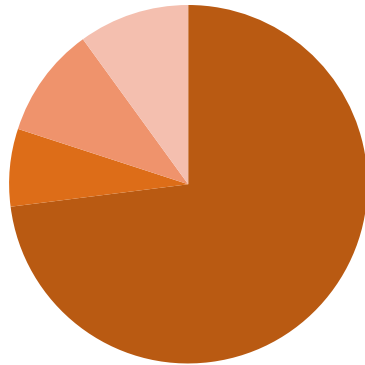
*Denial of Service Attacks, Legal/Regulatory Proceedings based on violations of data privacy regulations

¹ Europe, Middle East & Africa

² Previously, such attacks fell within the scope of 'other security failure/unauthorised access'.

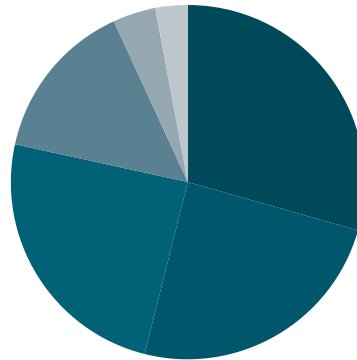
Cyberrisiken: Erfahrungen aus unserer Beratungspraxis

Angriffsszenarien



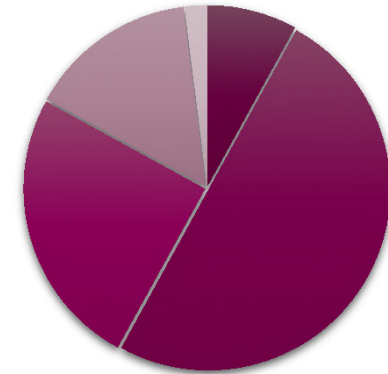
- Ransomware
- sonstig. Systemunterbrechung
- "Advanced Persistent Threat"
- Sonstiges

Schadensposten (nach Häufigkeit)



- Wiederherst. (IT-FK, SystemV., Mitarb.)
- Betriebsunterbrechung
- Krisenmanag. (IT-FK, Info., etc.)
- Rettungskosten
- Haftpflichtschäden
- DSGVO inkl. Datenschutz-Verfahren

Forensikkosten (Schätzung)



- < 50.000
- 50.000 bis 200.000
- 200.000 bis 1.000.000
- 1. Mio. - 5 Mio.
- > 5 Mio.

Key trends: Incident response & beyond



NOTIFICATION ISSUES



**CHANGES IN
LEGISLATION**



LIABILITY



**SILENT CYBER /
COVERAGE**



**RECOVERY /
FUND TRACING**



**CYBER
RESILIENCE**

FLUGGESELLSCHAFT

British Airways soll Millionenstrafe wegen gestohlener Daten zahlen

Die britische Datenschutzbehörde verhängt nach dem Hackerangriff im vergangenen Sommer eine Rekordstrafe gegen die Airline: Sie fordert über 200 Millionen Euro von British Airways.



Kerstin Leitel

08.07.2019 • Update: 08.07.2019 - 09:45 Uhr • [Kommentieren](#) • [3 x geteilt](#)



Cyberpolicen: „Nice to have“ oder unverzichtbar?

geschrieben von [Wessel Heukamp](#) am 17. Februar 2020 in [Abo,Allgemein,Kommentare,Legal Eye – Die Rechtskolumne](#).

[Legal Eye – Die Rechtskolumne](#) Die Gefahr von Cyberangriffen zählt zu den größten Risiken, denen sich Unternehmer zwangsläufig die Frage, ob und in welchem Umfang der Abschluss einer Cyberversicherung auch aus rechtlicher Sicht erkaufen können, stellen müssen. Wie es um die Lage bestellt bleibt, bleibt abzuwarten.



Wessel Heukamp ist Partner bei der Kanzlei Freshfields Bruckhaus Deringer

Cyberangriffe erfolgen immer häufiger. Damit spielen [die deutschen Unternehmen Cyberrisiken noch vor](#) kaum verwunderlich. So hat etwa die Schadsoftw Unternehmen entfielen dabei Schadenpositionen in einigen Jahren Cyberversicherungen abschließen. Berater KPMG für die DACH-Region (Deutschland,

Auf dem deutschen Markt gibt es inzwischen eine Vielfalt von Angeboten und des versicherten Risikos und somit im Umfang der Angebote. Zwar hat der Versichererverband GDV den Cyberversicherungsmarkt können sie schon heute nicht auf einen differenzierteren Versicherungsschutz an.



















Ist der Abschluss einer Cyberpolice Pflicht?























In Anbetracht des enormen Schadenpotenzials stellt sich die Frage, ob die Abschluss einer Cyberversicherung auch aus rechtlicher Sicht erforderlich ist. In den USA sind Manager infolge von Datenlecks durch Yahoo und ihre Geschäftsleitung auf die Zahlung von Schadensersatz für die Verantwortlichkeit von Vorstand und Geschäftsleitung geurteilt worden.

Für die Verantwortlichkeit von Vorstand und Geschäftsleitung

Folgende 40 Versicherer bieten das Produkt „Cyberversicherung“ an

A-Z ▾

 <p>AIG AIG Europe S.A. Direktion für Deutschland</p>	 <p>Allianz Allianz Versicherungs-Aktiengesellschaft</p>	 <p>ALTE LEIPZIGER Alte Leipziger Versicherung Aktiengesellschaft</p>	 <p>ARAG ARAG Allgemeine Versicherungs-Aktiengesellschaft</p>	 <p>AXA AXA Versicherung AG</p>	 <p>Basler Basler Sachversicherungs-AG</p>
 <p>VER SICHERUNGSKAMMER BAYERN Bayrischer Versicherungsverband Versicherungsaktiengesellschaft</p>	 <p>BGVA BGV-Versicherung AG</p>	 <p>CHUBB Chubb European Group SE Direktion für Deutschland</p>	 <p>CNA CNA Insurance Company (Europa) S.A. Direktion für Deutschland</p>	 <p>ERGO ERGO Versicherung AG</p>	 <p>EHL EULER HERMES Euler Hermes Deutschland Niederlassung der Euler Hermes SA</p>
 <p>GHV Gemeinnützige Haftpflicht-Versicherungsentst. Darmstadt</p>	 <p>Gothaer Gothaer Allgemeine Versicherung AG</p>	 <p>GVV GVV-Kommunalversicherung VVaG</p>	 <p>HAMBURGER FEUERKASSE Hamburger Feuerkasse Versicherungs-Aktiengesellschaft</p>	 <p>HDI HDI Global SE</p>	 <p>helvetia Helvetia Schweizerische Versicherungs-gesellschaft AG Direktion für Deutschland</p>

 <p>HISCOX HISCOX S.A. Niederlassung für Deutschland</p>	 <p>INTER Allgemeine Versicherung AG</p>	 <p>LVM Landwirtschaftlicher Versicherungsverein Münster a.G.</p>	 <p>Mannheimer Mannheimer Versicherung Aktiengesellschaft</p>	 <p>MSIG MSIG Insurance Europe AG</p>	 <p>Munich RE Münchener Rückversicherungs-Gesellschaft Aktiengesellschaft in München</p>
 <p>ÖSA Österreichische Feuerversicherung Sachsen-Anhalt</p>	 <p>PROVINZIAL Provincial Nord Brandkassen Aktiengesellschaft</p>	 <p>PROVINZIAL Provincial Rheinland Versicherung AG Die Versicherung der Sparkassen</p>	 <p>R+V R+V Allgemeine Versicherung AG</p>	 <p>R+V R+V Versicherung AG</p>	 <p>SIGNAL IDUNA SIGNAL IDUNA Allgemeine Versicherung AG</p>
 <p>SOCIETE GENERALE SOGECAP S. A. Deutsche Niederlassung</p>	 <p>SV Sparkassen Versicherung Sachsen</p>	 <p>SV Sparkassen Versicherung AG</p>	 <p>VER SICHERUNGSKAMMER BAYERN Versicherungskammer Bayern Versicherungsanstalt des öffentlichen Rechts</p>	 <p>VGH VGH Landschaftliche Brandkasse Hannover</p>	 <p>VHV VHV Allgemeine Versicherung AG</p>
 <p>PROVINZIAL Westfälische Provinzial Versicherung Aktiengesellschaft</p>	 <p>WV Württembergische Gemeinde- Versicherung a. G.</p>	 <p>WV Württembergische Versicherung AG</p>	 <p>ZURICH Zurich Insurance plc Niederlassung für Deutschland</p>		



**Unverbindliche Bekanntgabe des Gesamtverbandes der Deutschen Versicherungswirtschaft e.V. (GDV)
zur fakultativen Verwendung. Abweichende Vereinbarungen sind möglich.**

Allgemeine Versicherungsbedingungen für die Cyberrisiko-Versicherung (AVB Cyber)

**Musterbedingungen des GDV
(Stand: April 2017)**



Anzeige



DIE ALLIANZ ONLINE-TARIFIERUNG FÜR KLEINFLOTTEN.

In Privat Kraft auch für Camper, Kräder und Anhänger.

[JETZT INFORMIEREN](#)



22. Oktober 2018

Gewerbe-Cyberating von Franke und Bornberg konstatiert Luft nach oben

Die Ratingagentur Franke und Bornberg hat gewerbliche Cyberpolisen im deutschen Markt unter die Lupe genommen. Kein Produkt hat das Höchststrating FFF+ erreicht. Die zweitbeste Note FFF wurde von den stärksten Produkten denkbar knapp verpasst. Die mit FF+ stärksten Policen liefern AIG, HDI, Hiscox und Markel.

Meistgelesen

Am deutschen Markt sind Cyberversicherungen für Unternehmen seit gut acht Jahren präsent, zunächst für Industrie-Risiken und auf Basis anglo-amerikanischer Deckungskonzepte. Spätestens mit



[STARTSEITE](#) > [ABO](#) > **ASSEKURATA NIMMT CYBERPOLICEN UNTER DIE LUPE**

Assekurata nimmt Cyberpolicen unter die Lupe

VON [KATRIN BERKENKOPF](#) AM 26. OKTOBER 2020

 [ARTIKEL DRUCKEN](#)

Gerade kehren viele Mitarbeiter wieder ins Homeoffice zurück, die Gefahr von Cyberattacken steigt. Eine Cyberdeckung wird deshalb auch für viele kleinere Unternehmen zum Thema. Die Ratingagentur Assekurata hat sich die Policen für diese Kunden zum ersten Mal genauer angeschaut. Das Angebot ist sehr heterogen und selbst im Kleingedruckten sind die wichtigsten Informationen nicht leicht zu finden, sagen die Analysten. Dennoch gibt es für die meisten Anbieter gute Noten.



Die Ratingagentur Assekurata hat elf Anbieter von Cyberpolicen speziell für kleine und mittlere Unternehmen untersucht

© CCO Public Domain

Die Ratingagentur Assekurata hat sich erstmals mit Cybertarifen speziell für kleine und mittlere Unternehmen (KMU) beschäftigt. Durch den vermehrten Einsatz der Mitarbeiter im Homeoffice seien diese Deckungen für KMU immer wichtiger, erklärten die Kölner Analysten. Bislang verfügt nur eine Minderheit dieser Unternehmen über eine entsprechende Police. Es gibt auch noch keinen Marktstandard, so dass es für Kunden und Vermittler schwierig ist, den Inhalt der verschiedenen Angebote zu vergleichen. Diese große

Überblick über die Cyber-Risiken für Unternehmen

Risiken im Einzelnen



Cyber Schadensfall

Szenario

Die Transport AG unterhält seit dem 01.06.2020 bis zum 01.06.2021 eine Cyberversicherung über EUR 10 Mio.

Am 23.10.2020 (23.04.2020) dringen russische Hacker in das IT System ein und schalten am 28.10.2020 die Ransomware scharf, verschlüsseln die Daten der Transport AG und fordern EUR 1 Mio. „Lösegeld“. Die Gesellschaft zahlt, nachdem die Hacker Daten teils veröffentlicht haben. Wegen Datenschutzverletzungen erfolgen Meldungen nach Art. 33 DSGVO in Deutschland sowie nach entsprechenden Anforderungen in weiteren Ländern (Kosten EUR 500.000). Die Datenschutbehörde verhängt ein Bußgeld von EUR 1 Mio.

Die Transport AG schaltet unverzüglich die IT Systeme ab. IT Spezialisten untersuchen Vorfall. Die Kosten betragen später EUR 500.000. Der Betriebsunterbrechungsschaden beläuft sich bei der AG auf EUR 8,5 Mio. und bei einer mitversicherten Gesellschaft in China auf weitere EUR 2 Mio.





Die Versicherung reguliert wegen veralteter IT Security und Obliegenheitsverletzungen lediglich EUR 5 Mio. Die Transport AG will Regress bei ihren Vorstandsmitgliedern nehmen.

Versicherungslösungen bei Cyber-Risiken



Leistungsumfang

Die Cyberversicherung deckt...


✓ Eigenschäden

-  Wirtschaftliche Schäden durch **Betriebsunterbrechung**.
-  Zahlung eines Tagessatzes.
-  Kosten der **Datenwiederherstellung** und **System-Rekonstruktion**.
-  Übernahme der Kosten.

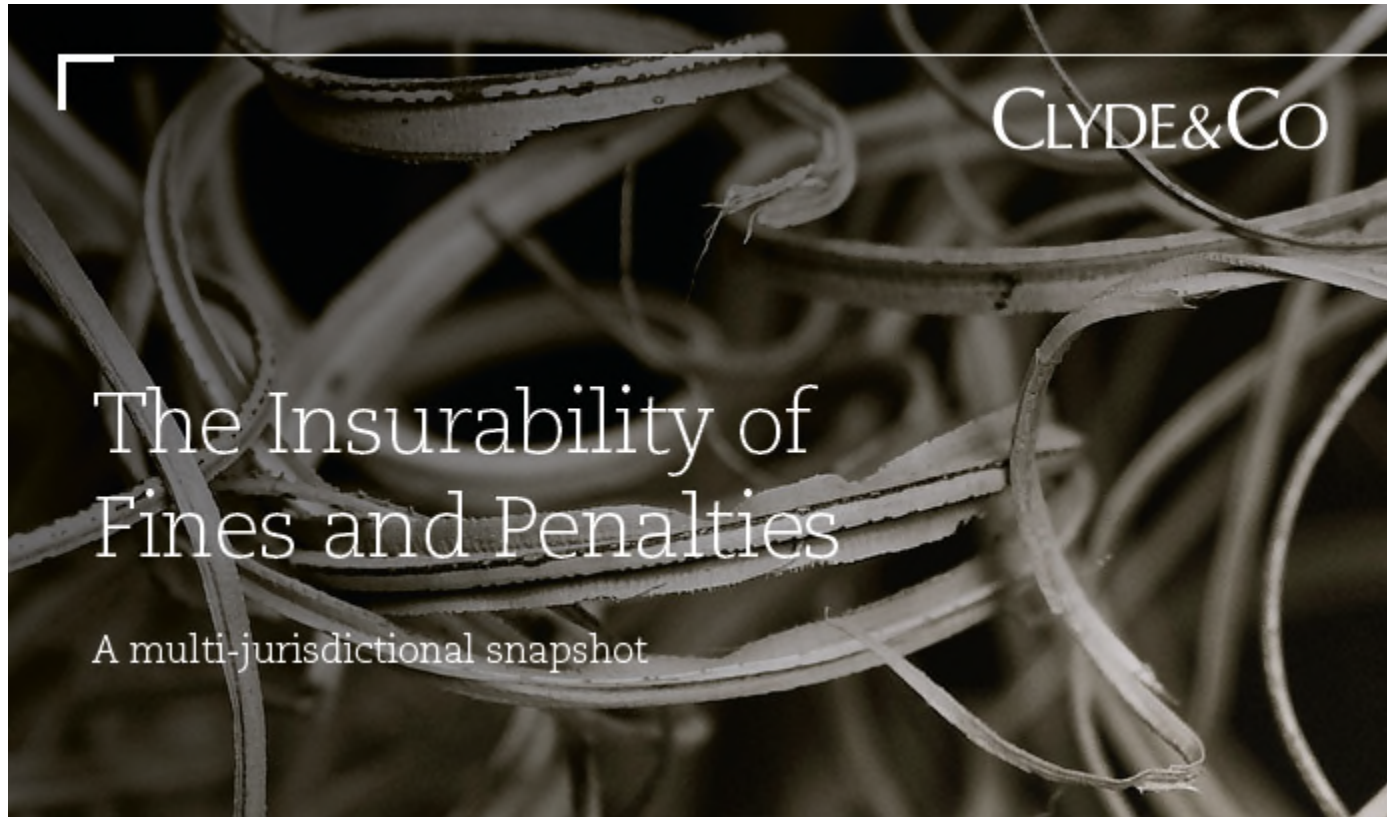
✓ Drittschäden

-  **Schadensersatzforderungen** von Kunden wegen **Datenmissbrauch** und/oder **Lieferverzug**.
-  Entschädigung berechtigter und Abwehr unberechtigter Forderungen.

✓ Service-Leistungen

-  **IT-Forensik-Experten** zur Analyse, Beweissicherung und Schadenbegrenzung.
-  **Anwälte für IT- und Datenschutzrecht** zur Erfüllung der Informationspflichten.
-  **PR-Spezialisten für Krisenkommunikation** zur Eindämmung des Imageschadens.
-  Jeweils Übernahme von **Service & Kosten**.

Aktuelle Themen



Versicherungslösungen bei Cyber-Risiken

Grenzen des Versicherungsschutzes und Schadensminderungspflicht

- Grenzen des Versicherungsschutzes
 - Nur bedingungsgemäßer Schutz – unterschiede in den Produkten
 - Bußgelder? Sachschäden (Hardwareschäden)? Systemverbesserungen?
 - Wissentliche Pflichtverletzungen und grob fahrlässige Schadensherbeiführung

Dieser Fall entscheidet, ob Hacken eine Kriegswaffe ist

Veröffentlicht am 14.12.2018 | Lesedauer: 5 Minuten

Von **Benedikt Fuest**



„Notpetya“ Vorgänger verlangte Lösegeld, deshalb fiel erst später auf, dass es diesmal um pure Zerstörung ging

Quelle: picture alliance/Bitdefender/dpa

Die Malware „Notpetya“ legte weltweit Konzerne lahm und verursachte Schäden in Milliardenhöhe. Doch trotz abgeschlossener Policen, will ein Versicherer nicht zahlen. Er verweist auf eine Klausel.

Aktuelle Themen

Kriegsausschluss

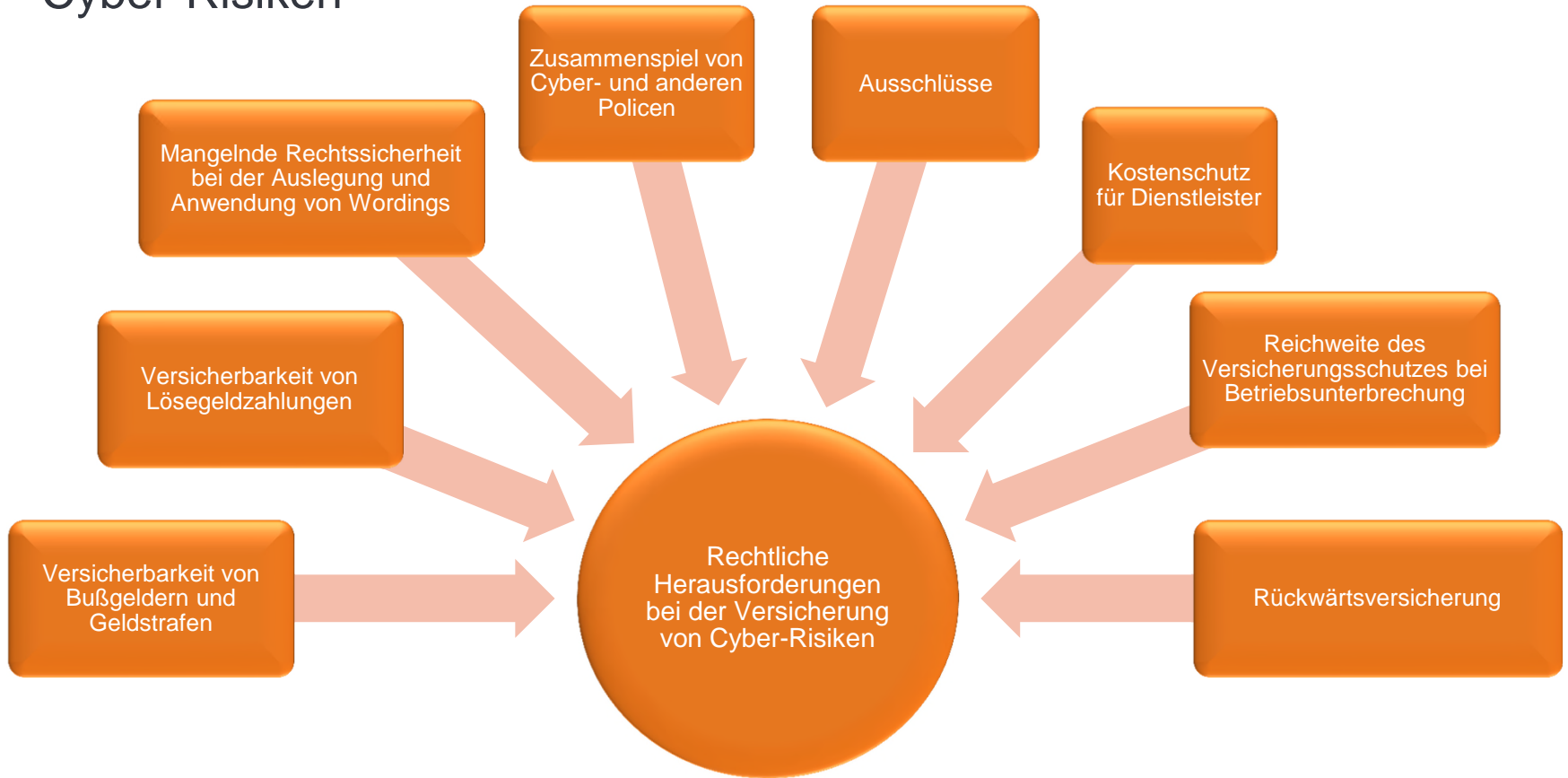
- Anlass der Diskussion
- Klauselbeispiele Cyberversicherung
 - „Versicherungsfälle oder Schäden aufgrund von Krieg. Krieg bedeutet: Krieg, Invasion, Bürgerkrieg, Aufstand, Revolution, Aufruhr, militärische oder andere Form der Machtergreifung.“ (AVB Cyber – Musterbedingungen des GDV, A1-17.2)
 - „die nachweislich auf Kriegsereignissen, anderen feindseligen Handlungen [...] beruhen, oder Maßnahmen von hoher Hand beruhen.“
 - Teilweise Definition von „**Cyberkrieg**“ oder Zusatz: „zur Erfüllung des Kriegsbegriffes i.S.d. AVB **bedarf es nicht der Anwendung physischer Gewalt**“
 - „Versicherungsfälle aufgrund von Krieg, Invasion, feindlichen Handlungen, Terrorismus [...]. Dieser Ausschluss **gilt nicht für** cyber-terroristische Handlungen, die zur Geltendmachung von Ansprüchen führen“

Aktuelle Themen (national)

Kriegsausschluss – Reichweite des Deckungsausschlusses für „Krieg“

- „Wenn der Angriffserfolg sich physisch manifestiert, genügt dies ohne weiteres, also z. B. **wenn es durch den Cyberangriff zu Sachschäden** kommt in Form von Brand- /Explosionsschäden und/oder Personenschäden. Es ist aber auch nicht ausgeschlossen, dass bei Fehlen von physischen Schäden die **Auswirkungen eines Cyberkrieges dem eines klassischen Krieges gleichkommen**, z. B. bei kompletter Unterbrechung der Kommunikationswege, der Transportmöglichkeiten und/oder der Stromversorgung. In diesem Falle kann auch der nicht physische Angriff ein „Krieg“ sein.“ (Günther, in: r+s 2019, 188)
- „Es ist kein Grund ersichtlich, warum ein durchschnittlicher VN den Kriegsausschluss bei Cyberversicherungen anders verstehen sollte, als bei Sachversicherungen. Insoweit stellt ein Cyberkrieg – was immer hierunter auch genau zu verstehen wäre – keinen Krieg im Sinne des Ausschlussstatbestandes dar. **Es fehlt an einer „bewaffneten Auseinandersetzung“**. Beim Cyberkrieg werden Computer, aber keine Waffen eingesetzt und Streitkräfte stoßen auch nicht physisch auf fremdes Staatsterritorium vor. Vor diesem Hintergrund ist es auch fraglich, ob generell argumentiert werden kann, dass Cybermaßnahmen zur Unterstützung eines konventionellen Kriegs unter den entsprechenden Ausschlussstatbestand subsumiert werden können.“ (Fortmann, in: r+s 2019, 429)
- „Auf Grundlage einer solchen Klausel wäre also z. B. zu entscheiden, ob für den Ausschluss eine **zielgerichtete Handlung des (angreifenden) Staates** gerade gegen den VN notwendig ist oder ob insoweit auch jeder **"Kollateralschaden" ausreicht**, d. h. jede (nicht beabsichtigte und gegebenenfalls weit entfernte) mittelbare Folge. Im Streitfall müsste der VR auch in tatsächlicher Hinsicht beweisen, dass der Virus bzw. der Cyberangriff von einem fremden Staat verübt wurde. **Dieser Beweis dürfte praktisch wohl kaum geführt werden können.**“ (Malek, Schütz, in: r+s 2019, 421)

Rechtliche Herausforderungen bei der Versicherung von Cyber-Risiken



04.07.2019 SCHLAGLICHT

Problemfall Silent Cyber: Versicherungskunden drohen harte Ausschlüsse

Von **Sabine Pawig-Sander**

Versicherungs-
wirtschaftHEUTE



Quelle: rgraymon/ Pixabay

Andere Versicherungen

Von “Silent Cyber” bis “Affirmative Coverage”

- Abgrenzung insbesondere:
 - Betriebshaftpflichtversicherungen
 - Sachversicherung
 - Vertrauensschadenversicherung
 - Subsidiaritätsregelungen / Vorrang Cyber Versicherung
- Komplementär:
 - D&O-Versicherung
 - Herbeiführung des Versicherungsfall als Deckungsausschluss/-begrenzung unter Cyber Versicherung

Managerhaftung für erfolgreiche Cyberangriffe

Pflicht zur Befassung und Verfolgungszwang (ARAG/Garmenbeck)

3 // Wirtschaftspraxis

Deutscher **Anwalt**Spiegel

Ausgabe 04 // 22. Februar 2017

IT-Sicherheit ist Chefsache

Bei der Abwehr von Cyberkriminalität sind Unternehmensleiter in der Pflicht

Von Dr. Michael Rath und Simon Heetkamp

Im Gegenteil, laut einer Untersuchung des Security-Herstellers Symantec konzentriert sich über ein Drittel der kriminellen Cyberaktivitäten auf Unternehmen mit weniger als 250 Angestellten. Mittlerweile sind bereits 69% der deutschen Industrieunternehmen Opfer von Cyberangriffen geworden. Hierdurch entstehen Schäden, die vom Digitalverband Bitkom auf über 50 Milliarden Euro jährlich taxiert werden. Die Bundesregierung hob Ende 2016 im Jahr ihrer „Cyber-Sicherheitsstrategie für Deutschland 2016“ hervor, dass Cybersicherheit ein gemeinsamer Auftrag für Staat und Wirtschaft sei.

Im Zuge ihrer Raubzüge greifen Hacker zu verschiedenen

einen bestimmten Betrag zahlt. Alternativ legen Hacker mit sogenannter „Ransomware“ die IT-Infrastruktur eines Unternehmens lahm oder sperren Teile der Software oder Daten. Erst wenn das Unternehmen ein „Lösegeld“ gezahlt hat, erlangt es wieder vollständigen Zugriff auf sein IT-System.

Im Folgenden soll dargestellt werden, welche Pflichten die Prävention derartiger Cyberangriffe für die Unternehmensleitung mit sich bringt und welche Folgen sich aus entsprechenden Pflichtverletzungen ergeben können.

Anforderungen an die Unternehmensleitung

Für die Betreiber kritischer Infrastrukturen gilt das IT-Sicherheitsgesetz, wonach effektive Sicherheitsmaß-

Dem elektronischen Griff in die Kasse muss ein leistungsfähiges IT-Sicherheitssystem entgegengestellt werden.



Managerhaftung

Compliance- und Organisationspflichten: Datenschutz und IT-Sicherheit

- **Da Cyberrisiken Bestandsrisiken sein können:**
 - IT-Sicherheit bildet einen integralen Bestandteil des Risikomanagements der Geschäftsleitung
- **Pflicht zur Schaffung und Erhaltung der IT-Sicherheit und Einhaltung Datenschutz**
 - Konkret: Pflicht „*angemessene und organisatorische Maßnahmen*“ zu treffen (=Organisationspflichten) und deren Einhaltung zu überwachen (=Überwachungspflichten)
- **Gesamtverantwortung der Geschäftsleitung:**
 - Vorstand muss als Kollegialorgan entscheiden, welche Maßnahmen für die unternehmensspezifische IT-Sicherheit notwendig sind
 - Kernaufgabe der Geschäftsleitung: Aufgabe ist nicht delegierbar! Aber: Ressortaufteilung möglich und Einbeziehung von fachkundigen Mitarbeitern möglich, aber (Gesamt-) Verantwortung bleibt
 - BGH: „*Auch eine für sich genommen zulässige Verteilung der Geschäftsführungsaufgaben entbindet denjenigen, dem hiernach nur bestimmte Aufgaben zur Erledigung zugewiesen sind, allerdings nicht von seiner eigenen Verantwortung für die ordnungsgemäße Führung der Geschäfte der Gesellschaft.* (BGH, Urteil vom 6.11.2018 – II ZR 11/17)

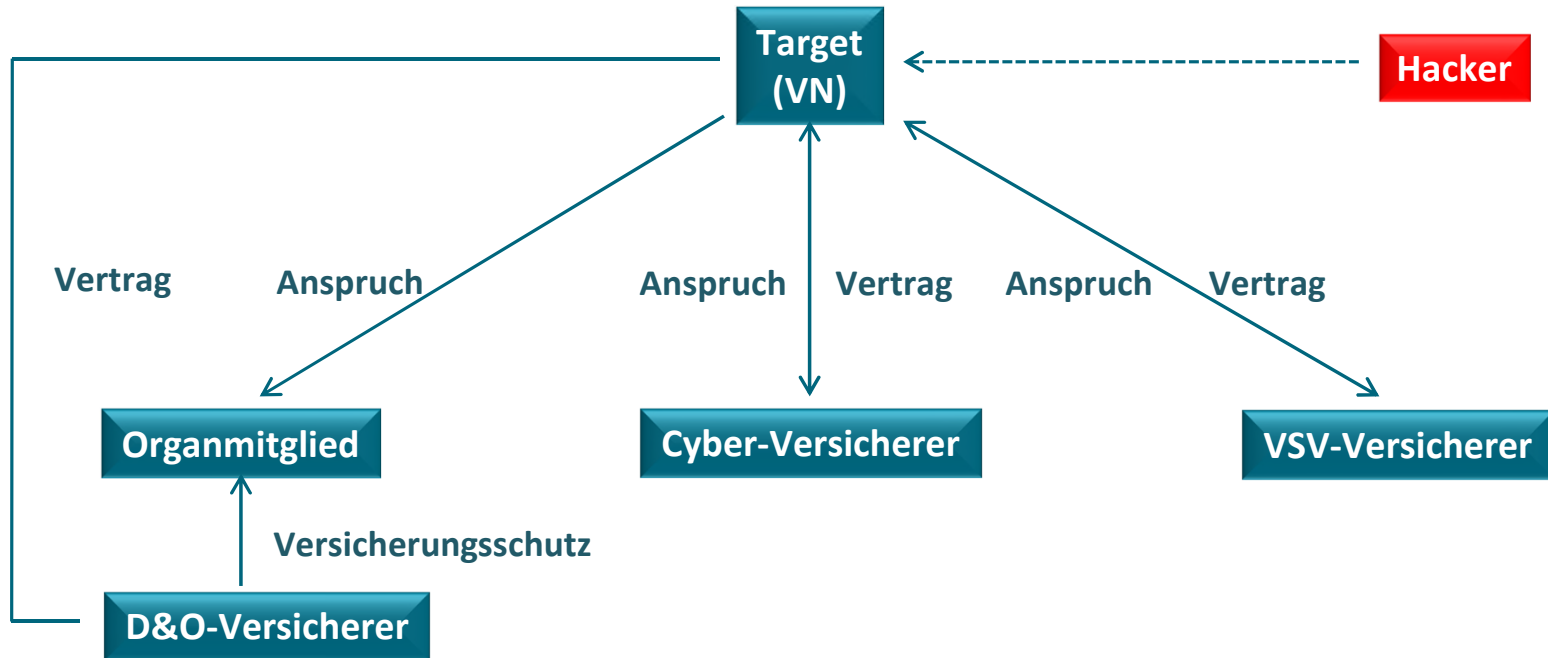
Rechtsfragen unter deutschen Cyber-Policen (Auswahl)

Mehrfachversicherung und Zusammenspiel mit anderen Policen

- Mehrfachversicherung und Subsidiaritätsklauseln
 - Beispiel: VSV, PI, Sach
 - Silent Cyber oder affirmative cover
 - Grundsatz: Vorrangigkeit Cyber-Versicherung und Folgen
- Insbesondere: Zusammenspiel und Abgrenzung mit D&O-Versicherung
 - Beispiel: Cyber-Angriff und Organisationspflichtverletzung
 - Eigenschaden- und Haftpflichtversicherung mit Stufenverhältnis
 - Herbeiführung des Versicherungsfalls (§ 81 VVG)

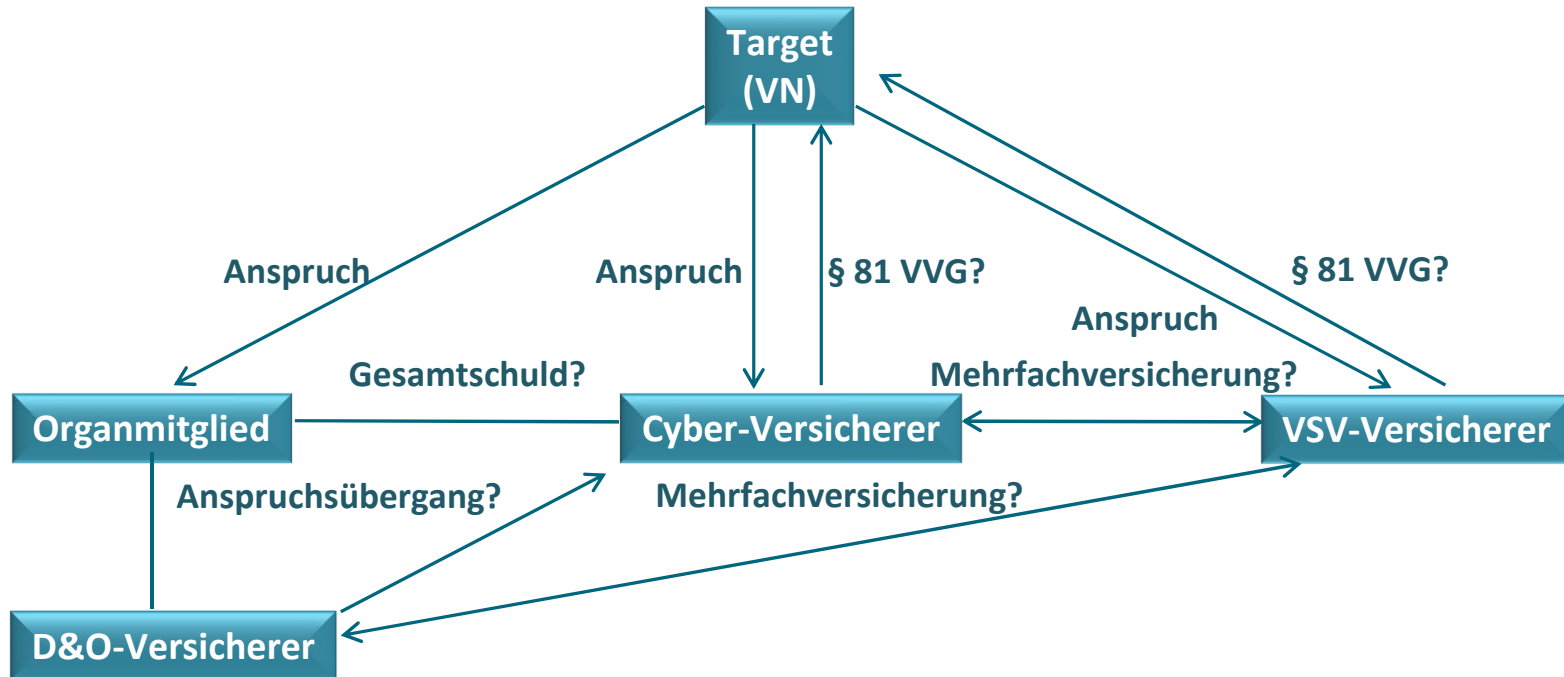
Schnittstellen zwischen D&O, Cyber und VSV

Ausgangslage



Schnittstellen zwischen D&O, Cyber und VSV

Schnittstellen-Überblick



Schnittstellen zwischen D&O, Cyber und VSV

Schnittstellen – allgemeine Überlegungen

- Cyber zu VSV
 - häufig Vorrang der Cyber-Versicherung geregelt, dann kein Regress
 - sonst Mehrfachversicherung abhängig von Subsidiaritätsklauseln
- Cyber / VSV zu D&O
 - wohl keine Gesamtschuld, sondern Stufenverhältnis / Vorrang Haftung der versicherten Person / Vertrauensperson / des Dritten
 - Folge: kein Anspruchsübergang zugunsten Organmitglied (§ 426 BGB), sondern Anspruchsübergang zugunsten Cyber / VSV (§ 86 VVG)
 - Folge: kein Anspruchsübergang zugunsten D&O-Versicherer, sondern grds. Regress durch Cyber / VSV möglich (sofern kein Verzicht)
- Problematik: Herbeiführung des Versicherungsfalls (§ 81 VVG)
 - bei Cyber ähnlich wie bei VSV: Organisationsverschulden (§ 81 II VVG)

Fazit

- Generell: Cyber-Versicherungsmarkt hat sich dynamisch entwickelt, ist wettbewerbsintensiv und mittlerweile durch eine hohen Zahl an Schadensfällen über alle Branchen einschließlich Transport und Logistik betroffen.
- Wettbewerb von Versicherern und Maklern schließt Suche nach besten Lösungen ein mit der Folge, dass Wordings sich stärker angleichen, jedoch durchaus signifikante Unterschiede in den Details verbleiben.
- Die Cyber-Versicherung ist in das Gesamt-Versicherungskonzept einzubinden und sinnvoll von anderen Versicherungen abzugrenzen oder diesen vorzuschalten.
- Die Schadenspraxis ist multidisziplinär, facettenreich und komplex. Unternehmen haben sich darauf präventiv dezidiert vorzubereiten.

Kontakt



Dr. Henning Schaloske
Partner

T: +49 (0)211 8822 8801
E: henning.schaloske@clydeco.com

Henning Schaloske leitet die deutsche Versicherungspraxis und den Düsseldorfer Standort von Clyde & Co und ist Mitglieds unseres European Boards.

Er berät im Haftungs-, Versicherungs- und Rückversicherungsrechts und verfügt über breite Erfahrung in staatlichen Gerichts- wie auch nationalen und internationalen Schiedsverfahren. Ein besonderer Schwerpunkt seiner Praxis liegt in den Financial Lines (D&O, PI, E&O, VSV), Cyber und W&I. Im Bereich Cyber hat Henning Schaloske bereite Erfahrung sowohl in der Wording-Entwicklung als auch in deutschen und internationalen Schadensfällen, insbesondere bei Breach Response & Notifications sowie Haftungsfällen, sowohl als Breach Response, Coverage und Monitoring Counsel.

Henning Schaloske wird als führender Experte und Thought Leader für Versicherungs-/Rückversicherungsrecht unter anderem durch JUVE, Wirtschaftswoche, Chambers Europe, Legal 500 und Who's Who Legal empfohlen.

50+

Offices

440

Partners

4,000

Total staff

2,500

Legal professionals

1,800

Lawyers

www.clydeco.com
