WILHELM

RECHTSANWÄLTE

Internationale Versicherungsprogramme

Cyberrisiken im internationalen Geschäft versichern

www.wilhelm-rae.de

November 2018

WILHELM
RECHTSANWÄLTE

Von Christian Drave, LL.M.

Internationale Versicherungsprogramme

Cyberrisiken im internationalen Geschäft versichern

Nahezu täglich berichten Medien von Cybervorfällen. Die Fälle zeigen, dass Cyberrisiken internationalen Charakter und entsprechende Auswirkungen haben. Die Internationalität von Cyberrisiken stellt besondere Anforderungen an den Versicherungsschutz. Der nachfolgende Beitrag geht exemplarisch auf Problemfelder ein, die Versicherungsnehmer bei der Versicherung von Cyberrisiken im Auslandsgeschäft beachten sollten, um Deckungslücken zu vermeiden.

1. KERNFUNKTIONEN DER CYBERVERSICHERUNG

Gegenstand der Cyberversicherung ist die Absicherung von (reinen) Vermögensschäden. Nicht unter den Deckungsschutz fallen Personen-, Sach- und sich daraus ergebende Folgeschäden. Cyberdeckungen sind regelmäßig modular aufgebaut und können durch *drei wesentliche Merkmale bzw. Funktionen* gekennzeichnet werden. Die *Drittschadendeckung* bietet dem Versicherungsnehmer Haftpflichtversicherungsschutz für den Fall, dass ein Dritter den Versicherungsnehmer aufgrund einer Informationssicherheitsverletzung/eines Cybervorfalls auf Schadenersatz in Anspruch nimmt. Die *Eigenschadendeckung* bietet Versicherungsschutz für bestimmte Eigenschäden des Versicherungsnehmers. Hier haben Betriebsunterbrechungsschäden aufgrund der Nichtverfügbarkeit von IT-Systemen oder Daten besondere praktische Relevanz. Als drittes typisches Merkmal umfasst die Cyberversicherung bestimmte *Serviceleistungen* im Schadenfall.[1]

2. ANFORDERUNGEN AN DIE DECKUNG

Die Internationalität von Cyberrisiken stellt für alle drei vorgenannten Kernfunktionen besondere Anforderungen an die Deckung. Die nachfolgendenden Hinweise gehen exemplarisch auf einzelne rechtliche Deckungsaspekte ein.

Szenario 1:

Ein Unternehmen mit Sitz in Deutschland produzierte Regelungstechnik. Diese umfasst eine Software mit Fernwartungsmöglichkeit. Kunden be-

[1] Z. B. IT-Forensik, Wiederherstellung von Daten und Systemen, Krisenkommunikation etc.

finden sich sowohl im Inland als auch im europäischen und außereuropäischen Ausland. Das Unternehmen unterhält eine Cyberversicherung bei einem hiesigen Versicherer. Infolge eines Programmierfehlers der Steuerungssoftware können Hacker auf die von der Versicherungsnehmerin produzierte Steuerungseinheit zugreifen.

Szenario 2:

Wie oben, die Versicherungsnehmerin hat hier allerdings eine ausländische Tochtergesellschaft, die unter der Cyberversicherung mitversichert ist.

2.1 Geltungsbereich des Versicherungsschutzes

Am Markt erhältliche Cyberdeckungen bieten teilweise Versicherungsschutz weltweit. Ist dies der Fall, gilt dieser räumliche Deckungsumfang für alle Leistungselemente (Bausteine/Module). Teilweise beschränken Cyberversicherungsbedingungen aber den Versicherungsschutz geographisch. Beispielsweise regeln die unverbindlichen Musterbedingungen des GDV in Ziffer A 1.-11 AVB Cyber[2]:

> *„Versicherungsschutz besteht für Versicherungsfälle weltweit.*
>
> *Dies gilt jedoch nur, soweit die Ansprüche in EWR-Staaten und nach deren Recht geltend gemacht werden."*

Die Klausel betrifft die Haftpflichtdeckung unter dem Drittschadenbaustein. Sie entspricht Regelungen in anderen Bereichen der Haftpflichtversicherung (Betriebshaftpflichtversicherung, Produkthaftpflichtversicherung, BHV-IT/Nutzer).

Die Klausel bedeutet eine erhebliche Einschränkung des Deckungsschutzes. Grundsätzlich versichert sind unter der Cyberversicherung Schadenersatzansprüche von Vertragspartnern auf Ersatz von Vermögensschäden im vereinbarten Umfang, soweit sie nicht über die gesetzliche Haftpflicht des Versicherungsnehmers hinausgehen und nicht das Interesse des Vertragspartners an einer ordnungsgemäßen Vertragserfüllung betreffen. Vertragsbeziehungen sind besonders haftungsrelevant. Den Versicherungsnehmer treffen nicht nur (möglicherweise nicht versicherbare) Hauptleistungspflichten, sondern umfassende Neben- und Schutzpflichten, insbes. auch bezüglich der Datensicherheit.

Geltungsbereich oft auf Europäischen Wirtschaftsraum beschränkt.

Allein die Tatsache, dass der Versicherungsnehmer wie im *Szenario 1* Kunden im Ausland hat, birgt das Risiko, dass Kunden bei einem vom Versicherungsnehmer zu vertretenden Cyberschaden im außereuropäischen Ausland und ggf. nach ausländischem Recht Ansprüche gegen den Versiche-

[2] Allgemeine Versicherungsbedingungen für die Cyberrisiko-Versicherung, Stand: April 2017.

rungsnehmer geltend machen. Ist zudem – wie in *Szenario 2* – ein im Ausland ansässiges Tochterunternehmen mitversichert, werden dessen Kunden ohnehin vor Ort gegen dieses Unternehmen Ansprüche erheben und eine Auslandsverteidigung auslösen. Dafür bieten die AVB Cyber keinen Versicherungsschutz. Daher besteht von vorneherein das Risiko relevanter Deckungslücken für den Versicherungsnehmer.

Ein erhebliches Risiko besteht auch hinsichtlich einer außervertraglichen (deliktischen) Haftung des Versicherungsnehmers gegenüber Dritten. Im Fokus stehen hier Fälle von massenhaftem Verlust von personenbezogenen Daten. Nach internationalprivatrechtlichen Grundsätzen kann ein betroffener Nutzer regelmäßig an seinem (Wohn)Sitz Ansprüche gegen seinen Versicherungsnehmer erheben (also auch im Ausland).

Verlust personenbezogener Daten kann Haftung in Drittstaaten nach sich ziehen.

Versicherungsnehmer sollten daher sicherstellen, dass der räumliche Geltungsbereich der Cyberdeckung ihrem tatsächlichen Absicherungsbedarf entspricht.

2.2 Haftpflichtschäden: Anrechnung von Abwehrkosten auf die Versicherungssumme

Sieht sich der Versicherungsnehmer nach einem Cybervorfall Schadenersatzansprüchen Dritter ausgesetzt, können weitere Probleme auch bei weltweitem Geltungsbereich des Haftpflichtversicherungsschutzes entstehen.

Die Hauptleistungspflicht des Cyberversicherers unter dem Drittschadenbaustein umfasst (wie die Haftpflichtversicherung generell) die Prüfung der Haftpflichtfrage, die Abwehr unberechtigter Haftpflichtansprüche sowie die Freistellung des Versicherungsnehmers von begründeten Haftpflichtansprüchen.

Problematisch dabei ist, dass Cyberversicherungsbedingungen teilweise vorsehen, dass die Kosten der Anspruchsabwehr bei Auslandschäden auf die Versicherungssumme angerechnet werden. So bestimmt Ziffer A 3.-6.4 AVB Cyber:

> *„Aufwendungen des Versicherers für Kosten der gerichtlichen und außergerichtlichen Abwehr der von einem Dritten im Ausland geltend gemachten Ansprüche, insbesondere Anwalts-, Sachverständigen-, Zeugen- und Gerichtskosten, werden – abweichend von A3-6.3 – als Leistungen auf die Versicherungssumme angerechnet."*

Die Klausel erfasst sämtliche (Arten von) Abwehrkosten. Die Kosten sollen unabhängig davon angerechnet werden, ob die Anspruchsabwehr erfolgreich war oder nicht. Die Klausel unterscheidet auch nicht danach, ob Kosten auf Veranlassung des Versicherers entstanden sind oder nicht. Die Anrechnung erfolgt nach dem Wortlaut ohne Begrenzung der anzurechnenden Kosten – also auch dann, wenn die Abwehrkosten die Versicherungssumme vollständig verbrauchen.

Die Kostenanrechnung nach A 3-6.4 AVB Cyber führt zu einer unangemessenen Benachteiligung der Interessen des Versicherungsnehmers und ist deshalb AGB-rechtlich *unwirksam*, § 307 Abs. 2 Nr. 1 und Abs. 1 S. 1 BGB.

Die Klausel ist eine Leistungsbeschränkung und unterliegt der AGB-rechtlichen Inhaltskontrolle. Nach § 101 Absatz 1 Satz 2 VVG muss der Haftpflichtversicherer bei erfolgloser Anspruchsabwehr den Versicherungsnehmer freistellen und darüber hinaus die Kosten der Anspruchsabwehr tragen und zwar auch und gerade dann, wenn die Freistellung die Versicherungssumme verbraucht. Von diesem gesetzlichen Leitbild[3] weicht die Kostenanrechnungsklausel zulasten des Versicherungsnehmers ab. Daher wird eine unangemessene Benachteiligung und somit eine Unwirksamkeit der Klausel widerleglich vermutet. Jedenfalls die AVB Cyber enthalten keine ausreichenden Kompensationselemente, die diese gesetzliche Vermutung der Unwirksamkeit beseitigen würden. Vielmehr bestätigt eine Gesamtbetrachtung und AGB-rechtliche Interessenabwägung die Unwirksamkeit der Kostenanrechnung im Fall der Auslandsverteidigung.

Die gesetzliche Grundkonzeption von § 101 Absatz 1 Satz 2 VVG entspricht dem Zweck der Haftpflichtversicherung, nämlich dem Vermögensschutz des Versicherungsnehmers. Diesen Vertragszweck gefährdet die unbegrenzte Kostenanrechnung im Fall der Auslandsverteidigung. Denn auch bei erfolgloser Anspruchsabwehr sollen die Kosten auf die Versicherungssumme angerechnet werden und können diese unter Umständen vollständig verbrauchen. Dann muss der Versicherungsnehmer im Ergebnis die Haftpflichtansprüche selbst ausgleichen und erhält – entgegen dem Hauptleistungsversprechen des Versicherers – keine Freistellung. Der versicherungsvertraglich bezweckte Vermögensschutz läuft leer.

Abwehrkostenanrechnung benachteiligt den Versicherungsnehmer unangemessen.

Mit der Kostenanrechnung schmälert der Versicherer einerseits seine Hauptleistungspflicht zur Freistellung von begründeten Ansprüchen. Andererseits verlagert der Versicherer mit der Kostenanrechnung ein Risiko auf den Versicherungsnehmer, das nach Gesetz und Rechtsprechung dem Versicherer zugewiesen[4] ist, denn: *„der Versicherer hat nicht das Recht, die mit der Abwicklung der Haftpflichtansprüche verbundenen Kosten auf den Versicherten abzuwälzen“*.[5] Hinzu kommt, dass die Kostenanrechnungsklausel dem

[3] Zum Leitbildcharakter von § 101 Absatz 2 Satz 1 VVG vgl. Terno, r+s 2013, 577, 579; a.A. Koch, VersR 2016, 1405.

[4] Vgl. etwa Fiedler, Aktuelle Probleme des Versicherungsvertrags-, Versicherungsaufsichts- und Vermittlerrechts, 2013, S. 75.

[5] BGH, NJW 2007, 2258, 2259.

Versicherungsnehmer nicht deutlich macht, in welchem Umfang die Anrechnung erfolgt und welcher Teil der Versicherungssumme ihm noch zur Freistellung verbleibt. Diese Ungewissheit bedeutet für sich einen deutlichen Nachteil für den Versicherungsnehmer.[6]

Die Kostenanrechnung schafft somit für den Versicherungsnehmer gravierende Nachteile, ohne dass die Versicherungsbedingungen demgegenüber eine ausreichende Kompensation vorsähen. Zwar mag ein Interesse des Versicherers an einer Kostenanrechnung bestehen. Dieses Abweichungsinteresse des Versicherers überwiegt aber nicht das schutzwürdige Interesse des Versicherungsnehmers an der Kostentragung durch den Versicherer nach der gesetzlichen Regelung nach § 101 Absatz 2 Satz 1 VVG. Die Kostenanrechnung nach A3-6.4 AVB Cyber ist daher unwirksam.

2.3 Eigenschadendeckung

Problematisch ist auch der weltweite Eigenschadenschutz unter Cyberpolicen. Wird im *Szenario 1* der Versicherungsnehmer Opfer eines Hackerangriffs und kommt es zum Systemausfall, können dem Unternehmen Schäden durch die Betriebsunterbrechung und Kosten der Wiederherstellung von IT-Systemen bzw. Daten entstehen. Der Versicherungsvertrag bietet daher unproblematisch Versicherungsschutz unter dem Eigenschadenbaustein bzw. dem Service-/Kostenbaustein.

[6] Terno r+s 2013, 577, 581.

Trifft der Schaden jedoch das Tochterunternehmen (*Szenario 2*), ist ein im Ausland belegenes Risiko betroffen. Dann stellt sich die Frage der Zulässigkeit des Versicherungsschutzes. Hintergrund ist, dass Staaten es teilweise aufsichtsrechtlich untersagen, dass ein Versicherer ohne Sitz bzw. Niederlassung in jenem Staat dort belegene Risiken versichert (regelmäßig bezeichnet als non-admitted-Problematik). Ob der deutsche Versicherer für die Auslandstochter Versicherungsschutz bieten darf, müssen Versicherungsnehmer und Versicherer bei Abschluss des Cyberversicherungsvertrages prüfen.

Zur Lösung der non-admitted-Problematik entstanden vor über zehn Jahren Ansätze durch die Versicherung des sogenannten Finanzinteresses (Financial Interest Cover, „FInC“). Vereinfacht beschrieben gehen FInC-Konzeptionen davon aus, dass der wirtschaftliche Schaden der Tochter den Wert der Beteiligung mindert, die die Muttergesellschaft (Versicherungsnehmerin) an der Tochter hält. Die Regelungen decken dann das (Finanz)Interesse der Mutter auf Ausgleich ihrer wirtschaftlichen Beeinträchtigung durch den Schaden der Tochter. Dazu fingieren FInC-Klauseln, dass das Finanzinteresse der Mutter in dem Umfang betroffen ist, in dem der Tochter ein Schaden entstand, der versichert wäre, wenn der Schaden im Inland eingetreten wäre (und deshalb versichert wäre). FInC-Klauseln sind in Industrie-

Im Einzelfall könnten FInC-Klauseln Cyberrisiken in Drittstaaten abdecken.

versicherungsverträgen/-programmen gebräuchlich. Allerdings bergen sie Unsicherheiten (z. B. bei Bestimmung und Nachweis des Finanzinteresses bzw. des Schadens) und können als mögliche Umgehungen aufsichtsrechtlicher Vorgaben anderer Staaten problematisch sein. Ob Eigenschäden durch Cyberrisiken im Ausland mit FInC-Klauseln gedeckt werden können, sollten Versicherungsnehmer im Einzelfall prüfen.

2.4 Serviceleistungen im Krisenfall

Keine Lösung bieten FInC-Klauseln für den Service-Baustein unter der Cyberdeckung. Dieser Baustein hat insbesondere für kleine und mittlere Unternehmen, die über keine entsprechenden Kapazitäten verfügen, erhebliche praktische Bedeutung im Schadenfall. Ein Cybervorfall erfordert regelmäßig eine schnelle Krisenreaktion auf unterschiedlichen Ebenen. Dies umfasst Maßnahmen zur Datensicherung, Wiederherstellung von Daten und IT-Systemen des Versicherungsnehmers um Ausfallzeiten zu minimieren. Dazu gehört aber auch eine geeignete Krisenkommunikation, insbesondere in Fällen massenhafter Verluste personenbezogener Daten. Unter dem Service-/Kostenbaustein erbringt der Versicherer diese notwendigen Leistungen (entweder durch eigene Ressourcen des Versicherers oder aber durch vom Versicherer ausgewählte Kooperationspartner).

Lokale Dienstleister sollten an jedem Standort zur Verfügung stehen.

Ist das Tochterunternehmen im Ausland vom Cybervorfall (*Szenario 2*) betroffen und deshalb auf Serviceleistungen angewiesen, hilft eine rein finanzielle Absicherung – zumal regelmäßig mit zeitlicher Verzögerung – über die Muttergesellschaft bzw. eine FInC-Deckung dabei nicht. Darf der Versicherer aber keine Versicherungsleistungen im Ausland erbringen, läuft der Versicherungsschutz unter dem Service-Baustein leer. Derartige Schadenkonstellationen im Ausland erfordern andere Lösungen, die sicherstellen, dass lokale Dienstleister bzw. Netzwerkpartner dem Versicherungsnehmer vor Ort im Schadenfall zur Verfügung stehen.

2.5 Erpressungsgelder

Wird ein Unternehmen Opfer eines Erpressungstrojaners (Ransomware), ist es vor eine Entscheidung gestellt. Um verschlüsselte Daten wieder zu erlangen, fordern die Täter „Lösegeldzahlungen“, zB in Kryptowährungen wie Bitcoin. Insbesondere um Ausfallzeiten zu minimieren, entscheiden sich Unternehmen regelmäßig zur Zahlung, wenngleich nicht in jedem Fall sicher ist, dass nach erfolgter Zahlung die Entschlüsselung der eigenen Daten glückt. Cyberpolicen decken derartige Lösegeldzahlungen teilweise. Teilweise schließen die Policen Lösegeldzahlungen aber auch von der Deckung aus und bleiben damit hinter dem Bedarf der Versicherungsnehmer zurück (z.B. die AVB Cyber in ihrer jetzigen Form nach Ziffer A1-17.1).

Ob und inwieweit Lösegeldzahlungen in rechtlicher Hinsicht versicherbar sind, hängt vom maß-

geblichen Aufsichtsrecht ab. In den meisten europäischen Staaten ist die Versicherung von Erpressungsgeldern zulässig. Die deutsche Versicherungsaufsicht erlaubt – anders als in der Vergangenheit – die Versicherung von Lösegeldzahlungen zusammen mit anderen Risiken in einer Cyberpolice.[7] Der Versicherungsnehmer und der Versicherer sollten jedoch prüfen, ob die Versicherung von Cyber-Lösegeldern in allen Ländern, in denen das Unternehmen IT-Infrastruktur besitzt, rechtlich zulässig ist.

3. FAZIT

Die Internationalität von Cyberrisiken erfordert eine genaue Analyse der grenzüberschreitenden Versicherbarkeit und des Deckungsumfangs im internationalen Geschäft. Versicherungsnehmer sollten bei Abschluss von Cyberdeckungen sicherstellen, dass und wie der Versicherer im Schadenfall Leistungen unter den einzelnen Deckungsbausteinen der Cyberpolice erbringt – auch außerhalb von EU und EWR. Auf die Möglichkeit der Einschaltung von Servicepartnern im Krisenfall sollten vor allem mittelständische Versicherungsnehmer bei Abschluss einer Cyberpolice besonderes Augenmerk legen.

Diesen Beitrag veröffentlichte die Zeitschrift *Die Versicherungspraxis* in ihrer Ausgabe 11/2018.

Für Rückfragen steht Ihnen der Autor gern zur Verfügung:

Christian Drave, LL.M.
Rechtsanwalt
Master of Insurance Law

WILHELM Partnerschaft von Rechtsanwälten mbB

Tel: +49 211 687746 43
christian.drave@wilhelm-rae.de

[7] Vgl. die Meldung der BaFin vom 15. September 2017, abrufbar unter: https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Meldung/2017/meldung_170915_loesegeldversicherung.html.

WILHELM

RECHTSANWÄLTE

Über uns:

Die Sozietät Wilhelm ist spezialisiert auf die Beratung von Unternehmen und deren Entscheidungsträgern in kritischen Situationen – vom Großschaden über die persönliche Inanspruchnahme bis hin zum Compliance-Verstoß im Unternehmen. Sechzehn Berufsträger an zwei Standorten (Düsseldorf und Berlin) vereinen hierfür Expertise aus den Bereichen Versicherung, Haftung, Wirtschaftsstrafrecht und Gesellschaftsrecht. Weltweit kooperiert die Sozietät mit Kanzleien unter anderem in Chicago, New York, London, Paris, Rom, Warschau und Brüssel. Mit seinen internationalen Kooperationspartnern bietet Wilhelm die Expertise zur Lösung grenzüberschreitender Haftungs- und Deckungsstreitigkeiten, M&A-Transaktionen sowie internationaler Großprojekte.

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

+ 49 (0)30.81 72 732-0
+ 49 (0)30.81 72 732-0

berlin@wilhelm-rae.de

JUVE 2017 AWARDS
Kanzlei des Jahres für Versicherungsrecht