Rechtliche Stolpersteine bei der Versicherung von Cyberrisiken

Dr. iur. Nicolas Bracher, LL.M.
Wenger & Vieli AG

Nicolas Bracher ist als Rechtsanwalt sowohl beratend als auch prozessierend für Unternehmen und Privatpersonen im Privat- und Wirtschaftsrecht tätig. Zu seinen Spezialgebieten zählt die Beratung und Prozessführung im Bereich Financial Services. Er hat mehrere wissenschaftliche Publikationen zum Wirtschafts-, Zivilprozess- und Datenschutzrecht verfasst und an der Queen Mary University in London einen LL.M. im Versicherungsrecht erworben.

Einleitung

Das Thema Cybersecurity rückt mehr und mehr in den Fokus der öffentlichen Aufmerksamkeit. Medienberichte über kleinere und grössere Cyberattacken und sonstige Pannen im Cyberspace häufen sich und führen uns mittlerweile fast täglich die neuen Bedrohungen der digitalen Welt vor Augen.

Ein wichtiger Bestandteil des Managements von Cyberrisiken kann deren Transfer an eine Versicherung sein. Weil Versicherungen ein Rechtsprodukt sind, hängt die Effizienz entsprechender Versicherungslösungen entscheidend von juristischen Fragestellungen ab. In den USA sind spezifische Cyberpolicen bereits weit verbreitet. Die dortigen Erfahrungen haben gezeigt, dass die Deckungslimiten solcher Policen bei grösseren Schadenereignissen aufgrund auch in der Schweiz verwendeter Vertragsklauseln sehr rasch erschöpft waren, sodass ein Grossteil der vermeintlich versicherten Schäden ungedeckt blieb. Der vorliegende Beitrag zeigt, nach einer einführenden Übersicht zu den relevanten Risiken und den angebotenen Versicherungslösungen, die wichtigsten juristischen Stolpersteine bei der Versicherung von Cyberrisiken auf.

Was sind Cyberrisiken?

Der Begriff Cyberrisk ist nicht eindeutig definiert. Gemäss einer aktuellen Studie des Instituts für Versicherungswirtschaft (IVW) der Universität St. Gallen («Cyber Risk: Risikomanagement und Versicherbarkeit», St. Gallen 2015) bezieht er sich auf eine Vielzahl potenzieller Risiken, die im Zusammenhang mit der Technologie oder mit Informationen eines Unternehmens stehen. Darunter fallen so unterschiedliche Vorfälle wie Verluste durch Cyberkriminalität oder Cyberterrorismus, unbeabsichtigter oder versehentlicher Verlust von eigenen oder fremden Daten, physischer Systemverlust sowie Haftbarkeit für Onlineaktivitäten und Aussagen in E-Mails. So vielfältig wie die Risiken selbst sind auch die daraus potenziell resultierenden Schäden: Die Bandbreite reicht von direkt messbaren Kosten wie Wiederherstellungskosten bei Datenverlusten, Lösegeldzahlungen bei Erpressungen, vertraglichen Schadenersatz- und Strafzahlungen gegenüber Dritten, Bussen und Rechtskosten bei Datenschutzrechtsverletzungen oder Ertragsausfällen bei Betriebsunterbrüchen bis hin zu indirekten, nur schwer messbaren Kosten wie Verlusten durch Reputationsschäden oder Marktwertverlusten bei einem publik gewordenen Negativereignis. Diese Aufzählung umfasst nur die häufigsten in diesem Zusammenhang genannten Risiken und Schäden und ist nicht abschliessend.

Die Kategorisierung von Cyberrisiken anhand ihrer jeweiligen Ursache ermöglicht einen systematischen Überblick über die potenziellen Bedrohungen. Im Fokus der öffentlichen Aufmerksamkeit stehen in letzter Zeit primär Risiken von Hackerangriffen durch Cyberkriminelle und -terroristen oder gewisse (halb-)staatliche Akteure. Das Spektrum der Ursachen von Cyberrisiken ist allerdings breiter und umfasst auch nicht deliktische Hintergründe wie Naturgefahren oder menschliches und technisches Versagen. In Anlehnung an die vorgenannte Studie des IVW können dabei Kategorien unterschieden werden (vgl. Tabelle Kategorisierung von Cyberrisiken anhand der Ursachen).

Die Quelle von Cyberrisiken kann in den meisten der vorgenannten Fälle sowohl innerhalb als auch ausserhalb des Unternehmens liegen. Dies gilt namentlich für deliktische Aktivitäten, also Straftaten oder zivilrechtlich unerlaubte Handlungen (z.B. nicht strafbare Markenrechtsverletzungen). Deren Urheber können nämlich nicht nur Aussenstehende, sondern ebenso gut auch eigene Mitarbeitende oder solche von Vertragspartnern wie Auftragnehmern oder Auftraggebern sein. Ähnliches gilt in Bezug auf technisches und menschliches Versagen. Auch dieses kann seinen Ursprung im Unternehmen selbst oder ausserhalb, bei Vertragspartnern oder weiteren Drittparteien haben.

Die saubere Analyse der potenziellen Risikoursachen und -quellen ist beim Abschluss einer Versicherung zur Deckung von Cyberrisiken von entscheidender Bedeutung, weil der Versicherungsschutz regelmässig von diesen Faktoren abhängt. Denn am Markt versicherbar sind aktuell nur spezifizierte Einzelrisiken.

Ebenso wichtig wie die Identifikation der potenziellen Risiken ist die Abschätzung der daraus drohenden Konsequenzen und Schäden. Mit Blick auf die Versicherbarkeit kann dabei zwischen Eigenschäden einerseits und Haftungsrisiken für Drittschäden andererseits differenziert werden, wobei zwischen Schadenskategorien unterschieden werden kann (vgl. Tabelle Kategorisierung der aus Cyberrisiken drohenden Schäden).

Kategorisierung von Cyberrisiken anhand der Ursachen

Ursachen	Beispiele resultierender Bedrohungen und Risiken
I. Nicht deliktische	
Höhere Gewalt	Verluste im Zuge von Naturkatastrophen (z.B. Datenverlust bei katastrophenbedingten Stromausfällen; Zerstörung von Computern oder Servern durch Brand oder Überschwemmung)
Technisches Versagen	Hardwareversagen mit Datenverlust; Softwarefehler
Menschliches Versagen	Versehentliches Veröffentlichen von Informationen; versehentlicher Verlust von mobilen Datenträgern
II. Deliktische	
Physische Angriffe	Physischer Datendiebstahl durch Entwendung von Datenträgern
Hackerangriffe	Einsatz von Malware (z.B. Viren, Würmer, Trojaner) zum Zweck der Spionage oder der Sabotage; Lahmlegen von Systemen mittels sogenannter Distributed-Denial-of-Service-Attacken (DDoS-Attacken)
Multi-Media-Delikte	Verleumdungen, Datenschutzverletzungen, Verletzung von geistigem Eigentum oder unlauterer Wettbewerb über Social Media

In Anlehnung an die erwähnte Studie des IVW sowie die im Jahr 2012 publizierte Studie «Review of Recent Developments in the Cyber Insurance Market» der britischen Association of Insurance and Risk Managers in Industry and Commerce (AIRMIC)

Kategorisierung der aus Cyberrisiken drohenden Schäden

Schadenskategorie	Beispiele
Eigenschäden	■ Kosten zur Wiederherstellung und Ersatzbeschaffung bei Datenverlust ■ Ertragsausfälle und Zusatzkosten bei Betriebsunterbrechungen ■ Direkte finanzielle Verluste durch Diebstahl von Geld, digitalen Vermögenswerten, Fabrikations- oder Geschäftsgeheimnissen ■ Erpressungszahlungen (Cyber Extortion) ■ Reputationsschäden bei publik gewordenen Datenrechtsverletzungen
Haftungsrisiken	■ Haftbarkeit für Drittschäden bei Datenschutzrechtsverletzungen (inkl. Beratungs- und Rechtskosten bei regulatorischen Verfahren, Bussen, PR-Kosten sowie Kosten für forensische Untersuchungen und für die gesetzlich vorgeschriebene Benachrichtigung Betroffener bei Datenschutzverstössen [sog. Data Breach Notifications]) ■ Haftbarkeit für Drittschäden aus Onlineaktivitäten, etwa bei Verletzungen oder widerrechtlicher Verwendung von geistigem Eigentum oder lauterkeitsrechtlichen Bestimmungen sowie bei Ehrverletzungen ■ Haftbarkeit für Drittschäden, die durch die eigenen Systeme oder Mitarbeiter (z.B. durch unbewusstes Einschleusen von Malware) an Daten oder Systemen Dritter entstanden sind (z.B. Wiederherstellungs-, Ersatzbeschaffungskosten, Ertragsausfälle) ■ Haftbarkeit für Drittschäden, die aus der Beeinträchtigung oder Verwehrung des berechtigten Zugangs von Kunden resultieren

In Anlehnung an die erwähnte Studie des IVW sowie die im Jahr 2012 publizierte Studie «Review of Recent Developments in the Cyber Insurance Market» der britischen Association of Insurance and Risk Managers in Industry and Commerce (AIRMIC)

Versicherungsprodukte und Deckungskonzepte

Cyberrisiken sind grossmehrheitlich neuere Erscheinungen, die in den letzten Jahren primär durch die zunehmende Digitalisierung und globale Vernetzung vieler Lebensbereiche entstanden sind. Ein weiterer wichtiger Entstehungsfaktor ist die exponenziell gestiegene Bearbeitung von Personendaten (insbesondere Kundendaten) durch Unternehmen und eine dadurch ausgelöste markante Verschärfung von Datenschutzbestimmungen in zahlreichen Ländern.

Aufgrund der Neuartigkeit der meisten Cyberrisiken hat sich bis anhin in der Schweiz, wie etwa auch in Deutschland, kein Branchenstandard für die Bedingungen von deren Versicherung entwickelt. Laut Gesamtverband der Deutschen Versicherungswirtschaft sollte sich dies aber für Deutschland noch im laufenden Jahr ändern. Aufgrund des bislang fehlenden Standards sind die Angebote der verschiedenen Versicherer oft unterschiedlich konzipiert und verwenden keine einheitliche Terminologie, sodass sie teilweise nur schwer vergleichbar sind.

In allgemeiner Weise können immerhin folgende Aussagen zum Angebot an Versicherungsprodukten gemacht werden:

- Policen, die ein Unternehmen umfassend gegen alle Arten von Cyberrisiken abdecken, existieren zurzeit nicht. Auch die im Markt angebotenen spezifischen Versicherungsprodukte zur Deckung von Cyberrisiken (im Folgenden: Cyberpolicen) bieten keine Allgefahrendeckung, sondern nur Versicherungsschutz gegen definierte Einzelrisiken.
- Die heute erhältlichen speziellen Cyberpolicen beziehen sich primär auf Risiken im Zusammen-

hang mit Cyberkriminalität und Datenschutzrechtsverletzungen. Sie bestehen meist aus verschiedenen Deckungsbausteinen und enthalten sowohl Elemente der Eigenschaden- als auch der Haftpflichtversicherung. Als Haftpflichtversicherung decken solche Policen regelmässig nur reine Vermögensschäden und keine Sach- oder Personenschäden. Als Zusatzleistungen werden häufig auch Dienstleistungspakete zu Risiko- und Krisenmanagement-Services durch spezialisierte Unternehmen wie IT-Forensiker oder PR-Agenturen angeboten.

- Nebst speziellen Cyberpolicen bieten gewisse Versicherer auch andere, nicht primär auf Cyberrisiken ausgerichtete Versicherungsprodukte oder Zusatzdeckungen zu solchen an, die einzelne spezifische Cyberrisiken decken. Zu nennen sind hier beispielsweise EDV-Anlagen- oder Vertrauensschadenversicherungen (zum Schutz gegen Vermögensschaden aus unerlaubten Handlungen von Mitarbeitenden und sonstigen Vertrauenspersonen eines Unternehmens), die teilweise Deckungskomponenten enthalten, die sich auch in typischen Cyberpolicen finden (insb. Wiederherstellungskosten bei Datenverlust; Versicherungsschutz gegen Hackerangriffe).

Individuelle Bedarfsanalyse

Obwohl das Management von Cyberrisiken heute praktisch jedes Unternehmen betrifft, ist der konkrete Versicherungsbedarf aufgrund des grossen Spektrums an Risiken und daraus resultierenden Schäden sehr individuell: Ein Zulieferbetrieb in der Maschinenindustrie hat andere Deckungsbedürfnisse als der Betreiber eines Online-Shops, der wieder andere hat als ein Finanzinstitut. Gerade weil die am Markt angebotenen Versicherungsprodukte – die vereinzelt sogar auf spezifische Branchenbedürfnisse zugeschnitten sind – unterschiedlich konzipiert sind und jeweils nur Einzelrisiken abdecken, ist eine individuelle Bedarfsanalyse vor Abschluss einer Versicherung zur Deckung von Cyberrisiken zentral.

Wichtiger Bestandteil dieser Analyse ist auch der bestehende Versicherungsschutz, zumal dieser im Einzelfall bereits ausreichend sein mag oder durch eine bedarfsgerechte Zusatzdeckung ergänzt werden kann. Dies gilt insbesondere dann, wenn bereits Policen bestehen, die typischerweise auch Cyberrisikokomponenten enthalten (z.B. EDV-Anlagen-Versicherung mit Zusatzdeckung; Vertrauensschadensversicherung). In solchen Fällen ist umgekehrt aber auch zu beachten, dass die bestehende Police möglicherweise nicht einen vergleichbar guten Schutz bietet wie spezifische Cyberpolicen. Als Beispiel wären hier Vertrauensschadensversicherungen zu nennen, die nur Schutz bei kriminellen Aktivitäten eigener Angestellter gewähren, nicht hingegen bei entsprechenden Aktivitäten von Auftragnehmern und deren Mitarbeitern, die Zugang zu den Daten oder Systemen des Versicherten haben.

Nicht zu unterschätzen sind sowohl bei der Risikobeurteilung im Rahmen des Risk-Managements als auch bei der individuellen Bedarfsanalyse die besonderen Herausforderungen, die sich aus den andauernden technologischen und rechtlichen Entwicklungen ergeben. Diese waren in den letzten Jahren stete Quellen zusätzlicher Cyberrisiken für Unternehmen. Was die rechtlichen Entwicklungen betrifft, ist primär auf die im Jahr 2018 in Kraft tretende Verschärfung des Datenschutzrechts in der Europäischen Union hinzuweisen, in deren Rahmen unter anderem umfangreiche Meldepflichten und einschneidende Sanktionen (insb. Bussen in Millionenhöhe) bei Datenschutzverletzungen durch Unternehmen eingeführt werden, von denen auch viele Schweizer Unternehmen erfasst sein können. Im Rahmen einer geplanten Revision des schweizerischen Datenschutzgesetzes werden ähnliche Regeln in den kommenden Jahren mit grösster Wahrscheinlichkeit auch in der Schweiz eingeführt werden.

Erste Informationsquellen für eine Bedarfsanalyse können auf dem Internet abrufbare Cyber-Risiko-Tests und Self-Assessment-Tools sowie öffentlich zugängliche Studien und Produktvergleiche sein, wie die bereits genannten des IVW sowie der britischen AIRMIC. Die Studie des IVW enthält beispielsweise eine vergleichende Übersicht und Beschrei-

bung von mehreren in der Schweiz im Jahr 2015 angebotenen Cyberpolicen. Aufgrund der Komplexität der Thematik und der Unübersichtlichkeit des Marktes wird es für viele Unternehmen indessen angezeigt sein, sich bei der Bedarfsanalyse und allfälligen Produktevaluation durch spezialisierte Dienstleister aus den Bereichen Risk-Management, Versicherungsvermittlung oder Versicherungsberatung unterstützen zu lassen.

Rechtliche Stolpersteine

Auch aus rechtlicher Sicht birgt die Versicherung von Cyberrisiken einige Tücken. Diese betreffen sowohl vertragsrechtliche Fragen als auch solche aus anderen Rechtgebieten.

Eine Grundproblematik liegt für Einkäufer von Versicherungsdeckung zunächst im bereits erwähnten Fehlen eines Branchenstandards hinsichtlich der Versicherungsbedingungen und der damit einhergehenden Unübersichtlichkeit der Angebote. Problematisch erscheint die Uneinheitlichkeit der Definitionen und Konzepte insbesondere im Hinblick auf die Vermeidung von Deckungslücken und Mehrfachversicherungen. Zur Illustration kann auf folgende Beispiele hingewiesen werden:

- Versicherungsfalldefinitionen können sehr eng formuliert sein. Dies gilt nicht nur in Bezug auf Cyberpolicen, sondern gerade auch bei den bereits erwähnten anderweitigen Produkten mit Cyberrisikokomponenten. So kommt es beispielsweise vor, dass ausdrücklich nur Schäden aus «zielgerichteten» Angriffen erfasst werden, was Schäden aus nicht zielgerichtet gegen das versicherte Unternehmen eingesetzter, sondern eine unbestimmte Vielzahl von Usern treffende Malware ausschliessen dürfte. Unerwünschte Einschränkungen des Versicherungsschutzes können sich auch aus anderweitigen restriktiven Umschreibungen der versicherten Gefahren ergeben. Dies ist etwa dann der Fall, wenn nur Schäden aus «Straftaten» oder «strafbaren Handlungen» von Mitarbeitenden gedeckt sind, was solche aus rein zivilrechtlich unerlaubten Handlungen ausschliesst (z.B. unlauterer Wettbewerb oder Verletzung von Markenrechten). Ähnliche Einschränkungen ergeben sich, wenn nur vorsätzliche Handlungen von Mitarbeitenden gedeckt sind, nicht aber Schäden aus blossem Versehen.
- Ausschlussklauseln ist auch in diesem Bereich gebührende Aufmerksamkeit zu schenken. Sie sehen regelmässig Deckungsausschlüsse vor, wenn keine fortlaufend aktualisierten Sicherheitsmassnahmen (Firewall, Einsatz von Anti-Viren-Schutz-Software) getroffen werden oder wenn nicht genügend leistungsfähige, d.h. veraltete Hard- oder Software benützt wird. Weil die Einhaltung dieser Anforderungen für Versicherungsnehmer mit hohen Kosten verbunden sein kann, besteht bezüglich der Auslegung der Tragweite solcher Klauseln einiges Konfliktpotenzial. Ebenso interpretationsbedürftig können weitere gängige Ausschlussklauseln sein. So sind etwa Schäden aus kriegerischen Ereignissen und Terror standardmässig vom Versicherungsschutz ausgeschlossen, wobei unklar erscheint, ob und inwieweit sich diese Ausschlüsse auch auf verwandte Phänomene im Cyberspace beziehen (z.B. Hackerangriff durch einen ausländischen Geheimdienst; Einsatz von Logikbomben).
- Gerade weil sich die Deckungskonzepte unterscheiden, sollte beim Einkauf neuer Versicherungsdeckungen im Bereich der Cyberrisiken ein Vergleich mit bestehenden Policen vorgenommen werden, um Deckungslücken und Mehrfachversicherungen zu vermeiden. Letztere können nicht «bloss» zu mehrfachen Prämienzahlungen führen, sondern im ungünstigsten Fall auch dazu, dass eine Deckung ganz entfällt (sog. qualifizierte Subsidiärklauseln).

Nicht nur die Bestimmungen zu Versicherungsfällen und Ausschlüssen, sondern auch weitere Klauseln können im Schadenfall einen erheblichen Einfluss auf den effektiven Deckungsumfang haben. Auch hier kann zu Illustrationszwecken auf relevante Beispiele verwiesen werden:

- Die Allgemeinen Versicherungsbedingungen enthalten regelmässig mehr oder weni-

ger umfangreiche Verhaltenspflichten der Versicherten (sog. Obliegenheiten). Wichtige Obliegenheiten bei der Versicherung von Cyberrisiken sind etwa Sicherungspflichten (z.B. regelmässiges Erstellen von «Backups») oder Anzeigepflichten bei Gefahrveränderungen sowie bei der Entdeckung von Schadensfällen. Die Rechtsfolgen einer Verletzung solcher Obliegenheiten variieren je nach Produkt und reichen von Leistungskürzungen bis zum gänzlichen Verlust des Anspruchs auf Versicherungsleistungen.

- Erhebliche Unterschiede können auch hinsichtlich des örtlichen und zeitlichen Geltungsbereichs der Police bestehen. In Bezug auf den örtlichen Geltungsbereich ist beispielsweise bei vielen Versicherungen eine weltweite Deckung vorgesehen. Die Musterbedingungen des SVV für die Versicherung von EDV-Anlagen beschränken die Deckung örtlich allerdings auf einen im Versicherungsvertrag bezeichneten Versicherungsort in der Schweiz oder dem Fürstentum Liechtenstein. Bei Zusatzdeckungen betreffend Datensicherheit (z.B. zur Deckung von Schäden bei Hackerangriffen) zu solchen Policen sollte unbedingt geprüft werden, ob der örtliche Geltungsbereich erweitert wird. Wo dies nicht der Fall ist, muss grundsätzlich davon ausgegangen werden, dass der Verlust von Daten, die in einer Cloud gespeichert sind, nicht vom Versicherungsschutz erfasst wird.
- Potenziell sehr erhebliche Einschränkungen des Deckungsumfangs können sich sodann gerade bei der Versicherung von Cyberrisiken mit hohem Schadenpotenzial auch aus sogenannten Serienschadenklauseln ergeben. Diese Klauseln werden von den meisten Versicherern in einschlägigen Policen verwendet, um die Risiken kalkulierbar zu machen und die Leistungspflicht zu begrenzen. Konkret fassen solche Klauseln mehrere Versicherungsfälle zu einem Versicherungsfall oder mehrere Schäden zu einem Schaden zusammen. Werden beispielsweise bei einem Hackerangriff die Kreditkartendaten von 1000 Kunden gestohlen, können die daraus resultierenden Drittschäden nur als ein Schaden und nicht als 1000 Schäden gelten, mit der Folge, dass die Deckungslimite nur einmal für alle Haftungsansprüche gemeinsam und nicht für jeden einzelnen Haftungsanspruch separat zur Anwendung kommt. Es liegt auf der Hand, dass die konkrete Ausgestaltung solcher Serienschadenklauseln und ihr Zusammenspiel mit Selbstbehalten, Deckungs- und Sublimiten beim Versicherungsabschluss genau geprüft werden sollten. In den USA gab es wie eingangs erwähnt bereits Fälle, in denen die effektive Deckung aus bestehenden Cyberpolicen wegen solcher Klauseln derart gering war, dass die Versicherungsnehmer bei Schadensereignissen versuchten, zusätzlich auf die normale Betriebshaftpflichtversicherung zurückzugreifen.

Aus juristischer Perspektive gilt bei der Versicherung von Cyberrisiken ein besonderes Augenmerk den bereits erwähnten zusätzlichen Risiken, die sich aus der Vernetzung von IT-Systemen im Rahmen von Outsourcing-Lösungen und sonstigen arbeitsteiligen Kooperationen mit anderen Unternehmen oder sonstigen Auftragnehmern (z.B. Freelancer) ergeben. Führen solche Kooperationen dazu, dass Mitarbeitende von Kooperationspartnern Zugang zu den Systemen des Versicherungsnehmers oder Zugriff auf dessen Daten haben oder dass Daten auf externe Datenträger ausgelagert werden (Cloud Computing; mobile Geräte von freien Mitarbeitern), ist zu prüfen, inwieweit die daraus resultierenden zusätzlichen Risikoexpositionen von einer konkreten Police erfasst sind.

Die Angebote sind hier wiederum individuell und produktspezifisch: Bei gewissen Policen sind nebst den Handlungen eigener Mitarbeiter auch solche von Freelancern, in den Betrieb eingegliederten Mitarbeitenden von Zeitarbeitsfirmen und Tochtergesellschaften eingeschlossen. Andere Policen gehen weiter und schliessen auch Handlungen von Mitarbeitenden externer Dienstleister in arbeitnehmerähnlicher Stellung (z.B. Reinigungs- oder Sicherheitspersonal) oder in

sensiblen Bereichen (IT-Dienstleister) in den Versicherungsschutz ein.

Nebst der Definition des erfassten Personenkreises sollte etwa auch darauf geachtet werden, welche Handlungen solcher Personen konkret gedeckt sind (besteht Deckung nur für deliktische Handlungen oder auch für blosses «menschliches Versagen»?), worin genau der Versicherungsschutz besteht (deckt die Versicherung die persönliche Haftpflicht dieser Personen selbst oder die Hilfspersonenhaftung des versicherten Unternehmens für deren Handlungen?), welche Obliegenheiten solche Personen treffen und welche Datenträger unter den Versicherungsschutz fallen (z.B. Mobilgeräte von Mitarbeitenden). Auch diesbezüglich bestehen erhebliche Unterschiede. Zudem sind die in den Allgemeinen Versicherungsbedingungen verwendeten Begriffe mitunter interpretationsbedürftig. So kann sich etwa fragen, ob der Begriff «Computer des Versicherten» auch das vom Unternehmen zur Verfügung gestellte Smartphone des Mitarbeitenden umfasst. In solchen Fällen lohnen sich unter Umständen Präzisierungen oder Ergänzungen in Individualabreden.

Nebst den behandelten vertragsrechtlichen Aspekten stellen sich bei der Versicherung von Cyberrisiken teilweise weitere juristische Fragen. Diese betreffen die grundsätzliche rechtliche Zulässigkeit der Versicherung einiger besonderer Risiken im Zusammenhang mit Rechtsverletzungen und Cyberkriminalität.

Zu nennen ist hier zunächst die Versicherbarkeit von Bussen und entsprechenden Verfahrenskosten bei regulatorischen Verfahren, namentlich im Zusammenhang mit Datenschutzverletzungen. Die Deckung entsprechender Kosten wird teilweise als Baustein spezifischer Cyberpolicen angeboten. Als Einkäufer muss man sich bewusst sein, dass namentlich die Abwälzung von Bussen, teilweise aber sogar diejenige von Rechtskosten im Zusammenhang mit entsprechenden Verfahren, auf eine Versicherung in zahlreichen Ländern unzulässig ist. Der vertragliche Anspruch auf entsprechende Versicherungsleistung ist dann rechtlich nicht durchsetzbar. In der Schweiz ist die diesbezügliche Rechtslage nicht restlos geklärt. Bussen mit Strafcharakter gelten nach dem Bundesgericht nicht als ersatzfähiger Schaden und sind dementsprechend grundsätzlich nicht versicherbar. Diese Rechtsprechung gilt allerdings nicht ausnahmslos, und gerade bei administrativen Bussen im Unternehmensstrafrecht besteht Raum für Ausnahmen. Angesichts der anstehenden Einführung scharfer Sanktionen im europäischen und schweizerischen Datenschutzrecht erscheint die Klärung dieser Frage von erheblicher praktischer Relevanz. Bis dahin ist beim Einkauf entsprechender Produkte grösste Zurückhaltung und Vorsicht geboten.

Juristisch diskutabel ist auch die Zulässigkeit der Versicherung von Lösegeldzahlungen bei Cybererpressung, einem weiteren typischen Baustein von Cyberpolicen. Die Versicherung dieses Risikos könnte nämlich als sittenwidrig angesehen werden, zumal Lösegeldzahlungen weitere kriminelle und terroristische Aktivitäten provozieren und auch finanzieren können. Es besteht deshalb ein gewisses rechtliches Risiko, dass entsprechende Policen zivilrechtlich nichtig sind. International tätige Unternehmen müssen sich ohnehin bewusst sein, dass die Zahlung solcher Lösegelder in anderen Ländern, namentlich im angelsächsischen Raum, gegen gesetzliche Bestimmungen zur Bekämpfung der Geldwäscherei und der Terrorismusfinanzierung verstossen kann. Auch beim Einkauf solcher Produkte ist somit entsprechende Vorsicht walten zu lassen.

Kernaussagen

- Die im Markt aktuell erhältlichen Versicherungslösungen decken jeweils nur Teile des breiten Spektrums an Cyberrisiken ab. Deshalb ist eine sorgfältige individuelle Bedarfsanalyse zentral.
- Aufgrund uneinheitlicher Deckungskonzepte und Versicherungsbedingungen besteht eine erhebliche Gefahr von Deckungslücken und Mehrfachversicherungen. Es empfiehlt sich daher eine vergleichende Analyse verschiedener Produkte unter Einbezug des bestehenden Versicherungsschutzes.
- Wichtige Einschränkungen des Versicherungsschutzes können sich auch aus vertraglichen Verhaltenspflichten des Versicherten oder sogenannten Serienschadenklauseln ergeben.
- Besonderes Augenmerk sollte dem Einbezug von Risiken gewidmet werden, die sich aus der Vernetzung von IT-Systemen im Rahmen von Outsourcing-Lösungen und sonstigen arbeitsteiligen Kooperationen mit anderen Unternehmen ergeben.

Das Handbuch für erfolgreiche Manager.

Mit Experten-Wissen zu brisanten Themen wie Steuern, Compliance, Aktienrecht, M&A, Personal und Wirtschaftsdelikten.

- ✓ Aktueller Überblick zu den laufenden Entwicklungen
- ✓ Praxisnahe Darstellungen
- ✓ Mit Tabellen, Checklisten und Kernaussagen für die schnelle Informationsaufnahme

schulthess manager handbuch 2017
280 Seiten, gebunden, ISBN 978-3-7255-7618-0, CHF 79.--

Schulthess
MANAGEMENT