



»Risikotransfer« als fester Bestandteil eines umfassenden Riskmanagements

## IT: No Risk is Fun!

Technisch machbar ist heute vieles. Mit dem immer weiterwachsenden Einfluss der IT wächst auch die Störanfälligkeit für unsere Gesellschaft.

**K**aum ein Lebensbereich in unserer Gesellschaft und in unserer Arbeitswelt, der heute ohne eine funktionierende IT noch vorstellbar wäre. Ob Forschung und Entwicklung, ausgefeilte Office-Anwendungen in der Verwaltung, die Verknüpfung der Systeme in der Produktion im Rahmen von Industrie 4.0, die komplette weltweite Logistik, Lieferkettenmanagement – ohne funktionierende IT-Systeme steht heute alles still. Wer dann nach Feierabend in sein »Smart Home« kommt, hängt wieder an den IT-Funktionalitäten. Und die Entwicklung kennt kein Halten: So stehen das autonome Fahren sowie die künstliche Intelligenz (KI) heute ganz oben auf der Innovationsliste. Kein Wunder also, dass die IT-Branche boomt und diese Unternehmen offensichtlich weitgehend immun gegen Wirtschaftsschwankungen sind.

Doch neben der Begeisterung für das technisch Machbare entwickelt sich eine enorme gesellschaftspolitische Verantwortung der Branche für die Sicherheit der Produkte und Leistungen. Besonders dramatische Folgen könnte eine fehlerhafte Software insbesondere bei Unternehmen aus dem Bereich »Kritische Infrastrukturen« haben. Eine rasante Entwicklung der Cyberkriminalität führt zu ständig wechselnden Bedrohungssituationen, zugleich verschärft die Politik durch immer neue Reglementierungen und Strafnormen, Stichworte DSGVO und Geschäftsgeheimnisgesetz GeschGehG, die Haftungssituation der Unternehmen. Auch ein noch so aufwendiges IT-Sicherheitsmanagement bietet keinen hundertprozentigen Schutz.

Hinzu kommt, dass von Seiten der Rechtsabteilungen bei großen Industrieunternehmen die IT-Dienstleister durch allzu einseitige Haftungsvereinbarungen zusätzlich unter Druck gesetzt werden. Gerade im Zusammenhang mit den zitierten wachsenden Cybercrime-Bedrohungsszenarien setzt sich zunehmend die Einsicht durch, dass ein umfassendes Riskmanagement im Bereich der IT-Unternehmen zwingend erforderlich ist. Vergleichbar dem Brandschutz in der Industrie, sind auch bei IT-Dienstleistern technische, personelle, aber auch organisatorische Maßnahmen notwendig. In welchem Umfang IT-Unternehmen entsprechende Sicherheitsmaßnahmen umsetzen, liegt in deren eigenem Verantwortungsbereich, flankiert durch entsprechende gesetzliche Auflagen und Forderungen beziehungsweise wirtschaftliche und rechtliche Rahmenbedingungen.

**Doch was tun, wenn alle IT-Sicherheitsmaßnahmen ins Leere laufen?** Ein beträchtlicher oder gar existenzbedrohender Schaden für das Unternehmen wäre die Folge. Im schlimmsten Fall gepaart mit weitergehenden Schäden für den einzelnen Kunden oder ganzen Bevölkerungsgruppen. Auch hier liegt der Vergleich zum Brandschutz nahe, denn dafür steht der sogenannte Risikotransfer in Form von geeigneten Versicherungspolicen etwa gegen Haftungs- oder Cybercrime-Risiken. Allerdings begibt sich hierbei das Management auf unsicheres Gelände, da auf externe Dienstleistungen gesetzt wird, die in ihrer Vielfalt an Angeboten und Spezialprodukten kaum transparent und in der Qualität wenig verifizierbar sind.

Eine gute Nachricht für alle IT-Unternehmen vorweg: In nahezu keinem anderen Segment wie in der IT-Branche finden sich heute im Bereich der Vermögensschadenhaftpflicht so viele Deckungserweiterungen über die reine, üblicherweise versicherbare gesetzliche Haftung hinaus.

Doch gerade die Komplexität der Haftungsrisiken und die sich ständig immer schneller wandelnden Rahmenbedingungen durch neue Technologien treiben die Versicherer und Berater vor sich her. Objektive Versicherungsvergleiche gibt es nicht, einerseits weil die bunte Welt der Versicherungsklauseln Vergleiche nahezu unmöglich macht, andererseits weil es nur sehr wenige spezialisierte Anbieter gibt, welche wirklich das Verständnis für die Branchenrisiken haben und zugleich in der Lage sind, daraus einen individuellen, flexibel anpass-

**7** **Versicherungsverantwortliche in IT-Unternehmen können davon ausgehen, dass die überwiegende Zahl ihrer Haftpflicht- und Cyberpolicen mehr oder weniger gravierende Mängel aufweisen.**

baren und trotzdem bezahlbaren Risikoschutz zu kreieren. So bleibt den allermeisten Versicherungsverantwortlichen in den Unternehmen als Entscheidungsgrundlage die Höhe der Prämie und ein subjektives Vertrauen in die Fähigkeiten des Beraters.

Doch wie kann ein Unternehmen hier für »Mehrwerte« in Form von optimal auf die Bedürfnisse abgestimmten Versicherungsprodukten schaffen? Hier empfiehlt es sich, einen qualifizierten Spezialmakler in Anspruch zu nehmen, der über langjährige Erfahrung im Umgang mit Risiken der Informationstechnologie verfügt. Unternehmen sollten sich die Zeit nehmen und sich eine umfassende Risikoanalyse anfertigen lassen, welche eine detaillierte Schwachstellenanalyse in Verbindung mit Optimierungsansätzen verbindet.

Versicherungsverantwortliche in IT-Unternehmen können davon ausgehen, dass die überwiegende Zahl ihrer Haftpflicht- und Cyberpolicen mehr oder weniger gravierende Mängel aufweisen. Dargestellt sei dies an zwei wichtigen Themen, welche für viele Unternehmen der Branche von Relevanz sind.

**Themenschwerpunkt: Haftungsvereinbarungen.** Als Dienstleistungsbranche ist die IT häufig Lieferant von Softwareprodukten oder Services. Abnehmer sind meist große, internationale Unternehmen, die über eine entsprechende Marktmacht verfügen und diese über deren Anwälte auch ausnutzen.

So werden in der täglichen Praxis Verträge geschlossen, welche mit Pönalen belegt werden, sofern zum Beispiel die Leistung nicht fristgerecht erbracht wird. Doch führt dieser Verzug beim Abnehmer denn auch zu einem echten Schaden? Versicherungsschutz bieten die Haftpflichtversicherer lediglich für »Schadensersatzansprüche«, welche auf einer gesetzlichen Haftung, also insbesondere auf Verschulden, basieren. Das geht in der Regel komplett am Versicherungsbedarf eines IT-Dienstleisters vorbei, da dieser häufig auch verschuldensunabhängig in die Haftung genommen werden kann. Diesen fatalen Fehler haben zwischenzeitlich viele IT-Haftpflichtversicherer korrigiert und die »verschuldensunabhängige Haftung insbesondere bei SLAs und Dauerschuldverhältnissen« in die Deckung mit aufgenommen.

Doch läuft auch diese Klausel ins Leere, sofern nach einem unverschuldeten Ereignis der IT-Dienstleister etwa seine SLAs nicht einhalten kann, in Verzug gerät und vertraglich dafür Pönalen zu leisten hat. Denn Pönalen sind unverändert in der Branche ein Ausschlusskriterium und damit ein Damoklesschwert über einem IT-Unternehmen. Dieses



**\*/ Über einen Mangel an Anbietern für Cyberpolicen brauchen wir heute nicht mehr zu klagen, doch wer versteht wirklich, was diese im Zweifelsfall decken?**

Problem zu lösen, bedarf es einer deckungstechnischen Überprüfung der Haftungsvereinbarungen sowie gegebenenfalls einer individuellen Klausellösung unter Einbeziehung von Strafzahlungen, wie sie bereits heute von einigen spezialisierten Versicherungsmaklern angeboten werden.

**Themenschwerpunkt: Cybercrime.** Über kaum ein anderes Thema wurde in den letzten Jahren so viel geschrieben, wie über die immer weiter ausufernden Risiken von Cyberattacken. Ein funktionierendes Riskmanagement ist heute unverzichtbarer Bestandteil eines jeden verantwortungsvollen unternehmerischen Handelns.

Doch ein Bereich wird trotz aller negativen Schlagzeilen immer noch geradezu stiefmütterlich behandelt, der Risikotransfer im Rahmen einer umfassenden Cyberversicherung. Zugegeben, es gibt spannendere Themen, als sich mit Versicherungsbedingungen herumzuschlagen. Und noch dazu bei der Absicherung eines so komplexen Themas wie Cyberrisiken, wo bis heute die Mehrzahl der Versicherungsmakler nur über rudimentäres Wissen verfügt. Über einen Mangel an Anbietern für Cyberpolicen brauchen wir heute nicht mehr zu klagen, doch wer versteht wirklich, was diese im Zweifelsfall decken? Und wer kann mir als Unternehmer die Deckungsunterschiede der einzelnen Anbieter erklären?

Wie im Bereich der IT-Haftpflicht zeigt sich die Qualität des jeweiligen Versicherungsprodukts an den Grenzen der Versicherbarkeit. Inwieweit werden »vertragliche« Haftungsvereinbarungen im Falle eines cyberbedingten Haftpflichtschadensanspruchs gedeckt? In welchen Fällen werden auch Vertragsstrafen übernommen? Wird eine 24-Stunden-Krisenhotline zu einem im Vorfeld fix vereinbarten Provider geboten? Wie ist die Qualität des Risk Consultant? Wer zahlt, wenn sich ein Verdacht auf einen Cybervorfall nicht bestätigt und Kosten für den Cyberconsultant anfallen? Kommt der Dienstleister schon im Verdachtsfall

zum versicherten Unternehmen? Was ist, wenn das Unternehmen eine cyberbedingte Betriebsunterbrechung erleidet und die Ursache außerhalb des Unternehmens zu suchen ist, beispielsweise bei einem Cloud-Service-Provider? Werden auch Fälle von Cyberspionage abgesichert? Und, und, und.

Die Liste der Qualitätsmerkmale ist mindestens so lang, wie der Unterschied in der Produktqualität groß ist. Auch hier empfiehlt es sich, den Rat eines auf Cyberrisiken spezialisierten, unabhängigen Versicherungsmaklers einzuholen. Das muss nicht gleichzeitig eine Abkehr vom bisherigen Versicherungspartner bedeuten, da Spezialmakler in der Regel auch eine Beratung und Betreuung in dieser Spezialsparte anbieten.

**Fazit.** Die IT verändert unser aller Leben. Damit wachsen auch die Risiken für die IT-Unternehmen, welche als Teil dieses Veränderungsprozesses Dienstleistungen erbringen. Doch genau so komplex wie die Anwendungen oder Services der IT-Branche sind auch die Risiken, die es im Vorfeld abzuwägen und einzugrenzen gilt. Dem »Risikotransfer« als festem Bestandteil eines umfassenden Riskmanagements wird heute oft noch zu wenig Bedeutung beigemessen. Doch so, wie die IT-Branche bei der Entwicklung neuer Technologien oder Dienstleistungen auf Spezialisten setzt, sollten IT-Unternehmen auch die Qualität ihres Risikotransfers von Branchenspezialisten überprüfen lassen. ■



Peter Janson,  
Versicherungsspezialist für die IT-Branche,  
Prokurist der Dr. Hörtkorn München GmbH  
[www.hoertkorn-muenchen.de](http://www.hoertkorn-muenchen.de)