



\$

\$



#



||



#

"

!

!





Nicht mehr nur das eigene Unternehmen im Blick • Risiken aus firmenübergreifendem Datenaustausch

## Risikopotentiale, Schadensszenarien, Lösungen Deckungen in der »Industrie 4.0«

**B**lickt man auf den Ursprung und die Entwicklungen der Industrieversicherung seit dem 17. Jahrhundert zurück, ist eindeutig zu erkennen, dass die Industrialisierung einen dauerhaft prägenden Einfluss auf die Branche hatte. Ohne die technischen Errungenschaften dieser Zeit gäbe es die Kompositversicherung in ihrer heutigen Form nicht. Umgekehrt wäre der rasante Fortschritt der Industrie ohne Versicherungen unmöglich gewesen. Nun erleben wir die Vierte Industrielle Revolution. Die »Industrie 4.0« beginnt.

Wie in der Vergangenheit auch birgt jede nachhaltige Veränderung Risiken, die neuen Versicherungsbedarf erzeugen und eine Evolution der Branche verlangen. Die Digitalisierung wirft Cyber-Risiken auf, zu deren Absicherung es schon seit einiger Zeit Versicherungsprodukte gibt. Um die Sparte ist ein Hype entstanden, doch das Zwischenfazit ist gemischt. Die gute Nachricht ist, dass sich Versicherer, Makler und Kunden mit dem Thema auseinandersetzen. Die schlechte Nachricht ist, dass sich noch kein Markt etabliert, so dass sich die vermeintliche Nachfrage nicht in Abschlüssen niederschlägt, obwohl es durchaus Anlässe gibt. Cyber-Attacken, die jede Branche und jede Betriebsgröße treffen können, werden ständig gemeldet. Sicherheitsexperten sagen, dass nicht zu fragen ist, ob Unternehmen Opfer von Cyber-Attacken werden, sondern wann. Woran scheitern die Abschlüsse?

Fast alle Industrieversicherer bieten inzwischen eigene Produkte an, wobei die Ansätze sehr verschieden sind, was allerdings auch der Natur der Sache geschuldet ist: Cyber-Risiken sind vielfältig und bedürfen mehrerer Betrachtungen, da der Begriff nicht eindeutig defi-

niert ist und diverse Einzelrisiken vereint, nämlich Datenverluste und Datenschutzverletzungen sowie Hacker-Angriffe, Cyber-Spionage, Cyber-Diebstahl oder Cyber-Erpressung sowie infolge dessen entstehende Kosten und Betriebsunterbrechungsschäden. Die Policen greifen die Risiken zwar auf, lösen aber zwei Probleme des Versicherungsnehmers nicht: Wo bestehen Überschneidungen zu bereits bestehenden anderen Versicherungen und wie kann man die Spezialprodukte vergleichen?

Ein Grund für die Heterogenität des Markts ist, dass die meisten Versicherer zunächst nicht wussten, wohin ihre Produkte intern gehören. Sie wurden in der Haftpflichtabteilung, bei den technischen Versicherungen oder in der Vermögensschadendeckung angesiedelt. Dadurch verschieben sich die Schwerpunkte des Produkts. Außerdem hat jeder Versicherer seine eigene Policensprache, was die Verwirrung fördert. Trotz dieser Varianten ist es möglich, die Versicherungsgegenstände in zwei Bereiche einzuteilen:

► **Haftpflichtteil:** Unternehmen haben Daten und Informationen von Dritten nach geltendem Recht zu schützen. Verstöße gegen die Verpflichtung sind meldepflichtig und können Ansprüche des Geschädigten nach sich ziehen. Die Cyber-Versicherung bietet Schutz für die Prüfung, Abwehr oder Entschädigung des Haftpflichtanspruchs. Ebenfalls gedeckt, aber formell dem Eigenschadenteil zuzurechnen, sind die mit der Meldung verbundenen Kosten, wobei man mit rund 150,- Euro pro Datensatz rechnet.

► **Eigenschadenteil:** Hier sind Vermögensschäden im Unternehmen gedeckt, die Schadenbeseitigung, die Datenwiederherstellung, die Instandsetzung des IT-Systems und Betriebsunterbrechungsschäden.



Tomasz Kosecki

Für Unternehmen in der »Industrie 4.0« sind die technische Wiederherstellung der IT-Infrastruktur, die laufenden Kosten und der entgangene Gewinn durch die Betriebsunterbrechung die versicherungswürdigsten Bereiche. Hinzu kommen Risiken aus der digitalisierten Lieferkette und der digitalen Wartung der Produktion, über deren Reichweite man heute nur spekulieren kann. Dabei wird selbstverständlich sein, dass Maschinen online miteinander kommunizieren, so dass unerwünschte Effekte auf das eigene Unternehmen, auf Kunden, Lieferanten und Dienstleister denkbar sind. Der un-

ternehmensübergreifende, automatisierte Datenaustausch ruft viel neue Verantwortung für sich und andere hervor, sofern die Kommunikation gestört, unterbunden oder manipuliert wird und die Ursache dafür im eigenen System steckt. Das Thema wird unter Versicherungsaspekten noch diskutiert, wobei bereits Grenzen der Versicherbarkeit gezogen wurden, so dass die (Schaden-)Erfahrung zeigen wird, welche Risiken versicherbar bleiben oder versicherbar werden.

Die Prüfung des Versicherungsumfangs wird wegen der individuellen Risiken und der Komplexität eine Herausforderung bleiben. Versicherer und Makler sind gefordert, ihre Kunden transparent zu beraten, damit sie fundierte Entscheidungen treffen können.

Zu betonen ist noch, dass auch die Unternehmen gefragt sind. Der Risikotransfer ist nur ein Teil der Lösung. Eine Cyber-Versicherung entbindet Unternehmer nicht davon, ein adäquates Risikomanagement einzurichten, das auch präventiv wirkt. Hierzu gehört eine zeitgemäße IT-Sicherheit sowie ein Notfallplan für verschiedene Szenarien. Der Gesetzgeber hat schon mit der EU-Datenschutz-Grundverordnung (DSGVO) reagiert, die im Mai 2018 in Kraft treten soll. Unternehmen haben dann noch 72 Stunden Zeit, um eine Cyber-Attacke zu melden. ■

*Tomasz Kosecki LL.M., Geschäftsführer FINLEX GmbH, Frankfurt/M.*

### Schadenbeispiel:

Die Datenbank eines Hochregallagers wird durch einen Virus beeinträchtigt. Ein störungsfreier Arbeitsablauf ist nicht mehr gewährleistet.

#### Finanzielle Auswirkungen:

Betriebsunterbrechungs-Schaden aufgrund der kontrollierten Systemabschaltung	300.000 €
Dekontamination infizierter Daten	45.000 €
Wiederherstellung der Daten aus »Back-up«-Sicherungen	15.000 €
Manuelle Auslagerung und Neufassung eines Teils der Lagerware	160.000 €
Vertragsstrafen aufgrund der verspäteten Auslieferung	175.000 €
<b>Versicherte Gesamtkosten</b>	<b>695.000 €</b>

Quelle: ACE Group (heute Chubb), 2013