André Gießer/VerkehrsRundschau

**Sascha Michel Kessel (links) leitet das Competence Center Cyber bei der Schunck Group und Niels Joehnk leitet das Competence Center Financial Lines des Versicherungsmaklers**

# „Die Gefahr nimmt ständig zu“

**Ob WannaCry oder Petya.A: Cyberangriffe auf Logistikunternehmen häufen sich. Im Interview erklären Niels Joehnk und Sascha Michel Kessel vom Versicherungsmakler Schunck, warum das Risiko nicht zu unterschätzen ist.**

**Im Frühling haben weltweite Hackerangriffe zig Unternehmen lahmgelegt. Unter ihnen waren auch mehrere aus der Transport- und Logistikbranche. Wie wichtig ist es, sich gegen Schäden durch Cyberkriminelle abzusichern?**

**Kessel:** Die Gefahr, dass Unternehmen aufgrund von Cyberattacken einen existenzbedrohenden Schaden erleiden, nimmt ständig zu. Trotz der jüngsten globalen Angriffe durch die Schadsoftware wie WannaCry oder Petya.A unterschätzen viele Spediteure bisher das Risiko, selbst Opfer solcher Krimineller zu werden.

**Woran liegt es, dass trotz des Risikos bisher noch große Zurückhaltung herrscht?**

**Kessel:** Oft herrscht der Irrglaube, Cyberkriminelle hätten es auf die großen Konzerne abgesehen und das eigene Geschäft sei nicht interessant genug. Manche Unternehmer sind bisher auch davon ausgegangen, dass Cyberattacken eher Wirtschaftszweige treffen, in denen es mehr Geld zu holen gibt. Nach den jüngsten Angriffen durch Schadsoftware wie WannaCry oder Petya.A auf Unternehmen aus allen möglichen Branchen weltweit, die unter anderem DHL, Maersk, TNT Express und Raben getroffen haben, bemerken wir aber inzwischen ein Umdenken. Die Einschläge kommen immer näher und das Bewusstsein für diese neue Gefahr steigt.

**Joehnk:** Die Berichterstattung in den M edien und die zunehmende gesetzliche Regelung – Stichwort: das bereits geltende IT-Sicherheitsgesetz und die im nächsten Mai in Kraft tretende EU-Datenschutz-Grundverordnung – haben ebenfalls zur Sensibilisierung der gewerblichen Versicherungskunden beigetragen. Wir gehen davon aus, dass der Abschluss einer Cyber-Police in absehbarer Zeit genauso selbstverständlich zum Standard-Versicherungs-Portfolio gehören wird wie eine Betriebshaftpflicht- oder Feuerversicherung.

**Ignoriert der Großteil der Unternehmen leichtsinnig das steigende Risiko?**

**Kessel:** Viele warten auch ab, wie sich die Prämien entwickeln. Schließlich ist der

ONLINE-SEMINAR

## Cyber-Risiken richtig versichern

Erst WannaCry, dann Petya.A: Die Cyberangriffe auf die Wirtschaft nehmen zu. Allein in der ersten Hälfte dieses Jahres haben diese beiden Verschlüsselungstrojaner weltweit diverse Unternehmen lahmgelegt und für Schäden in Millionenhöhe gesorgt.
Auch die Transport- und Logistikbranche ist zunehmend betroffen!
In Gefahr sind nicht nur Konzerne, sondern auch kleinere Betriebe, deren IT-Sicherheitssysteme in der Regel anfälliger sind. Als Schnittstelle namhafter und solventer Kunden aus Industrie und Handel ist die Transport- und Logistikbranche im Visier immer raffinierterer Hacker.
Doch kaum ein Unternehmen redet über die Schäden durch Cyber-Attacken. Und wenige Transport- und Logistikbetriebe sind dagegen versichert. Sascha Michel Kessel, Leiter des Competence Centers Cyber der Schunck Group, erklärt, warum es fatal ist, auf eine entsprechende Police zu verzichten, und worauf vor allem kleine Unternehmen bei der Wahl des Versicherungsschutzes achten sollten.
Der Experte gibt einen Überblick über die aktuellen Angebote und Preise im Versicherungsmarkt. Und er zeigt anhand von Branchenbeispielen und mit Blick auf das Preis-Leistungs-Verhältnis, welche Cyber-Versicherungen für Transport- und Logistikunternehmen sinnvoll sind. Im Rahmen des Online-Seminars können die Teilnehmer über eine Chat-Funktion gezielt Fragen an den Fachmann stellen.

Natalia Merzlyakova/stock.adobe.com

**Cyber-Versicherungen bieten Schutz**

**Termin:** 8. November 2017, 15.00-16.00 Uhr

**Referent:** Sascha Michel Kessel, Leiter des Competence Centers Cyber der Schunck Group

**Moderation:** André Gieße, Redakteur der VerkehrsRundschau

**Themenschwerpunkte:**
- Zweck einer Cyber-Versicherung und Gefahrenpotenzial für Logistiker
- Aufbau, Inhalt und Leistungsumfang einer Cyber-Versicherung
- Überblick über Versicherungsanbieter und -kosten für Logistiker
- Sinnvolle Versicherungs-Bausteine und regelmäßige Ausschlusskriterien
- Preis-Leistungs-Vorschläge anhand repräsentativer Unternehmensbeispiele
- Notwendige Präventionsmaßnahmen zum Erhalt des Versicherungsschutzes

**Zielgruppe:** Inhaber, Geschäftsführer und IT-Beauftragte von Transport-, Speditions- und Logistik-Unternehmen *ag*

Abschluss einer solchen Police gerade für kleinere Unternehmen mit Margen von zum Beispiel einem Prozent eine wichtige finanzielle Entscheidung. Sie rechnen damit, dass die Tarife sinken, weil der Wettbewerb in diesem relativ jungen Versicherungssegment ständig zunimmt. Das ist aus meiner Sicht aber fatal. Ich erwarte, dass es künftig tendenziell eher teurer wird, sich gegen Cyberschäden zu versichern.

**Was macht Sie da so sicher?**
**Kessel:** Bisher hat kaum ein Versicherer in Europa ausreichend Erfahrung mit der möglichen Menge und dem durchschnittlichen Ausmaß der Cyberschäden gesammelt. Das heißt, die Prämien basieren auf Schätzungen. Unternehmen, die schon dagegen versichert sind oder sich jetzt versichern lassen, könnten später froh sein über diesen dann „Altvertragsstatus". Denn sie erhalten für vergleichsweise geringes Geld umfangreiche Leistungen. Sie können davon ausgehen, dass die Prämien teurer und die Bedingungswerke schmaler werden, wenn die Schadenhäufigkeit und -höhe in diesem Bereich weiter so massiv steigen. Denn wenn das Verhältnis von Deckung und Dienstleistung einerseits und den dafür anfallenden Beiträgen andererseits so bliebe, dann könnten die Versicherer es sich bald nicht mehr leisten, diesen Schutz anzubieten. Sie haben auch eine Verantwortung ihren Kunden gegenüber, zahlungsfähig zu bleiben.

**Wie wahrscheinlich ist es, dass die Policen für einen Cyberschutz aufgrund des zunehmenden Wettbewerbsdrucks im Versicherungsmarkt günstiger werden?**
**Kessel:** Die Chance ist durchaus da, weil weitere Versicherer dieses Wachstumssegment für sich entdecken. Die Tarifentwicklung hängt allerdings – wie eben erläutert – nicht nur von Angebot und Nachfrage ab, sondern auch maßgeblich vom tatsächlichen Schadensszenario. Die Versicherer wollen letztlich Geld mit ihren Produkten verdienen. Das bedeutet, sie müssen sie zu realistischen Preisen anbieten, sodass abzüglich aller Services und Erstattungen noch etwas übrig bleibt.
**Joehnk:** Wir schätzen die Chance aber als gering ein, weil Unternehmen durch neue Vorschriften wie die EU-Datenschutz-Grundverordnung ab dem nächsten Jahr beim Umgang mit personenbezogenen Daten leichter gegen das Gesetz verstoßen können und deshalb gezwungen sind, sich finanziell besser gegen Strafen und Schadensersatzforderungen abzusichern. Es besteht eine Pflicht, nicht nur geeignete technische und organisatorische Maßnahmen zum Datenschutz einzuführen, sondern auch den Versicherungsschutz an die gestiegenen Anforderungen anzupassen. Unternehmen drohen bei Verstößen etwa Geldbußen in Höhe von bis zu 20 Millionen Euro oder bis zu vier Prozent des Jahresumsatzes – je nachdem, welche Summe höher ist.

**Betrifft das auch kleine und mittlere Unternehmen aus der Branche?**
**Kessel:** In Deutschland hat der Gesetzgeber bisher die großen Unternehmen der Transport- und Logistikunternehmen durch das IT-Sicherheitsgesetz und die dazugehörige Verordnung in die Verantwortung genommen. Diese Konzerne erwarten nun aber von ihren Auftragnehmern zum Schutz der Lieferkette den Nachweis gewisser Zertifizierungen und einer Cyber-Risk-Deckung. Die Datenschutz-Grundverordnung der EU gilt darüber hinaus ab dem 25. Mai 2018 unmittelbar in allen Mitgliedstaaten und betrifft auch kleine und mittlere Unternehmen.

**Welche Cyberangriffe kommen derzeit am häufigsten vor?**
**Joehnk:** Das sind Erpressungsversuche durch ein Botnetz von Schadsoftware, das wahllos IT-Systeme attackiert und Computer mit Sicherheitslücken so lange blockiert, bis die Betroffenen einen gewissen Betrag zahlen. Sie lassen sich schnell programmieren und haben durch ihre breite Streuung eine große Wirkung.

**Wie viele Versicherer bieten aktuell in Deutschland eine Police zum Schutz vor Cyberschäden an?**
**Joehnk:** Heute gibt es schon 30 Anbieter, die in Deutschland eine Vielzahl von Lösungen für Gewerbekunden anbieten. Bei einigen stehen etwa die Daten und die möglichen Schäden durch Erpressung und



VR, 16.10.2017

Datendiebstahl im Vordergrund, weniger die Betriebsunterbrechung. Die Versicherer konzentrieren sich nun auch mehr auf kleine und mittlere Unternehmen. Bislang schienen ihnen bei diesem Kundenkreis mitunter der Prüfaufwand oder die Risiken und Kosten im Schadensfall zu groß.

**Kessel:** Es gibt wenige Versicherer, die einzelne Branchen ausschließen. Darüber hinaus gibt es welche, die erst ab einer gewissen Umsatzgröße einem Unternehmen ihre Dienste anbieten. Ein eigenes Konzept für die Transport- und Logistikbranche bietet unseres Wissens nach nur Schunck an.

**Wie viele Unternehmen haben sich denn inzwischen für das Versicherungskonzept von Schunck entschieden?**

**Joehnk:** Wir bewegen uns langsam im dreistelligen Bereich. Mehr als die Hälfte der Neuabschlüsse unserer Kunden aus den Transport- und Logistikbranchen beziehen sich auf unsere Cyber Risk Premium Police, die wir seit 2015 anbieten. Sie besteht aus einer Eigenschadenversicherung, einer Haftpflichtversicherung bei Drittschäden und enthält zahlreiche Assistance- sowie Kostenbausteine. Besondere Highlights sind eine sehr weitgehende Mitversicherung von vertraglichen Haftungsansprüchen, eine deutliche Erweiterung der Ertragsausfalldeckung, ausgefeilter Schutz bezüglich Reputationsschäden sowie spezielle Assistance-Dienstleistungen durch unsere Partner. Wir merken in den Beratungen, dass das Interesse stetig wächst.

**Worauf sollten kleine und mittlere Transport- und Logistikunternehmen bei der Suche nach der passenden Cyberschutz-Versicherung achten?**

**Kessel:** Für Gewerbekunden empfehlen sich unsere einfachen Antragsmodelle. Bei überschaubaren Geschäftsmodellen mit einer Handvoll Kunden sind die Risiken oft weniger groß oder ausgefallen als bei größeren Unternehmen oder Konzernen, die hoch spezialisiert in sensiblen Segmenten tätig sind und viele Beziehungen nach außen pflegen. Die Analyse für den passenden Versicherungsschutz lässt sich auch bei größeren Kunden durch einen einfachen Fragebogen einsteuern.

**Welche Bausteine sind wirklich wichtig und welche können sich Unternehmen im Zweifel sparen?**

**Kessel:** Nach meiner Erfahrung ist grundsätzlich keiner der unsererseits angebotenen Bausteine verzichtbar, weil jedes erst einmal abstrakte Szenario eintreten und ein Unternehmen im Ernstfall bis zu mehreren Millionen Euro und somit sogar die Existenz kosten kann.

Um mal vor Augen zu führen, was ohne Cyberschutz an Folgekosten anfällt: Allein ein IT-Forensiker zur Ermittlung oder Beweissicherung einer Computerattacke verlangt pro Tag durchschnittlich 2000 Euro. Die Prämie für eine Versicherung, die solche Services enthält, liegt bei Kleinunternehmen deutlich darunter.

VR plus Mehr zum Thema finden Sie im Dossier „Versicherung“
*www.verkehrsrundschau.de/dossiers*

**Welche Kosten muss ein Unternehmen für die Cyberschutz-Versicherung einplanen?**

**Kessel:** Kleinere Betriebe können sich schon für wenige 100 Euro im Jahr Versicherungsschutz mit sehr kleinen Deckungssummen einkaufen. Günstig ist aber nicht immer gut. Auch kleine Betriebe sollten mindestens ein oder zwei Millionen Euro Deckungssumme anstreben. Für zwei Millionen Euro Deckungssumme sind in unseren Konzepten Prämien ab 1600 Euro möglich. Je nach Risikosituation und Wahl des Versicherungsumfangs sind bei gleicher Deckungssumme auch Prämien von 3000 oder 5000 Euro denkbar. Größere Unternehmen mit Deckungssummen ab drei oder fünf Millionen sollten für unsere sehr guten Premium-Produkte mindestens zwischen 5000 und 10.000 Euro einplanen.

**Joehnk:** Der Versicherungsmarkt befindet sich noch in einer Phase der Preisfindung. Vor zwei, drei Jahren gab es durchaus Angebote mit einer Deckungssumme von zwei Millionen Euro, die im Jahr 80.000 Euro gekostet haben und für die meisten Unternehmen zu teuer waren. Inzwischen sind wir bei einem Niveau angekommen, das für alle Beteiligten akzeptabel scheint. Die angesprochene Schadenentwicklung wird die Prämien aber zunehmend beeinflussen.

**Was sagen Sie Unternehmen, die glauben, die Versicherungen sind zu teuer und Cyberkriminelle hätten es eher auf Schwergewichte in der Wirtschaft abgesehen?**

**Joehnk:** Cybercrime gehört mittlerweile zu den Top-drei-Risiken für Unternehmen. Es gibt diverse Arten, durch die Nutzung von Computern und Internet zum Opfer von Kriminellen zu werden. Oft haben es Cyberkriminelle auf keine bestimmten Unternehmen abgesehen, wenn sie Schadprogramme in Umlauf bringen. Sie nutzen beispielsweise Sicherheitslücken in Systemen und man wird Zufallsopfer. Professionelle Täter hingegen, mit klarem Ziel, umgehen die hohen technischen Hürden der großen Industrie- und Handelskonzerne, indem sie verhältnismäßig einfach über deren kleinere Dienstleister an ihr Ziel gelangen. Sie nutzen gerne die größte Schwachstelle in jedem Unternehmen – den Mitarbeiter. Zum Beispiel durch Bewerbungs- oder Angebotsmails mit gefährlichem Anhang, liegen gelassene USB-Sticks oder durch gezielte Manipulation oder Erpressung von Mitarbeitern.

**Kessel:** Das gilt auch für die Transport- und Logistikbranche. Denn mal ehrlich, wie viele kleine Unternehmen können sich einen eigenen IT-Beauftragten leisten oder beschäftigen sich ausreichend mit strategischen Präventionskonzepten? Die meisten ahnen nicht, welches Risiko ihnen droht.

*André Gießе*

**CYBER-POLICEN**

## Das bieten die Versicherer

Cyber-Policen decken Schäden ab, die sich aus einer Verletzung der Informationssicherheit ergeben, sei es durch einen fahrlässig herbeigeführten Datenverlust durch Mitarbeiter oder einen gezielten Hackerangriff. Sie bietet also immer dann Schutz, wenn etwa Daten gestohlen, gelöscht, verschlüsselt, verändert, missbraucht oder unrechtmäßig veröffentlicht wurden. Alle Assekuranzen bieten zwei Bausteine an: eine Eigenschadenversicherung und eine Haftpflichtversicherung, die Schäden von Kunden und Geschäftspartnern abdeckt. Einige Policen decken auch die Kosten ab, um die IT-Systeme zu bereinigen und in puncto Sicherheit auf den neuesten Stand zu bringen. Darüber hinaus lassen sich Leistungen einschließen, die Unternehmen helfen, im Krisenfall Reputationsschäden zu begrenzen: Dazu gehört die Unterstützung durch Rechtsanwälte, PR-Fachleute und IT-Berater. Vertragsstrafen wegen der Verletzung von Geheimhaltungspflichten müssen oft zusätzlich abgesichert werden. Bei manchen Versicherern ist der Ertragsausfall infolge einer Betriebsstörung im Standardschutz enthalten, bei anderen ein separater Leistungsbaustein. *sah*



VR, 16.10.2017