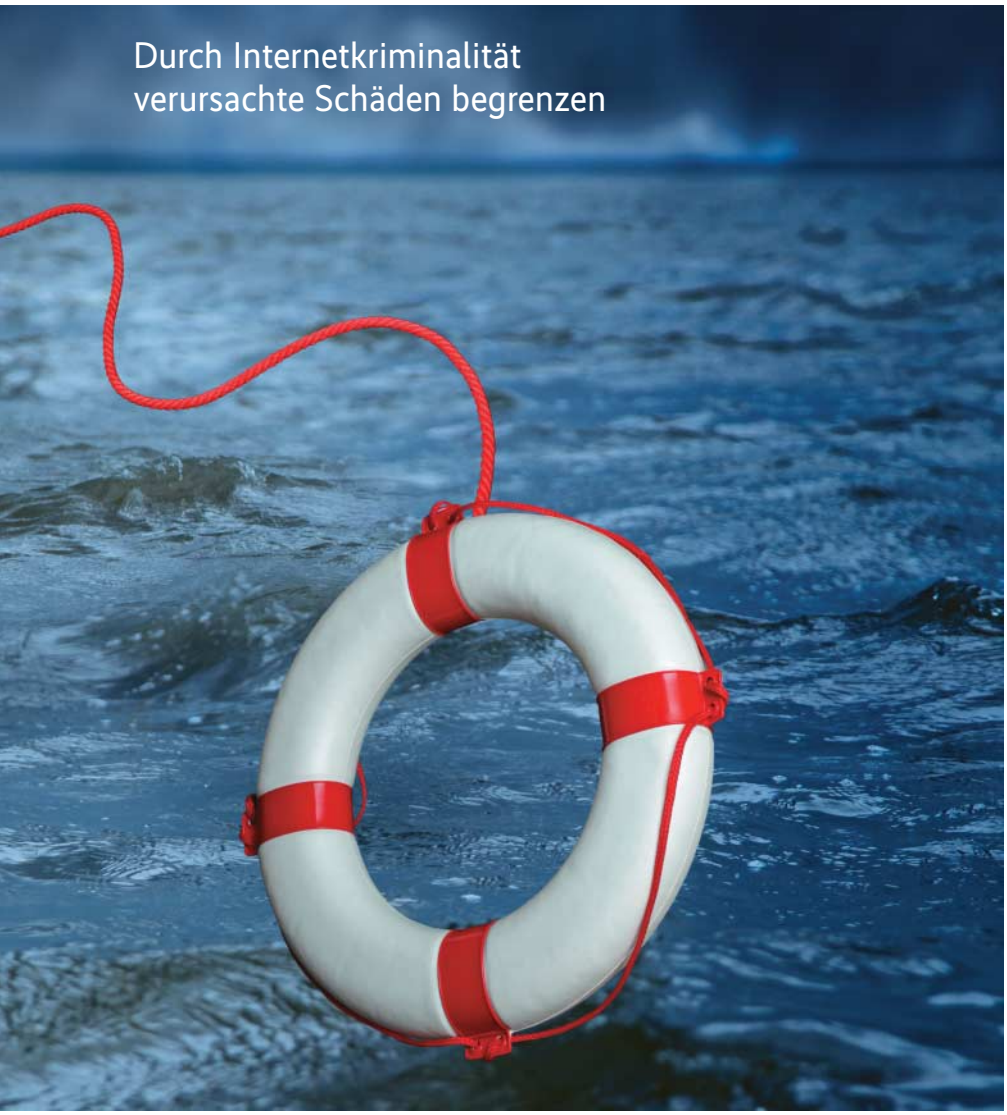


Sicherheits-halber

Thomas Fritzsche, Alexander Geschonneck

Das Risiko für Unternehmen, Opfer eines Cyberangriffs zu werden, ist in den vergangenen Jahren stark gestiegen. Der Diebstahl von Kundendaten, Betriebsunterbrechungen oder Erpressungen können schnell zu Verlusten in Millionenhöhe führen. Welche Leistungen bieten Cyberversicherungen, wer kann sich versichern und was sollte man vor Abschluss einer Police unbedingt wissen? Ein Überblick.

Cyberkriminelle entwenden oder manipulieren vertrauliche Daten, schleusen Schadsoftware in Netzwerke ein oder legen Produktionsanlagen lahm. Dass solche Angriffe bei den Betroffenen unter Umständen Schäden in Millionenhöhe verursachen, konnte man an Beispielen wie Sony Pictures, dem Deutschen Bundestag oder dem zerstörten Hochofen sehen, dessen Fall das Bundesamt für Sicherheit in der Informationstechnik (BSI) in seinem „Bericht zur Lage der IT-Sicherheit in Deutschland 2014“ dokumentierte. Und auch mittelbare Schäden wie der Missbrauch des eigenen Firmennamens für Betrugsmaschen oder zahlreiche andere Vorfälle können ein Unternehmen teuer zu stehen kommen.

Deutschland als fragwürdiger Spitzenreiter

Gemessen an der Wirtschaftsleistung sind diese Schäden nirgends so hoch wie in Deutschland, wie aus einer weltweiten Untersuchung des „Center for Strategic and International Studies“ hervorgeht (dieser und alle weiteren Links des Artikels sind über „Alle Links“ im blauen Kästchen zu finden). Das bestätigt auch die aktuelle E-Crime-Studie 2015 der Wirtschaftsprüfungsgesellschaft KPMG (Abbildung 1): 40 % der befragten Unternehmen waren in den letzten zwei Jahren von Cyberkriminalität oder auch „E-Crime“ betroffen – Tendenz steigend. Das Risiko, dass deutsche Unternehmen Opfer von E-Crime werden, schätzen 98 % der Studienteilnehmer als hoch oder sehr hoch ein („Alle Links“). Den Gesamtschaden durch E-Crime in den vergangenen zwei Jahren veranschlagt die KPMG mit circa 54 Milliarden Euro. Die bittere Erkenntnis: Ein vollständiger Schutz vor Cyberangriffen ist für technologieabhängige Unternehmen nicht erreichbar.

Dennoch, so schätzen die Versicherer, sichern sich lediglich bis zu 10 % der deutschen Unternehmen gegen das Risiko eines Cyberangriffs mit einer entsprechenden Versicherung ab. Wie sind diese Zahlen zu interpretieren? Eine Erklärung könnte sein, dass das Thema Cyberrisiken bei deutschen Unternehmenslenkern noch nicht vollständig angekommen ist. Immerhin hat ein Viertel der deutschen CEOs noch nie an einer Sitzung mit Führungskräften oder Vorstandskollegen zum Thema „Cyber Security“ teilgenommen. Das ist im weltweiten Vergleich der höchste Wert (Durchschnitt: 5 %).

Die Frage ist also: Kennen die Unternehmensführungen die Möglichkeiten

von Cyberversicherungen? Eventuell fehlt der Dialog, um die Potenziale einer Versicherung auf die eigenen Cyberrisiken übertragen zu können – vorausgesetzt, diese sind im Unternehmen überhaupt bekannt. Vielleicht sehen Unternehmen die kumulierten Schadenssummen bei relevanten Cybervorfällen als viel zu hoch an, als dass diese kaufmännisch sinnvoll versichert werden könnten. Zumindest Konzerne kommen im Dialog mit den Versicherern bei Multimillionen-Euro-Schäden in Einzelfällen zu diesem Schluss.

Eine durchschnittliche Gesamtschadenssumme von circa 370 000 Euro mit Ermittlungs- und Folgekosten von rund 70 000 Euro über verschiedene Deliktstypen hinweg spricht allerdings für ein breites Spektrum kaufmännisch sinnvoll versicherbarer Schäden. Insbesondere wenn man berücksichtigt, dass einige Deliktstypen 50 Mal und häufiger innerhalb von zwei Jahren auftreten, wie die genannte E-Crime-Studie belegt.

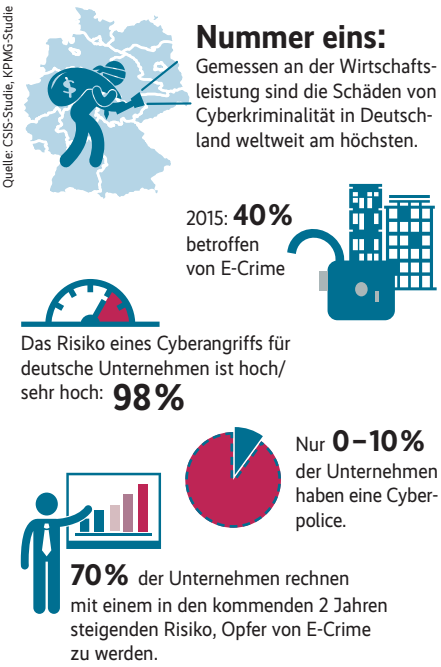
Eine Branche im Aufwind

Seit 2011, als die erste Cyberversicherungspolice auf den deutschen Markt kam, haben solche Angebote kontinuierlich zugenommen. Mittlerweile bieten 13 Versicherer ihre Cyberpolicen für Geschäftskunden in Deutschland an. Im Rahmen der für diese Marktübersicht durchgeführten Befragung von Versicherungsunternehmen haben von den 13 Versicherern neun Informationen zu ihren Versicherungsprodukten geschickt. Mehrere Unternehmen befinden sich aktuell in der Produktentwicklung und möchten daher noch keine konkreten Details preisgeben. Der Blick über die Ländergrenzen zeigt, dass Cyberversicherungen in den USA und in Großbritannien zu den Trendprodukten der Versicherungsbranche gehören.

Grundsätzlich kann eine Cyberversicherung ein großes Spektrum an Risiken von Standardangeboten bis hin zu Individuallösungen abbilden. Die Angebote unterscheiden sich im Umfang der abgesicherten und ausdrücklich ausgeschlossenen Risiken (siehe Tabelle „Versicherungsleistungen im Detail“). Sämtliche Anbieter übernehmen die Kosten für das Abwehren unberechtigter und das Begleichen berechtigter Schadensersatzansprüche Dritter sowie die Haftpflicht infolge von Hackerangriffen, Denial-of-Service-Attacken, Datenschutzverletzungen oder nicht funktionierender digitaler Kommunikation.

Ebenso verhält es sich mit dem Übernehmen der direkten Schäden durch Denial-of-Service-Attacken, der Kosten für die Aufrechterhaltung des Geschäftsbetriebs sowie der Verdienst- und Ertragsausfälle bei Betriebsstörungen. Gleichermaßen einheitlich ist die Regulierung von Schäden durch gefälschte, ausgespähte und abgefangene Daten, Computersabotage und das Erschleichen von Zugangsdaten. Dieser Aspekt der Deckung ist besonders hervorzuheben, da sich hieraus potenziell die Regulierung von Schäden zahlreicher Spielarten von Deliktstypen ergibt. Eine Ausnahme bildet beispielsweise die Sabotage von IT-Anlagen zur Steuerung von Maschinen und Anlagen. Einen daraus resultierenden Schaden würden nicht alle Versicherungsanbieter begleichen. Zudem würden nur wenige die Kosten für Ersatzleistungen, Reparaturen oder Neuanschaffungen erstatten. Fragen Sie also vor Abschluss einer Versicherung nach, was die Übernahme von Schäden durch Sabotage im Detail bedeutet.

Bemerkenswert ist an dieser Stelle auch, dass der Missbrauch unternehmenseigener Computer durch Cyberkriminelle nicht von allen Versicherungsanbietern gedeckt ist. Wie verhält es sich aber, wenn dieser Missbrauch zum Ausspähen von



Die Studien der KPMG und des CFIS beleuchten das Sicherheitsgefühl in deutschen Unternehmen, das zwar der tatsächlichen Sicherheitslage entspricht, sich aber nicht in entsprechenden Vorsorgemaßnahmen niederschlägt (Abb. 1).

Daten oder eben zur Sabotage genutzt wird? Wie ist diese Regelung in Bezug auf die widerrechtliche Nutzung eines Unternehmensservers zum Speichern und Streamen von (kinder-)pornografischem oder verfassungsrechtlich bedenklichem Material auszulegen? Hieraus können sich drastische strafrechtliche Konsequenzen sowie enorme Reputationsschäden ergeben. Gut, dass zumindest die Möglichkeit besteht, dass die Versicherer die Kosten der Rechtsverteidigung übernehmen. Potenzielle Reputationsschäden schließen einige Anbieter ausdrücklich aus oder verweisen auf entsprechende Zusatzprodukte.

Die Kosten für das Wiederherstellen gestohlener, zerstörter, beschädigter oder blockierter Daten, Programme und Netzwerke nach einer Cyberattacke würden alle Versicherungsanbieter übernehmen. Hierbei sollten Unternehmen aber mit ihrem Anbieter für ihre spezifischen Geschäftsrisiken klären, was das im Einzelfall heißt. Unternehmen, deren Geschäftsmodell beispielsweise größtenteils aus der Nutzung von Kundenkontaktdaten besteht, sollten sich bestätigen lassen, ob darunter der Einkauf komplett neuer Kundenkontaktdaten fällt. Im Zweifelsfall könnte die Regelung auch nur bedeuten, dass die Kosten für die Entschlüsselung unautorisiert verschlüsselter Daten übernommen werden. An dieser Stelle ist darauf hinzuweisen, dass nicht alle Versicherungsan-

iX-TRACT

- Obwohl laut einer aktuellen Umfrage viele Unternehmen die Bedrohung durch Cybervorfälle fürchten, hat nur ein geringer Teil von ihnen eine Cyberversicherung abgeschlossen.
- Die Regelwerke der Versicherer definieren explizit abgedeckte sowie ausdrücklich ausgeschlossene Schadensfälle. Das Analysieren der eigenen Risiken für eine gegebenenfalls individuell zugeschnittene Cyberversicherung ist dennoch für Unternehmer unumgänglich.
- Schulungsmaßnahmen und Sicherheitskonzepte sind für Unternehmen ratsam. Sie verringern das Risiko, dass ein Cybervorfall passiert, und wirken sich unter Umständen günstig auf die Versicherungstarife aus.

bieter die Schäden durch den Diebstahl von Datenträgern inklusive Folge- und Nebenschäden tragen.

Hilfe bei Erpressung

Bei fast allen Anbietern sind auch die Schäden und Aufwendungen bei Erpressungen über das Internet zumindest theoretische Regulierungsfälle – insbesondere Lösegeldzahlungen sind lediglich bei einem Versicherer explizit ausgeschlossen. Erpressungsversuche sind aktuell nicht gerade selten, vorrangig im Zusammenhang mit sogenannter Ransomware. Diese Schadsoftware verschlüsselt Daten wie Systeme und fordert die Zahlung von Lösegeld für die Entschlüsselung. Selbst wenn sich hier mitunter ein Verhaltenskodex bei den Angreifern etabliert hat, der eine Entschlüsselung bei Lösegeldzahlung tatsächlich vorsieht, ist nicht unbedingt gesichert, dass sich diese erfolgreich umsetzen lässt. Zahlt die Versicherung auch zusätzlich zum Lösegeld die Folgeschäden, wenn ein Entschlüsseln nicht zustande kommt? Diese Frage wäre auf alle Fälle zu stellen.

Beim klassischen Internetbetrug oder der Urkundenfälschung zahlen nicht alle Anbieter. Letztere ist ein klassisches Mittel, um bei sogenannten Fake-President-Betrugsmaschen beispielsweise die Freigabe von Zahlungsanweisungen durch Geschäftsführer vorzutäuschen. Gerade

Versicherungsleistungen im Detail

	ACE*	AIG	Allianz	AXA	DUAL	HDI Gerling	Hiscox	W&W	Zürich DE
Welche Ereignisse stellen einen Regulierungsfall Ihrer Cyberversicherung dar? Schäden und Aufwendungen aufgrund von ... / infolge der ...									
Abwehr unberechtigter Schadensersatzansprüche Dritter	✓	✓	✓	✓	✓	✓	✓	✓	✓
Ausgleich berechtigter Schadensersatzansprüche Dritter	✓	✓	✓	✓	✓	✓	✓	✓	✓
Sabotage von IT-Anlagen zur Steuerung von Maschinen und Anlagen	–	✓	✓	✓	✓	–	✓	✓	✓
Löschung und Manipulation von Daten durch Bedienungsfehler sowie vorsätzliche Programm- oder Datenänderungen Dritter (z. B. Hacker)	✓	✓	✓	✓	✓	–	✓	✓	✓
Denial-of-Service-Angriffen	✓	✓	✓	✓	✓	✓	✓	✓	✓
Ersatzleistungen, Reparaturen oder Neuanschaffungen	–	✓	✓	–	✓	–	–	–	–
technischen Problemen wie Überspannung oder durch höhere Gewalt wie Blitzschlag	✓	–	✓	–	–	–	–	–	–
gefälschten, ausgespähten und abgefangenen Daten, Computersabotage, Erschleichen von Zugangsdaten	✓	✓	✓	✓	✓	✓	✓	✓	✓
Diebstahl von Datenträgern inkl. Folge- und Nebenschäden	–	✓	✓	✓	–	–	✓	✓	✓
Internetbetrug oder Urkundenfälschung	–	✓	✓	✓	–	–	✓	✓	–
Erpressung über das Internet	–	✓	✓	✓	✓	✓	✓	✓	✓
Unternehmensmitarbeitern, die Schwachstellen in Informations- und Kommunikationstechnologien sowie Kontrollmaßnahmen ausnutzen	–	✓	✓	✓	✓	–	✓	✓	✓
vorsätzlichen Programm-/Datenänderungen durch Mitarbeiter/vorsätzlicher, widerrechtlicher Nutzung von IT-Systemen der Mitarbeiter	–	✓	✓	✓	✓	–	✓	✓	✓
Verdienst- und Ertragsausfällen bei Betriebsstörungen	✓	✓	✓	✓	✓	✓	✓	✓	✓
Aufrechterhaltung des Geschäftsbetriebs	✓	✓	✓	✓	✓	✓	✓	✓	✓
Wiederherstellung gestohlener/zerstörter/beschädigter/blockierter Daten/Datenträger/Programme/Netzwerke nach einer Cyberattacke	✓	✓	✓	✓	✓	✓	✓	✓	✓
Wiederbeschaffung gestohlener/zerstörter Daten und physischer Datenträger nach einer Cyberattacke	✓	✓	✓	✓	✓	–	✓	✓	✓
Schadensermittlung	✓	✓	✓	✓	✓	✓	✓	✓	✓
Beauftragung externer IT-Forensik-Sachverständiger und IT-forensischer Untersuchungen	✓	✓	✓	✓	✓	✓	✓	✓	✓
Auswertungen von Daten und elektronischen Dokumenten im Rahmen von Rechtsstreitigkeiten oder regulatorischen/behördlichen Anfragen	–	✓	✓	✓	–	–	✓	–	✓
Rechtsverfolgung	✓	✓	✓	✓	✓	✓	✓	–	–
Datenschutzverletzungen (z. B. zur Erbringung von Meldepflichten bei Datenschutzbehörden, Schadenersatzforderungen)	✓	✓	✓	✓	✓	✓	✓	✓	✓
Einschaltung eines externen Krisen- und Kommunikationsmanagers zwecks Reputationsschutz	✓	✓	✓	✓	✓	✓	✓	✓	✓
durch Cyberkriminelle verursachtem Missbrauch unternehmenseigener Computer	–	✓	✓	✓	✓	–	✓	✓	✓
Cyberangriffen bei verbundenen Dritten (z. B. Cloud-Anbieter, Geschäftspartner, die Unternehmensdaten nutzen/bereitstellen)	–	✓	✓	✓	–	–	✓	–	✓
Haftpflicht infolge von Hackerangriffen, Denial-of-Service-Attacken, Datenschutzverletzungen oder fehlerhafter digitaler Kommunikation	✓	✓	✓	✓	✓	✓	✓	✓	✓
durch den Versicherungsnehmer verursachten direkten oder indirekten Vermögensschäden bei dessen Kunden aufgrund von Softwareentwicklungsfehlern	–	–	✓	✓	–	–	–	–	–
unbeabsichtigter Verbreitung von Malware	✓	✓	✓	✓	✓	–	✓	✓	–
Rechtsverteidigung	✓	✓	✓	✓	✓	✓	✓	✓	✓
Welche Schäden deckt Ihre Cyberversicherung ausdrücklich nicht ab?									
Reputationsverlust	k. A.	–	✓	✓	–	–	–	–	✓
Schäden, bei denen der Verursacher nicht identifiziert werden konnte	k. A.	–	–	–	–	–	✓	–	–
Personen- und Sachschäden	k. A.	✓	✓	✓	✓	✓	–	✓	✓
Strafzahlungen nach Verurteilungen	k. A.	–	✓	✓	–	✓	–	✓	–
Urheberrechtsverletzungen	k. A.	–	–	–	–	–	–	–	–
Schäden, die über die reguläre Haftpflichtversicherung abgedeckt sind	k. A.	–	–	✓	–	–	–	–	✓
die durch eine andere Versicherung bereits abgedeckten Schadensfälle	k. A.	–	–	–	–	–	–	–	–
Lösegeldzahlungen	k. A.	k. A.	–	–	–	–	✓	–	–

* ausgefüllt auf Basis des gelieferten Produktinformationsblattes; ✓ ja/vorhanden/trifft zu; – nein/nicht vorhanden/trifft nicht zu; k. A. keine Angabe

solche Vorfälle, bei denen Mitarbeiter – bewusst oder unbewusst – zu Mittätern werden, erfordern das Einbinden externer Sachverständiger, die die Vorfälle objektiv aufklären und aufarbeiten.

Oft reagieren Unternehmen jedoch genau gegenteilig und versuchen, die Cybervorfälle eigenständig aufzuarbeiten, selbst wenn sie nicht über ausreichend interne Kapazitäten und Fachwissen verfügen. In der Regel führt das zu höheren Schäden, da es die Aufklärung verzögern kann. Zumeist findet in diesen Fällen keine tiefere Ursachenermittlung statt, das heißt, man läuft Gefahr, dass sich solche Vorfälle wiederholen, weil Schwachstellen, Täter und Motivationen nicht ermittelt wurden. Ein einfaches Beispiel wäre die Wiederherstellung einer Systemumgebung nach einem Schadsoftwarebefall, nach dem Motto „mal schauen, was passiert". So ist jedoch keine effektive Abwehrstrategie zukünftiger Vorfälle möglich. Weitere Schäden sind absehbar, ganz zu schweigen vom Reputationsschaden durch sich wiederholende Vorfälle.

Diesem finanziellen Risiko begegnen die Versicherer bewusst durch das Übernehmen der Kosten für die Schadensermittlung, das Einbinden externer IT-forensischer Sachverständiger sowie IT-forensische Untersuchungen.

Wahrung des guten Rufs

Versicherer tragen in der Regel zudem die Kosten für einen externen Krisen- und Kommunikationsmanager, der die Reputation des Unternehmens schützt, sowie von Juristen für die Rechtsverteidigung sowie -verfolgung. Versicherer weisen vereinzelt darauf hin, dass es sich nicht um einen aktiven Rechtsschutz handelt. Unternehmen sollten ihren Versicherer nach der freien Auswahl eines Sachverständigen, Krisenmanagers oder Rechtsanwaltes fragen und sich über eine Deckelung der Honorarsätze oder des Gesamthonorars informieren. Häufig stellen Versicherer Kontakte zu Experten her, deren Beauftragung und Kostendeckung bereits abgestimmt und freigegeben ist. Dies erleichtert auch schnelles Reagieren im Ernstfall.

Betrifft der Cybervorfall personenbezogene Daten, sind möglicherweise Datenschutzbehörden zu informieren. Die Aufwendungen dafür übernehmen alle befragten Versicherungsunternehmen. Auch hier lohnt sich aber die Nachfrage, ob darüber hinaus mögliche Meldepflichten im Rahmen des seit Juli 2015 geltenden IT-Sicherheitsgesetzes oder das Publizieren eines Vorfalls in überregionalen Tageszeitungen im Einzelfall gedeckt sind.

Leichte Unterschiede zwischen den Versicherungen ergeben sich im Hinblick auf die Behandlung von Schäden durch interne Täter – nach wie vor eines der meistunterschätzten Risiken rund um den Begriff „Cyber", der stark von der Vorstellung eines externen Angriffs über ein Netzwerk geprägt ist. Dennoch übernehmen fast alle Versicherer die Schäden infolge des Löschens und Manipulierens von Daten durch Bedienungsfehler. Bei genauer Betrachtung handelt es sich dabei nicht um einen Cyberangriff, aber um Vorfälle in einer Cybersystemumgebung mit potenziell vergleichbaren Auswirkungen. Die zentrale Frage an den Versicherer sollte hier lauten: Ist nur der veränderte Zustand der Daten selbst oder die daraus resultierende Auswirkung gedeckt? Beispiele sind etwa falsch konfigurierte Produktionsanlagen oder Handelsplattformen mit asynchronen Systemzeiten.

Eine vergleichbare Konstellation findet sich bei der Deckung von Schäden durch das unbeabsichtigte Verbreiten von Malware, etwa durch Weiterleiten befallener E-Mail-Anhänge oder verseuchte Websites. Auch diese Schäden sind durch fast alle Versicherungsanbieter gedeckt. Zwei Anbieter würden darüber hinaus direkte oder indirekte Vermögensschäden bei Kunden des Versicherungsnehmers aufgrund von Softwareentwicklungsfehlern übernehmen.

Ganz ähnlich handhaben die Versicherer die Problematik der internen Täter, die vorsätzlich handeln: Gedeckt sind Schäden, die auf Mitarbeiter zurückzuführen sind, die Schwachstellen in Informations- und Kommunikationstechnologien sowie Kontrollmaßnahmen ausnutzen. Auch Schäden durch vorsätzliche Programm- und Datenänderungen durch Mitarbeiter sowie die widerrechtliche Nutzung von IT-Systemen werden von fast allen Versicherungsanbietern reguliert. Darüber hinaus sind neben den durch Vorsatz entstehenden Schäden auch solche infolge fehlerhaften Handelns gedeckt. Zu erfragen bleibt allerdings beim Versicherer der Umgang mit fahrlässigem Handeln.

Wenn Dritte involviert sind

Besonders aufzupassen gilt es bei den Regelungen zu Cyberangriffen auf verbundene Dritte, zum Beispiel Cloud-Anbieter oder Geschäftspartner, die Unternehmensdaten nutzen oder bereitstellen. Hier bietet sich bei den Versicherern ein äußerst heterogenes Bild. Letztendlich verdeutlicht

das die Notwendigkeit einer intensiven Diskussion darüber, wie verbundene Dritte zu definieren sind. Sind davon auch Konzerngesellschaften betroffen? Wie sind Minderheitsbeteiligungen geregelt? Ist die Möglichkeit der Einflussnahme auf verbundene Dritte erheblich?

Ausdrücklich nicht abgesichert werden bei fast allen Versicherern beispielsweise Personen- und Sachschäden. Strafzahlungen nach Verurteilungen sind bei einem Großteil ebenfalls explizit nicht gedeckt. Dafür übernehmen einige Anbieter auch die Kosten für Auswertungen elektronischer Dokumente und Daten im Zusammenhang mit Rechtsstreitigkeiten oder regulatorischen beziehungsweise behördlichen Anfragen (auch E-Discovery genannt).

Die vorgenannten Beispiele zeigen, dass die Regelungen der Versicherungsanbieter versuchen, alle abgedeckten sowie alle ausdrücklich ausgeschlossenen Schadensfälle hinreichend zu definieren. Dennoch besteht für Versicherungsnehmer die Notwendigkeit, konkrete Risikoszenarien für das eigene Unternehmen zu definieren und diese im Risikodialog mit dem Versicherer anhand des jeweiligen Bedingungswerks zu prüfen. Nur so ist zu gewährleisten, dass der Versicherungsnehmer bekommt, was er sich von einer standardisierten, aber insbesondere auch individuell gestalteten Cyberversicherung erhofft.

Cyberversicherung – was ist das?

Im Gegensatz zu herkömmlichen Versicherungsprodukten unterscheiden sich Cyberversicherungen vor allen Dingen in ihrem ganzheitlichen, spartenübergreifenden und sachschadenunabhängigen Ansatz. So

Zielgruppen und Rahmenbedingungen

Anbieter	ACE*	AIG	Allianz	AXA	DUAL	HDI Gerling	Hiscox	W&W	Zürich DE
Name der Versicherung	ACE Data Protect PLUS	AIG Cyber-Edge 2.0	Allianz Cyber Protect	Byte Protect	DUAL Cyber Defence	HDI-Gerling Cyber+	Cyber Risk Management	Die Cyber-Police	Zurich Cyber & Data Protection
Zielgruppe von Unternehmen (gemessen am Umsatz in Euro)									
bis 10 Mio.	✓	✓	–	✓	✓	✓	✓	✓	–
ab 10 Mio. und unter 100 Mio.	✓	✓	–	✓	✓	✓	✓	–	–
ab 100 Mio. und unter 250 Mio.	✓	✓	✓	✓	✓	✓	✓	–	✓
ab 250 Mio. und unter 3 Mrd.	✓	✓	–	✓	✓	✓	✓	–	✓
ab 3 Mrd.	–	✓	–	–	–	✓	–	–	✓
geografische Zielmärkte	weltweit	DE, EU, USA	DE, EU, AU, ZA, Asien, weitere	DE, EU	DE, EU	DE, EU	DE, EU, USA	DE	DE, EU, USA, Asien
Maßgebliche Faktoren zum Versicherungsbeitrag und möglicher Deckungssummen									
Reifegrad der IT- und Informationssicherheit im Unternehmen	✓	✓	✓	✓	✓	✓	✓	✓	✓
Risiko von Drittschäden	✓	✓	✓	✓	✓	✓	✓	✓	✓
Risiko von Eigenschäden	✓	✓	✓	✓	✓	✓	✓	✓	✓
Vertragslaufzeit	✓	–	✓	–	–	–	✓	–	–
Mehrfachdeckung durch andere Versicherungen	–	–	✓	–	–	–	✓	–	–
Sonder- und Mehrfachleistungen	–	–	✓	–	–	✓	✓	–	–
Selbstbehalte	–	✓	✓	✓	✓	✓	✓	✓	–
Empfehlung zum Beibehalten bisheriger Versicherungsprodukte (zusätzlich zur Cyberversicherung); Begründung/Ergänzung	✓, ggf. Überprüfung und Anpassung des Portfolios	Individuell zu prüfen, in der Regel ergänzen sich die Versicherungsprodukte	✓, ggf. Überprüfung und Anpassung des Portfolios	✓, aber Vermeiden einer Mehrfachversicherung über Prüfung und ggf. Anpassung des Portfolios	✓	✓, da sonst kein risikoadäquater Versicherungsschutz	k. A., ggf. Überprüfung und Anpassung des Portfolios	✓, Erweiterung des Versicherungsschutzes, kein Ersatz	✓, Ausschließen von Deckungslücken
Deckungssumme									
minimale bzw. maximale Deckungssummen in Euro	mind. 250 000, max. 50 Mio.	mind. 500 000, max. 25 Mio.	kein Minimum, max. 100 Mio.	kein Minimum, max. 10 Mio.	mind. 50 000, max. 10 Mio.	mind. 1 Mio., max. 50 Mio.	mind. 250 000, max. 15 Mio.	mind. 125 000, max. 2 Mio.	mind. 1 Mio., max. 25 Mio.
Deckung der Feststellungskosten des Versicherungsfalls durch Dritte									
ja, ohne Einfluss auf die Höhe der Deckungssumme	–	–	✓	–	✓	–	✓	✓	–
ja, mit Einfluss auf die Höhe der Deckungssumme	✓	✓**	–	✓	–	✓	–	–	✓
nein	–	–	–	–	–	–	–	–	–
Eigenanteil									
definierter Betrag in Höhe von ... Euro	variabel	ab 1000	mind. 5000	ab 1000	variabel	variabel	1000 bis 500 000	1000	25 000 bis 10 Mio.
definierte Ausfallzeiten, deren Kosten selbst zu tragen sind, in Höhe von ... Stunden	variabel	12 (variabel)	–	ab 4, je nach Risiko	variabel	variabel	12	24	–

* ausgefüllt auf Basis des gelieferten Produktinformationsblattes; ** ja, im Rahmen der Höhe der Deckungssumme (ggf. auf vereinbarte Sublimits); ✓ ja/vorhanden/trifft zu; – nein/nicht vorhanden/trifft nicht zu; k. A. keine Angabe; DE Deutschland; EU Europäische Union; ZA Südafrika; AU Australien

werden sowohl Eigen- als auch Drittschäden (Haftpflichtkomponente) mitversichert. Ebenso wenig spielt die Herkunft des Täters (unternehmensintern oder -extern) eine Rolle, sie hat keinen Einfluss auf die Regulierung im Schadensfall. Zudem bieten Cyberversicherungen dem Kunden die Möglichkeit, sich zusätzliche Expertenunterstützung durch IT-Forensik-Sachverständige oder Kommunikationsmanager einzukaufen. Das ist laut den Versicherern konzeptionell bei den traditionellen Produkten nicht zu leisten.

Trotzdem sind sich die meisten Versicherungsunternehmen einig, dass Unternehmen ihre bisherigen Versicherungspolicen beibehalten sollten. Sie begründen es damit, dass die Cyberversicherung lediglich eine Erweiterung des Versicherungsschutzes als Reaktion auf eine wachsende Bedrohungslage ist und ihn nicht ersetzt. Dennoch empfehlen einige Versicherer ein Überprüfen und gegebenenfalls Anpassen des Versicherungsportfolios gegen Beitragsminderungen von anderen Policen. Hierbei ist zu beachten, dass die Cyberpolice zumeist vorrangige Deckung vor anderen Versicherungen hat. Oft sind die tatsächlichen Überschneidungen aber geringer als allgemein angenommen.

Das Abschließen einer Cyberpolice lohnt sich nach Ansicht der Versicherer grundsätzlich für jedes Unternehmen. Am meisten profitieren Industrieunternehmen, Dienstleister oder Firmen IT-naher Branchen, deren Umsätze stark von Informationstechnik abhängen.

Dauer des Versicherungsschutzes

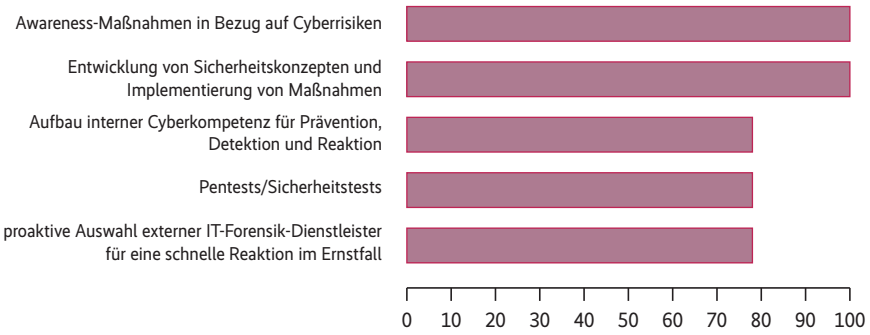
Die Versicherungsdauer, während der der Schutz besteht, variiert je nach Anbieter. Während bei manchen die Regelung existiert, dass das versicherte Ereignis innerhalb der Vertragslaufzeit erfolgen muss, gibt es bei anderen eine unbegrenzte Rückwärtsdeckung und eine automatische Nachhaftung von fünf Jahren. Fast alle Versicherer wenden das Claims-made-Prinzip an, das heißt, dass unabhängig vom Zeitpunkt des Schadeneintritts (etwa dem Erstzugriff durch einen Cyberkriminellen) der Zeitpunkt der Anspruchserhebung gegen den Versicherer (das Feststellen des Angriffs) ausschlaggebend ist. Sie ist also das Ereignis, das innerhalb der festgelegten Versicherungsdauer liegen muss.

Generell deckt das Angebot der Versicherer Unternehmen jeder Größe – gemessen am Umsatz – und sämtlicher Branchen ab (siehe Tabelle „Zielgruppen und Rahmenbedingungen“). Dabei konzentrieren sich die Versicherungsunternehmen zum Beispiel auf kleinere Unternehmen ausgewählter Branchen wie der produzierenden Industrie oder Transport und Verkehr mit einem Umsatz von unter 10 Millionen Euro. Ein anderer Schwerpunkt liegt auf Unternehmen mit einem Umsatz von bis zu 3 Milliarden Euro und einer übergreifenden Branchenabdeckung oder spezifischem Schwerpunkt auf Finanzdienstleistungsunternehmen. Einige Versicherer konzentrieren sich auf die produzierende Industrie ab einem Umsatz von 5 Millionen Euro. Aber auch Unternehmen jeder Branche ab einem Umsatz von 100 Millionen Euro sind eine Zielgruppe. Angesprochen werden dabei überwiegend der deutsche und europäische Markt.

Was man vor einem Abschluss wissen muss

Sollte man sich als Unternehmen dafür entscheiden, eine Cyberversicherung abzuschließen, kann man je nach Bedarf zwischen standardisierten Deckungsbausteinen und individuellen Lösungen wählen. Die Deckungssumme ist bei allen Versicherern nach oben und oft auch nach unten hin begrenzt. Die größte Flexibilität wird bei ausbleibender Minimalgrenze der Deckungssumme und einer Maximalgrenze bei 100 Millionen Euro erreicht. Individuelle Regelungen sind jedoch immer möglich. Der Eigenanteil des Versicherungsnehmers – auch im Hinblick auf vorab definierte Ausfallzeiten – ist mit den meisten Versicherern individuell verhandelbar. Untergrenzen liegen häufig bei 1000 Euro beziehungsweise vier Stunden (siehe Tabelle „Zielgruppen und Rahmenbedingungen“). Dies ist jedoch wie bei anderen Versicherungsformen stark abhängig vom gewählten Deckungsumfang.

Bevor Versicherer eine Police abschließen, unterziehen sie das zu versichernde Unternehmen einer Risikoprüfung. Art und Umfang dieser Prüfung hängen von der Deckungssumme, der Größe des Unternehmens und den exponierten Risiken ab. Das Spektrum ist breit und beginnt bei der Selbstauskunft durch Ausfüllen eines Fragebogens. Eine weitere Variante wäre ein Risikodialog zwischen internen Sachverständigen des potenziellen Versicherungsnehmers sowie IT-(Sicherheits-) und Forensik-Experten über den Gefährdungsgrad (welche Risiken bestehen konkret und wie groß wäre der mögliche Schaden?) und den vorhandenen Schutz (welche spezifischen Schutzmaßnahmen sind implementiert?). Schließlich sind auch so-



Mit einer Versicherung allein ist es nicht getan. Unternehmen sollten Mitarbeiter schulen und Sicherheitsmaßnahmen ergreifen – das verminderte Risiko schlägt sich unter Umständen in günstigeren Versicherungstarifen nieder (Abb. 2).

genannte Penetrationstests durch externe Sachverständige denkbar.

Standardisierte Beurteilungskriterien für die Gesamtbranche haben sich noch nicht etabliert. Allerdings gibt es Anbieter, die ihr Fachwissen in eine Software einfließen ließen. So ist eine online durchgeführte Selbsteinschätzung (Self-Assessment) ebenso möglich wie die Darstellung der unternehmenseigenen Risikodisposition und Reaktionsfähigkeit auf Cybervorfälle im Benchmark. Bei Bedarf fließen in die Assessments Umfeldanalysen in der Branche und Recherchen zur Schadenshistorie ein. Das Hinzuziehen unabhängiger Sachverständiger für die Risikobeurteilung im Vorfeld des Versicherungsabschlusses – egal durch welchen der beiden Vertragspartner – ist eine etablierte Option, die das Verfahren vereinfacht und objektiviert.

Der Versicherungsbeitrag und die tatsächlich festgesetzte Versicherungssumme ergeben sich vor allem aus dem Reifegrad der IT- und Informationssicherheit im Unternehmen, dem Selbstbehalt und dem Risiko von Dritt- und Eigenschäden. Das mögliche Ausmaß Letzterer leitet sich sowohl von den Sicherheitsmaßnahmen ab, die einen Cybervorfall verhindern sollen (Intrusion Prevention), als auch von denjenigen zum Erkennen (Intrusion Detection) eines Vorfalls sowie ersten Reaktionen darauf (Incident/Cyber Response). Immer mehr an Bedeutung gewinnt in diesem Zusammenhang die Fähigkeit von Unternehmen, über die eigentliche Abwehr und Schadensbegrenzung hinaus entscheiden zu können, welcher Vorfall forensische Reaktionsmaßnahmen im Sinne einer gerichtsfesten Beweisdatensicherung und -analyse erfordert, und entsprechende interne und externe Spezialisten umgehend zu mobilisieren.

Um den Versicherungsbeitrag zu reduzieren und die Versicherungssumme zu erhöhen, können Unternehmen einen aktiven Beitrag in Form von Zertifizierungsnachweisen und externen IT-Audits leisten. Generell ist die Vorbereitung auf einen Schadensfall durch das Erstellen von Notfall-, Management- und Wiederanlaufplänen mit definierten Verantwortlichkeiten und regelmäßig durchgeführten Penetrationstests, Notfallübungen und Systemupdates zu empfehlen. Einige Versicherungsanbieter bieten auch präventive Maßnahmen an. Unternehmen sollten ihren Versicherungsanbieter oder Makler darauf ansprechen.

Wenn der Schadensfall eintritt

Kommt es zum Schadensfall, ist die Erstreaktion besonders kritisch. Unklare Zuständigkeiten sowie Fehler in der Beweissicherung und der Kommunikation haben oft irreparable Auswirkungen. Auch die Versicherer weisen im Falle eines Schadens auf die Wichtigkeit der sofortigen Kontaktaufnahme mit dem dafür vorgesehenen Notfall-Service und gegebenenfalls internen IT-Sicherheitsexperten hin. Konkret besteht dieser Notfall-Service der Versicherer in einer Notfall-Hotline, zumeist ergänzt von einer umfangreicheren Cyber-Assistance durch IT-Forensik-Experten.

Diese stellen mit ihrer Erfahrung und globalen Netzwerken sicher, dass die Beteiligten schnell, koordiniert und angemessen auf die Situation reagieren, selbst wenn zeitgleich an mehreren Unternehmensstandorten Reaktionsmaßnahmen erforderlich sind. Sie unterstützen bei der Schadenseindämmung, Beweisdatensicherung und -analyse, Aufarbeitung sowie Bewältigung des Schadens. Sie geben Empfehlungen zum Beheben des Cybervorfalls oder für das Einbinden weiterer Spezialisten, beispielsweise Anwaltskanzleien. Zumeist handelt es sich dabei um Wirtschaftskanzleien, spezialisiert auf Datenschutzrecht, Arbeitsrecht und Strafrecht. Für Unternehmen ist es wichtig zu berücksichtigen, dass Cybervorfälle keiner technisch orientierten Reaktion und Aufarbeitung bedürfen.

In der Regel sind nicht nur beim eigentlichen Cyberangriff personenbezogene Daten von Kunden oder Mitarbeitern des Unternehmens betroffen. Auch bei der nachfolgenden Untersuchung können Persönlichkeitsrechte der Betroffenen verletzt werden. Die Gestaltung der Sonderuntersuchung (das „Wie" der Maßnahme) könnte ein Mitbestimmungsrecht des Betriebsrats begründen, das in der Regel mit einer vollumfänglichen Beteiligung der Arbeitnehmervertretung einhergeht. Darüber hinaus stellt sich gerade beim Aufarbeiten des Vorfalls die Frage, ob und inwieweit das Datenleck durch ein strafbares Verhalten eines Mitarbeiters entstand und ob dieses Fehlverhalten strafrechtlich und arbeitsrechtlich sanktioniert werden kann.

IT-Forensiker arbeiten überdies eng mit PR-Beratern zusammen. Sie stellen die komplexen technischen Sachverhalte einfach und verständlich dar und ermöglichen somit klare Aussagen nach innen und außen. Sie wissen auch im Bedarfsfall, für welche ausgewählten Einzelfragen weitere technische Spezialisten, beispielsweise für Fragen zu proprietärer Software, einzubeziehen sind.

Nach Beurteilung der Versicherer nehmen die IT-Forensik-Experten eine Schlüsselrolle im Schadensfall ein. Ergänzend zur Weiterführung der Geschäfte (Krisenmanagement, Business Continuity Management, Disaster Recovery) sichern sie den Bestand der Daten und Beweise während und nach einer Krise. Im Bedarfsfall definieren sie auch Kriterien für ein vertieftes Monitoring kritischer Daten und Systeme für einen Übergangszeitraum, um ein erneutes Aufflammen komplexer Vorfälle zu verhindern. In Zeiten, in denen man davon ausgehen kann, dass früher oder später jedes Unternehmen von Sicherheitsvorfällen betroffen sein wird, trägt die professionelle Reaktion im Ernstfall auch dazu bei, Reputationsschäden zu reduzieren.

Der gute Ruf ist unbezahlbar

Diese können gravierende Folgen für ein Unternehmen haben, selbst wenn der daraus resultierende finanzielle Schaden nur schwer messbar und der Zusammenhang mit dem Ereignis vielleicht nicht zu belegen ist. Aus diesem Grund decken einige Versicherer das Risiko des Reputationsverlusts ausdrücklich nicht ab.

Konkret bezifferbar sind hingegen Maßnahmen im Zusammenhang mit Reputationsschäden, zum Beispiel die Kosten für Kampagnen zur Neukundenakquise nach einem ereignisbedingten Kundenverlust.

Gerade für kleine und mittelständische Unternehmen ist das Einbeziehen externer Spezialisten enorm wichtig, da entsprechende Fachkenntnisse oftmals nicht intern vorhanden sind. Die Feststellungskosten des Versicherungsfalls durch IT-Forensik-Sachverständige sind von den Versicherern gedeckt. Bei manchen Cyberversicherungen kann dies Einfluss auf die Höhe der Deckungssumme haben (siehe hierzu Tabelle "Zielgruppen und Rahmenbedingungen").

Einfluss auf die Regulierung im Schadensfall kann auch der Sitz eines Unternehmens haben sowie der internationale Standort, an dem der Angriff erfolgt beziehungsweise der Schaden entstanden ist. So schließen manche Versicherer eine Haftung in den USA aus, da dort deutlich höhere Schadenersatzforderungen und Geldstrafen zu erwarten sind.

Zusätzliche Maßnahmen zur Cyberversicherung

Als Ergänzung zu einer Cyberversicherung empfehlen die Versicherer einhellig die Sensibilisierung von Mitarbeitern für Cyberrisiken sowie das Einführen von Sicherheitskonzepten im Unternehmen. Mehrheitlich empfehlen sie zudem den Aufbau interner Kompetenz für Prävention, Detektion und Reaktion, Penetrations- und Sicherheitstests sowie die proaktive Auswahl externer IT-Forensik-Dienstleister für eine schnelle Reaktion im Ernstfall (Abbildung 2).

Insbesondere Sensibilisierungsmaßnahmen für die Beschäftigten liegen in der Rangordnung weit vorne, da Unachtsamkeit als Nummer eins der begünstigenden Faktoren für Cyberkriminalität gilt. So können gezielt eingesetzte Mittel die nötige Umsicht im Umgang mit Systemen, Daten, Prozessen sowie potenziellen Tätern fördern. Bei der Planung und Einführung von Sicherheitskonzepten sind sinnvolle erste Schritte beispielsweise Schulungen zur Verschlüsselung von Daten und Datenträgern sowie eine regelmäßige Überprüfung des Schutzbedarfs von Daten und Systemen. Beim Aufbau interner Cybersachkenntnis für Prävention, Detektion und Reaktion könnte der angespannte Markt für Fachkräfte mit notwendiger Qualifikation ein Hindernis sein.

Was die Zukunft bringt

Maßnahmen zum Reduzieren des Risikos von Cyberangriffen werden immer wichtiger. Das belegt unter anderem der Bericht zur Lage der IT-Sicherheit des BSI („Alle Links"), aus dem hervorgeht, dass mit der zunehmenden Digitalisierung und Vernetzung auch eine dynamische Gefährdungslage einhergeht. Dies zeigt auch in der erwähnten KPMG-Studie die diesbezüglich pessimistische Einschätzung der Unternehmen (Abb. 1)

Ein Teil der Versicherer vermutet angesichts des steigenden Risikos, Opfer von E-Crime zu werden, dass es vermehrt zu Allianzen mit Rückversicherern kommt. Unterstützt wird diese Annahme von der sich kontinuierlich steigernden Nachfrage nach Cyberpolicen seit ihrer Markteinführung. Hier sehen die Versicherungsunternehmen eine deutliche Entwicklung in den nächsten fünf Jahren hin zu einer etablierten Standardversicherung für Unternehmen. Vor allem Unternehmen, deren Geschäftsbetrieb in hohem Maße von IT abhängig ist und die einen großen Bekanntheitsgrad genießen, dürften sich zunehmend an die Cyberversicherer wenden.

Aus Sicht der Autoren wird der Aspekt der Standardisierung der Cyberversicherung einhergehen mit einer verfeinerten Methodik, die messbare Reaktionsfähigkeit von Unternehmen auf Cybervorfälle in Beziehung zu Versicherungsbeitrag und -summe zu setzen. Zwangsläufig ist dafür eine breitere Basis von ausgewerteten Schadensfällen und Vergleichsinformationen zum Reifegrad der Unternehmen notwendig. Mit der Standardisierung wird auch der Bedarf der Versicherungsanbieter verbunden sein, sich mit ihrem Produkt von dem der Konkurrenz zu unterscheiden – idealerweise aber nicht vorrangig durch den Preis. Versicherer werden im Zuge des individuellen Vertragsabschlusses dann zunehmend auf Unternehmen treffen, die ganz genau wissen, welche ihre spezifischen Cyberrisiken sind und wie sie ihnen wirksam begegnen. (ur)

Alexander Geschonneck

leitet als Partner bei der KPMG AG Wirtschaftsprüfungsgesellschaft das Forensic Team in Deutschland.

Thomas Fritzsche

ist als Senior Manager im Cyber Forensic Team der KPMG AG für Cyber Insurance Assistance Services verantwortlich.

Alle Links: www.ix.de/ix1509040