

- Immer mehr deutsche Versicherer wagen sich mit Cyber-Versicherungen auf den Markt. Die modular aufgebauten Policen versprechen Hilfe bei einem Angriff auf die Informationstechnik. Versicherungsvermittler und Makler zeigen sich indes zurückhaltend beim Vertrieb der Cyber-Risiken. Welche Gefahren deckt die neue Sparte konkret ab? Wo liegen die Grenzen der Versicherbarkeit? Und was ist beim Vertrieb der Policen zu beachten?

Was zeichnet eine Cyber-Versicherung überhaupt aus? Was ist das Neue an diesen Policen? Und welche Inhalte verbergen sich konkret in den Policen der Versicherer? Eine einheitliche Definition, die wissenschaftlich und branchenübergreifend akzeptiert und verifiziert ist, gibt es nicht. Das liegt allein daran, dass es sich bei dieser Sparte um ein recht junges Betätigungsfeld handelt. Allein die Bezeichnung der entsprechenden Policen kann variieren. Neben dem Schlagwort „Cyber-Versicherung“ können gleichfalls weitere Synonyme verwendet werden. So kann ebenso gut von einer Hacker-Versicherung, oder besser einer Anti-Hacker-Versicherung, gesprochen werden. Weitere alternative Bezeichnungen können zum Beispiel sein: Datenschutz-Versicherung, Elektronik-Versicherung, IT-Versicherung, Web-Versicherung, Online-Schutz-Versicherung, Multimedia-Versicherung, Cyberspace-Versicherung, Cybercrime-Versicherung, usw.

Das Bundeskriminalamt (BKA) hat in seinem *Bundeslagebild 2012* unter dem Stichwort „Cybercrime“ strafrechtlich relevante Delikte zusammengefasst. Zu diesen zählen unter anderem der Computerbetrug, die Datenfälschung, die Computersabotage, das Ausspähen von Daten, das Abfangen von Daten einschließlich deren

Vorbereitungshandlungen. Eine Antwort auf die Frage, was das Wesen einer Cyber-Versicherung im Kern ausmacht, erhält man deshalb sehr gut, wenn man sich die versicherten Risiken, die diese Policen versprechen abzusichern, anschaut. Und der Versicherungs- respektive Deckungsumfang ist natürlich auch ein Spiegel der Risiken, die unter anderem das BKA in seinen jährlichen Lagebildern analysiert.

So leisten Cyber-Versicherungen klassischerweise bei einer Beschädigung von Daten, einem Diebstahl von Daten oder einer unerlaubten Veröffentlichung von Daten. Die Policen helfen bei der Datenwiederherstellung, bei einer Betriebsunterbrechung, bei der Krisenkommunikation, der Benachrichtigung von Kunden, Dienstleistern und weiteren Betroffenen. Zum Leistungsumfang der Policen gehört ebenso die Kostenerstattung bei der Ursachensuche, also Kosten für IT-forensische Untersuchungen für Software-Spezialisten. Zum Deckungsumfang zählen auch aus Datenrechtsverletzungen resultierende Haftpflichtansprüche, Kosten für Rechtsstreitigkeiten oder Hilfe bzw. Schadenersatz bei einem Fehlverhalten von Mitarbeitern oder bei einer Verletzung von Betriebsgeheimnissen. Die Leistungen reichen bis zur Erstattung der Kosten bei einer Cyber-Erpressung. Auch der Cloud-Ausfall kann inzwischen bei einigen Anbietern versichert werden. So ziemlich alle in einem Schadenfall entstehenden Kosten können versichert werden: Belohnungen für die Ergreifung der Täter, Vertragsstrafen, Bußgelder oder auch der Reputationsverlust. „Unter den Internet-Risiken nimmt die Betriebsunterbrechung eine zentrale Stellung für Unternehmen ein“, schildert ein Versicherer, weshalb auch diese Gefahr in den Bausteinen vertreten ist.

2.1 Vertrieb: Keine Gießkannen-Beratung

Die Liste der versicherbaren Gefahren ließe sich noch um einige weitere Deckungsmöglichkeiten ergänzen. Die beispielhafte Auflistung zeigt jedoch: der Katalog an aktuell, heute schon zu versicherbaren Schäden und Kosten umfasst ein recht breites Spektrum. Eine Herausforderung im Vertrieb besteht deshalb darin, gemeinsam mit den Kunden jene passgenauen, individuellen Bausteine herauszunehmen und aufeinander abgestimmt zusammenzustellen, die der Kunde tatsächlich für seinen Betrieb benötigt. Hierzu bedarf es vorab einer risikotechnischen Analyse der IT-Sicherheit. Es gibt in diesem Bereich nämlich keine pauschale Gießkannen-Lösung. Die Versicherer bieten allesamt ihrem Vertrieb im gesamten Prozess aktive Hilfestellung an. Die Vermittler sollten sich nicht scheuen, diese Hilfen aktiv in Anspruch zu nehmen. Die Risikoanalyse startet meist mit einem Fragenkatalog, mit einer Selbstauskunft des Kunden.

Anhand der Antworten kann bereits eine erste Bewertung vorgenommen werden, wie es um die IT-Sicherheit steht und welchen Risiken das Unternehmen aus-

gesetzt ist. Hier hilft auch die Frage, was das Unternehmen im Kern ausmacht. An welcher Stelle ist es am verwundbarsten? Der Vertrieb sollte den Mehrwert dieser Beratungsleistung unterstreichen. Der Kunde bekommt im Idealfall nämlich einen Überblick über seinen aktuellen Schutz. Mit der Analyse des Status quo kann der Kunde zunächst Lücken in seiner IT zum Beispiel durch den Einsatz neuer Software minimieren. Wissensdefizite der Mitarbeiter können durch gezielte Weiterbildung angegangen werden. Oder durch Änderungen innerbetrieblicher Strukturen wird der Gefahr eines IT-Angriffs vorgebeugt. Das verbleibende Restrisiko, die Kronjuwelen, kann der Kunde dann in eine Cyber-Police stecken. Einer der Gründe nämlich, weshalb die Mehrzahl der Unternehmen immer noch ohne IT-Versicherungsschutz dasteht ist der Vertrieb.

Die Versicherungsvertriebe und die Makler scheuen, wie es in einer Studie der Beratungsgesellschaft Steria Mummert Consulting heißt, den „aufwendigen und haftungsträchtigen Verkauf einzelner Gewerbeprodukte“ (*Branchenkompass 2013 Versicherungen*). Diese Studie von Oktober 2013 zeigt, dass viele unternehmerische Risiken unentdeckt bleiben, schlicht weil Vermittler im Kundengespräch nicht danach fragen. Hierzu zählen vor allem Cyber-Risk-Versicherungen, die heute kaum angeboten würden. „Null-Risiko gibt es nicht, das ist den meisten IT-Entscheidern klar. Die Bedrohungen nehmen zu und die Angriffe werden aggressiver und erfolgreicher“, kommentiert Gerald Spiegel, Leiter Information Security Solutions bei Steria Mummert Consulting, die Studienergebnisse.

„Neben der notwendigen Vorhaltung und Beachtung der Security-Policy ist es daher heute wichtiger denn je, risikoorientiert zu handeln“. Dazu gehöre, sich rechtzeitig gegen Cyber-Angriffe zu versichern und so die möglichen negativen Folgen eines Betriebsausfalls zu minimieren. „Viele Unternehmen sind gegenüber einer solchen Bedrohung kaum abgesichert“, ergänzt Lars Matzen, Versicherungsexperte von Steria Mummert. Häufig sei dies die Folge einer unvollständigen Beratung. Eine massive Unterbrechung des Geschäftsbetriebs werde dann für den Gewerbetreibenden schnell zur wirtschaftlichen Überlebensfrage. „Mit einer schrittweisen Verbesserung der Beratungsqualität ist aus unserer Sicht deutlich mehr Geschäft mit Gewerbekunden möglich“, ist Matzen überzeugt. Versicherer und ihre Vertriebspartner sollten deshalb eine Gruppe von Vermittlern auswählen und sie intensiv in den Gewerbethemen und Produkten schulen, empfiehlt der Berater. Mit Hilfe moderner Softwaretools könnten Gewerbeberater nahezu jedes Risiko aufdecken, das in dem Betrieb vorhanden sei und so ihren Kunden passende Versicherungsleistungen anbieten.

„Eine moderne Beratungssoftware unterstützt den Vermittler mit einem Katalog mit mehr als 1.000 möglichen Fragen. Eine solche Software unterstützt den Beratungsprozess zielgerichtet, indem nur die relevanten Fragen zum Einsatz kommen und so Expertenwissen eingebracht wird“, so Matzen. „Die Mitglieder sind weit-

gehend informiert, dass es diese neue Versicherungsform gibt“, hakt der *Verband Deutscher Versicherungs-Makler e. V. (VDVM)* ein. Die überwiegende Anzahl der Mitglieder spreche das Thema bei den Kunden auch an. „Das Marktpotential wird erkannt“, so der VDVM. Allerdings seien die Kunden selber überwiegend noch nicht über das Thema Cyber-Versicherungen informiert, würden aber durch die ständige Medienberichterstattung in zunehmenden Umfang über das Risiko als solches sensibilisiert. In geringem Umfang sprächen die Kunden inzwischen sogar die Makler von sich aus an, so die Erfahrung beim VDVM.

„Unsere Erfahrung hat gezeigt, dass die Risiken im Umgang mit Daten sehr individuell sind“, ergänzt die Allianz. Daher sollte man auf die Kunden unvoreingenommen zugehen, nicht gleich mit einer fertigen Lösung, rät der Versicherer. Cyber-Risiken seien nämlich vielfältig und jede Branche habe ihre Besonderheiten, an die man die Versicherungslösungen anpassen müsse. So hätten produzierende Unternehmen in der Regel einen größeren Versicherungsbedarf im Bereich der Betriebsunterbrechung. Sollte der Kunde jedoch mehr mit Daten Dritter arbeiten, wie zum Beispiel Krankenversicherer, Kaufhäuser, Hotels, sollte bei der Risikobetrachtung der Fokus stärker auf den Umgang mit den personenbezogenen Daten gelegt werden. Da die Analyse des jeweiligen Risikos komplex sei, stünden „erfahrene Underwriter und Risikoexperten“ für Gespräche beim Kunden zur Verfügung. „Es ist nämlich nicht nur eine Versicherungspolice – der Mehrwert durch Assistance-Dienstleistungen ist ebenfalls ein wichtiger Bestandteil des Gesamtkonzeptes“, so die Allianz.

„Für die Makler gilt eigentlich das Gleiche wie für die Versicherer“, fasst Marcel Braun zusammen, Head of Professional Lines für Deutschland, Österreich und Osteuropa bei der XL Group. Man müsse vorab sorgfältig analysieren, über welche bestehenden Policen der Kunde vielleicht schon (teilweise) abgesichert sei, und wo es Deckungslücken gebe. Dann müsse man den Kunden fragen, ob er bereit ist, diese verbleibenden Risiken selbst zu tragen oder lieber doch mit einer vollwertigen Cyber-Versicherung abzudecken. „Ganz wichtig in diesem Zusammenhang ist aber auch die Frage, wie ich Risiken vorbeugen kann“, so Braun. Denn der beste Schutz sei immer dann gegeben, wenn der Schadenfall erst gar nicht eintrete oder eintreten könne. Hier könnten am besten regelmäßig durchgeführte Penetrations-tests helfen, die Schwachstellen im IT-System der Kunden aufdecken, um sie dann ganz gezielt zu schließen. „Als Makler sollte man also auch darauf achten, dass der Versicherer ein Servicepaket mitliefern kann und nicht nur eine Geldersatz-Lösung parat hat“, rät denn auch Braun.

Nach wie vor werde das Verständnis über den Umfang der Deckung, die Risikoermittlung und der Mehrwert oft nicht richtig verstanden, bilanziert CNA-Manager Dittmann. Hierin sieht er einen Grund für das noch zögerliche Kaufverhalten seitens der Kunden. „Aber auch die Unkenntnis und Unsicherheit vieler Makler

hindert uns als Versicherer daran, dass Produkt beim Kunden richtig zu platzieren“, sagt Dittmann selbstkritisch. Die Makler müssten sich strategisch überlegen, wie sie das Thema beim Kunden platzieren, ohne die IT-Abteilung direkt zu involvieren. „Wir stellen fest, dass dies oft nicht zielführend ist, weil die IT Abteilung sich unter permanentem Rechtfertigungszwang sieht – zu Unrecht!“, sagt Dittmann. Die erfolgreichen Abschlüsse gingen auf ein Zusammenspiel zwischen kaufmännischer Leitung und IT unter der Einsicht nur limitiert machbarer, technischer Sicherheit zurück. „Auch geben wir den Maklern immer den Hinweis, sich auf Branchen und Kunden zu konzentrieren, bei denen sie sich gut auskennen und eine gute Beziehung haben. Nur dann hat der Makler auch die innere Sicherheit ein Thema anzusprechen, in dem er sich unsicherer fühlt, als in klassischen Versicherungssparten“, so Dittmann. Er ergänzt: „Wir als CNA können vorbereitend für diese Termine eine branchenspezifische Präsentation mit Schadenbeispielen, Deckungsschwerpunkten und auch erste Preisindikationen erstellen und dem Makler zur Verfügung stellen oder den Makler bei den Kundenterminen begleiten“. Weiter habe CNA eine Kooperation mit einem IT-Unternehmen, welches sich auf das Entdecken von ungewöhnlichen Netzaktivitäten in Unternehmen spezialisiert habe. Diese Technik setze erst nach Firewall und Antiviruschutz an. „Kritische Kunden können wir diese Technik für 30 Tage kostenlos zur Verfügung stellen, so dass wir danach aufzeigen können, was im Unternehmen bereits nach den klassischen Schutzmechanismen passiert. In der Regel geht es in der Kundendiskussion dann nicht mehr um das ‚ob‘ der Cyber-Versicherung, sondern um das ‚wie‘“, schildert Dittmann.

2.2 Die sieben größten IT-Risiken

Doch selbst Fachleute für Cyber-Sicherheit sind sich nicht darüber im Klaren, wie sich der Ausfall einzelner Unternehmen oder Technologien zu einem systemweiten Risiko ausweiten könnte. Das geht aus einer Untersuchung des Versicherers Zurich hervor. Die Abhängigkeit von der Informationstechnologie habe ein komplexes Netz aus eng miteinander verbundenen Risiken geschaffen, so der Versicherer. Das Internet sei das komplexeste System, das die Menschheit jemals entworfen habe, so Zurich-Risikomanager Axel Lehmann. Über die letzten Jahrzehnte habe sich das Internet zwar als unglaublich widerstandsfähig erwiesen. Doch das Risiko liege darin, dass die „Komplexität, die den Cyberspace relativ risikolos gemacht hat, sich als Bumerang erweisen kann und sehr wahrscheinlich wird“, lautet denn die Einschätzung von Chief Risk Officer Lehmann. Der „*Zurich Cyber Risk Report*“ listet sieben miteinander verbundene Risiken auf (Tab. 2.1).

Tab. 2.1 Die Cyber-Schocks der Zukunft. (Quelle: Zurich Insurance Group Ltd)

Risiko	Beschreibung	Beispiele
Interner IT-Betrieb	Risiken eines Unternehmens im Zusammenhang mit dem kumulierten Zusammenspiel der (hauptsächlich internen) IT	Hardware; Software; Server und damit verbundene Personen und Prozesse
Kontrahenten und Partner	Risiko durch die Abhängigkeit von oder direkte enge (normalerweise nicht vertraglichen) Verbindungen mit einem externen Unternehmen	Universitäre Forschungspartnerschaften; Beziehungen zwischen konkurrierenden/kooperierenden Banken; Joint-Venture-Unternehmen; Branchenverbände
Outsourcing und Vertragsdienstleistungen	Risiko, normalerweise aus einem Vertragsverhältnis mit externen Dienstleistern, z. B. aus den Bereichen Personalwesen, Recht oder IT sowie Cloud-Providern	IT und Cloud-Provider; Personalwesen, Recht, Buchhaltung und Beratung; Auftragsfertigung
Supply Chain	Sowohl Supply Chain-Risiken für die IT-Branche als auch Cyber-Risiken für traditionelle Supply Chains und Logistik	Engagement in einem einzigen Land; gefälschte oder manipulierte Produkte; Risiko der Unterbrechung von Supply Chains
Umwälzende Technologien	Risiken aus unsichtbaren Auswirkungen von Störungen durch oder an neuen Technologien, die entweder bereits bestehen aber wenig verstanden werden oder bald erscheinen	Internet der Dinge; Smart Grid; eingebaute mechanische Geräte; selbstfahrende Autos; die weitgehend automatische digitale Wirtschaft
Vorgelagerte Infrastruktur	Risiken aus der Störung von Infrastruktur, auf die Wirtschaften und Gesellschaften angewiesen sind, insbesondere Elektrizität, Finanzsysteme und Telekommunikation	Internetinfrastruktur wie Internetknotenpunkte und Unterwasserkabel, bestimmte Schlüsselunternehmen und zum Betrieb des Internets verwendete Protokolle (BGP und Domain Name System); Internet Governance
Externe Schocks	Risiken aus Vorfällen außerhalb des Systems, jenseits der Kontrolle der meisten Unternehmen und mit der Wahrscheinlichkeit einer Ausweitung	Ernste internationale Konflikte; Malware-Pandemie

2.3 Kumulgefahren rückversichern

„Für Unternehmen ist es selbstverständlich, dass sie ihre Fabrikgebäude gegen Feuer und andere Gefahren versichern. An das Firmennetzwerk denken jedoch nur wenige“, so Johannes Behrends vom internationalen Versicherungsmakler *Aon Risk Solutions (Aon)*. So fordert Thomas Blunck, Mitglied des Vorstands beim *Rückversicherer Munich Re*, dass eine „adäquate Versicherung gegen Datenschutzverletzungen... ein Standardelement der Gewerbeversicherung“ sein sollte. „Denn jedes Unternehmen kann in diesem Kontext Umsatzeinbußen oder einen Imageverlust erleiden“, so Blunck. Blunck verweist auf ein Ergebnis eines britischen Marktforschungsunternehmens, nach dessen Angaben „in Europa bislang nur fünf Prozent der Unternehmen gegen Cyber-Risiken versichert sind“. Hingegen betrage der Anteil bei großen US-Unternehmen 30%, die mit einer Cyber-Risiko-Deckung ausgestattet seien. Vorstandsmitglied Blunck, der u. a. für den Bereich Special and Financial Risks zuständig ist, sieht dennoch eine gestiegene Sensibilität für Angriffe aus dem Netz.

„Die Nachfrage nach Versicherungslösungen, die auf diesen neuen Risikosituationen und deren Kumule eingehen, steigt kontinuierlich“, sagt er. Für Aon-Manager Behrends beginnt das Handeln dabei mit der Erkenntnis bei Unternehmen, wenn sie nicht mehr glaubten, ihre Netzwerke seien so sicher, dass man sie nie durchbrechen könne. Der Fokus sollte laut Behrends auf „risikomindernde Datenschutzmaßnahmen“ und in der Prävention liegen. Denn „wenn personenbezogene Daten verloren gehen, muss das Unternehmen berechnete Ansprüche Dritter, zum Beispiel wegen Verletzung ihrer Persönlichkeitsrechte, befriedigen“. Laut Behrends belaufen sich die durchschnittlichen organisatorischen Kosten eines Datenverlusts für ein deutsches Unternehmen auf 3,4 Mio. €.

Im Bereich der Cyber-Risiken und deren Deckungsmöglichkeiten bietet die Munich Re eigenen Angaben zufolge die „meiste Kapazität an und ist auch in der Lage, Kumulgefahren wie Schäden durch Würmer und Viren rückzuversichern“, heißt es selbstlobend in der hauseigenen Publikation *„Cyber-Risiken – Herausforderungen, Strategien und Lösungen für Versicherer“*. Andreas Schleyer, Underwriter bei Munich Re im Bereich Special and Financial Risks, erläutert darin die Möglichkeiten, welche Risiken durch eine spezielle Police abgedeckt werden können – und welche nicht. Nicht versicherbar ist der „Ausfall des Internets als Kriegs- und Terrorszenario“, sagt Schleyer. „Denn der Ausfall des Internets lässt sich im Gegensatz zum Computervirus und Würmern nicht modellieren“. Und Schleyer erinnert daran: „Hundertprozentige Sicherheit gibt es nicht und es bleibt immer ein Restrisiko. Gerade bei Risiken mit niedriger Frequenz, aber hoher Intensität“.

2.4 Schäden gehen in die Millionen

So summiert sich denn in deutschen Großunternehmen der finanzielle Schaden durch Cybercrime im Durchschnitt auf 4,8 Mio. €. Nur in den USA waren die Kosten im Tatort Internet mit 6,9 Mio. € noch höher. Auf Rang drei kommt Japan mit 3,9 Mio. €. Dies geht aus der dritten Studie „Cost of Cyber Crime“ des amerikanischen IT-Unternehmens *Hewlett-Packard (HP)* hervor. Im Auftrag von HP befragte das *Ponemon Institute* insgesamt 418 Fach- und Führungskräfte aus 43 deutschen Unternehmen und Behörden (Ponemon, L, 2012, *3rd Annual Cost of Cyber Crime Study*). Deutsche Unternehmen wurden in der dritten Studie dabei zum ersten Mal berücksichtigt. Laut der Studie schaffen es die Täter pro Woche im Durchschnitt 1,1 Mal mit Erfolg ihre virtuellen Angriffe durchzuführen (USA 1,8 Mal pro Woche). Während für Deutschland in der dritten Auflage der Studie noch keine Vergleichswerte vorlagen, da hiesige Unternehmen erstmals in der Untersuchung aufgenommen wurden, lässt sich für die USA eine Verdoppelung der Web-Angriffe feststellen.

Damit stiegen auch die Kosten auf circa 40%, die Datendiebe und Hacker verursacht haben. Besorgniserregend: die kriminelle Energie von „Insidern“ sorgt für die höchsten Schäden, gefolgt von Sabotage, sogenannten Denial-of-Service-Attacken, sowie von Schadprogrammen (Malware). Diese drei Kriminalitätsformen machen in deutschen Unternehmen insgesamt 58% des Schadens aus. Mit 51% ergibt sich ein Übergewicht der untersuchten Unternehmen aus der Finanzwirtschaft, den Behörden sowie der Dienstleistungs- und IT-Branche. In die Studie aufgenommen wurden Unternehmen und Behörden zwischen 1.044 und 95.419 PC-Arbeitsplätzen. Die finanziellen Kosten, die HP ermittelt hat, entstehen in deutschen Unternehmen hauptsächlich durch Datenverluste (40%) und deren Folgen (28%). Weitere Kostenfaktoren entfallen der Studie zufolge auf die Prävention (33%) und die Entfernung des angerichteten Schadens (23%). Während die Beseitigung der von Insidern hervorgerufenen Schäden durchschnittlich 42 Tage in Anspruch nimmt, vergehen bei den restlichen „externen“ Schäden 22 Tage. In dieser Zeitspanne entstehen durchschnittliche Kosten in Höhe von 294.829 Euro, heißt es in der Studie.

Dass die Sicherheitsbehörden tatsächlich auch hierzulande immer stärker mit solchen Schadendimensionen konfrontiert werden, wurde beim Besuch des Bundesinnenministers Thomas de Maiziére Ende März 2014 im BKA klar. Im Gespräch mit BKA-Präsident Jörg Ziercke wurde deutlich, dass neben der Organisierten Kriminalität und dem Terrorismus auch die Cyber-Kriminalität die Sicherheitslage in Deutschland prägt. Die zunehmende Nutzung moderner Kommunikationsmittel wie das Internet entgrenze kriminalgeografische Räume und damit die Reichweite der Bedrohung und der Betroffenen, so das BKA. Sie stellten die Polizei vor im-

mer neue Herausforderungen wie den Umgang mit elektronischen Massendaten und Kryptografie oder die Sicherung von Daten in virtuellen „Clouds“. „Die Methoden der Bekämpfung in der analogen Welt können nicht auf die virtuelle Welt übertragen werden“, sagte Ziercke. Mit der immer weiterreichenden Verbreitung moderner Informationstechniken in alle Bereiche des täglichen Lebens steigt nach Angabe der Polizeibehörde das Risiko ihrer Nutzer, Opfer krimineller Machenschaften zu werden.

Das Spektrum der Bedrohung reicht dem BKA zufolge vom Angriff auf Computersysteme, der Verbreitung von Schadsoftware und Trojanern und der digitalen Erpressung bis hin zu Angriffen auf kritische Infrastrukturen und Cyber-Spionage. Einigkeit beim Treffen bestand mit Minister de Maizière darüber, dass das sogenannte „Deepweb“ – jener Teil des Internets, der nicht über normale Suchmaschinen auffindbar ist und die Anonymität der Nutzer durch Verschleierung der Verbindungsdaten wahrt – nicht zu einem strafverfolgungsfreien Raum werden dürfe. Denn solche Online-Plattformen seien Umschlagplätze für Drogen, Waffen, entwendete Kreditkartendaten und illegale Dienstleistungen, etwa das Ausspähen von Daten oder die Auftragstötung. Dieser Entwicklung könne die Polizei alleine nicht begegnen.

Kriminellen Netzwerken müssten nicht nur gut ausgebildete Ermittler, sondern auch Informationsnetzwerke und Allianzen mit externen Partnern entgegengestellt werden. „Nur wenn wir fachlich, technisch und rechtlich mit den Entwicklungen unserer Zeit Schritt halten können, wird es uns möglich sein, Cybercrime wirkungsvoll zu bekämpfen“, sagte Ziercke. Dabei müsse der Spagat zwischen Freiheit und Sicherheit gelingen. Denn ein Klima der Angst und des Misstrauens gegenüber den Strafverfolgungsbehörden und dem staatlichen Umgang mit Daten würde zu einem Vertrauensverlust führen. Ziercke: „Ohne das Vertrauen unserer Bürgerinnen und Bürger aber kann die Polizei nicht erfolgreich sein“.

2.5 Höchstes Dunkelfeld bei Cybercrime

In Deutschland werden offizielle Zahlen zur Internetkriminalität bundesweit in der sogenannten Polizeilichen Kriminalstatistik (PKS) erfasst. In diesem Datenwerk finden jedoch nur solche Straftaten Eingang, die durch Anzeigen von Betroffenen oder Ermittlungen der Polizei bekannt werden. Das ist das sogenannte „Hellfeld“ der Kriminalität. Das Dunkelfeld dagegen bleibt naturgemäß weitgehend unbekannt. Um dennoch eine Vorstellung vom Ausmaß und die Entwicklung der nicht angezeigten Straftaten zu bekommen, hat das Landeskriminalamt Niedersachsen eine *Befragung zum Dunkelfeld der Kriminalität* durchgeführt. Erste Ergebnisse dieser Untersuchung stellte der niedersächsische Innenminister Boris Pistorius vor.

Für die Dunkelfeldstudie wurden 40.000 Personen ab 16 Jahre, die in Niedersachsen ihren Hauptwohnsitz haben, angeschrieben. Sie wurden gebeten, Fragen zu ihren Erfahrungen mit Kriminalität im Jahr 2012 zu beantworten. Außerdem wurde nach ihrer Furcht, Opfer zu werden, ihrem Verhalten zum Schutz vor Straftaten, ihrer Wahrnehmung der Polizei und einigen personenbezogenen Daten wie Alter und Geschlecht gefragt. Der Fragebogen bestand aus insgesamt 20 Seiten mit 50 Fragen, so Uwe Kolmey, Präsident des niedersächsischen Landeskriminalamtes.

Der Studie zufolge beträgt der Betrug mittels Internet etwa das Vierfache der bekannten Fälle. Das Dunkelfeld bei Phishing betrage das Zehnfache und bei Datenverlusten und finanziellen Einbußen durch Viren und Trojanern sogar mehr als das Zwanzigfache des der Polizei bekannt gewordenen Fallvolumens. Von allen erfragten Deliktsbereichen der Dunkelfeldstudie weist dem Bericht zufolge der Bereich Cybercrime das größte Dunkelfeld auf. Das Internet sei für sehr viele Menschen inzwischen eine Art zweites Zuhause geworden, mit sozialen Kontakten und natürlich einem riesigen Marktplatz, so Innenminister Pistorius. Die Ergebnisse der Dunkelfeldstudie belegten, dass alle sehr genau darauf achten müssten, wie persönliche Daten im Netz zu schützen seien.

„Natürlich heißt das auch, dass die Bekämpfung der Cybercrime weiter intensiviert werden muss“, so der Politiker. Nach Angaben des niedersächsischen Innenministeriums hätten von den 40.000 angeschriebenen Personen 18.940 an der Befragung teilgenommen. Das entspricht einer Rücklaufquote von 47 %. Damit lägen in Niedersachsen für das Jahr 2012 erstmals in der Bundesrepublik Deutschland verlässliche Dunkelfelddaten auf der Basis einer umfassenden, repräsentativen Bevölkerungsbefragung vor. Außerdem betonte Pistorius, dass außer den Menschen vor allem Unternehmen und auch Verwaltungen ihre Inhalte in besonderer Weise vor Spionage oder Sabotage schützen müssten. Mit Blick auf den Wirtschaftsstandort gelte das Sicherheitsinteresse gleichzeitig den bedeutsamen Klein- und Mittelständischen Unternehmen (KMU) und der öffentlichen Verwaltung. Ein Ziel der Kampagne sei auch, insbesondere diese bezüglich der hohen Anforderungen an ihre IT-Sicherheit zu sensibilisieren.

Der *Landesverband Niedersachsen des Bundes Deutscher Kriminalbeamter (BDK)* sieht in der Dunkelfeldstudie einen „mutigen Schritt in die richtige Richtung“. Schon seit Jahren fordert der BDK eine Abkehr von der PKS als alleiniges Instrumentarium zur Erklärung „polizeilicher Erfolge“. Die PKS spiegele kaum die Realität des Kriminalitätsgeschehens wider, sei zum Teil unlogisch und widersprüchlich und erzeuge immer wieder „Begehrlichkeiten für Manipulation und Verzerrung“ der tatsächlichen Kriminalitätsentwicklung. Es wäre, so die Forderung des BDK, politisch sehr mutig, neben der Dunkelfeldforschung auch dazu überzugehen, eine Opferstatistik einzuführen. Damit wäre dann zwar das künftige Kriminalitätslagebild voraussichtlich in einigen Deliktsbereichen

Der Cyber-Versicherungsmarkt in Deutschland

Eine Einführung

Choudhry, U.

2014, IX, 45 S., Softcover

ISBN: 978-3-658-07097-7