world of risk

Aktuelle Informationen aus der Welt von Chance und Risiko

heroldconsult **Nr. 109.01.24**

Zu dieser Ausgabe

man könnte sagen, das neue Jahr startet wie das alte aufgehört hat – katastrophal. In großen Teilen Deutschlands stürmt und regnet es gefühlt seit Wochen, Und nun äußern Experten auch noch Kritik am Hochwasserschutz- wo ist die Lernkurve aus dem Hochwasser im Sommer 2021?

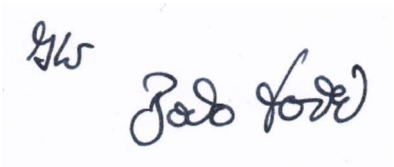
Neben Naturkatastrohen bedeuten aber auch Krieg, politische Unruhen, die Gefahr von Terroranschlägen sowie eine hohe Kriminalitätsrate für Unternehmen und Personen ein hohes Sicherheitsrisiko, genauso wie eine schlechte medizinische Versorgung oder gefährliche Infektionskrankheiten. Die interaktive Weltkarte „Risk Map“ zeigt, wo auf der Welt Sie 2024 besonders vorsichtig sein müssen.

Eine gemeinsame Studie vom Bundesverband Materialwirtschaft, Einkauf und Logistik e.V. und Expense Reduction Analysts bestätigt, dass Risikomanagement in Unternehmen ständige Wachsamkeit und Anpassung bedarf – klingt simpel, aber die Realität sieht häufig anders aus, z. B. mit lediglich jährlicher Überprüfung.

Der BDVM-Präsident Thomas Haukje moniert die Lage aus Sicht der Versicherungsmakler: Versicherer würden weiter Prämien und Verträge anpassen, Risiken ausschließen und Kapazitäten reduzieren. Zudem würden kurzfristige Kündigungen von seiten der Versicherer ein geordnetes Renewal kaum möglich machten. Mögen Prämienanpassungen oft nachvollziehbar sein, kurzfristige Kündigungen sind dies sicher nicht.

In einem von EY initiierten Interview wird über Sinn und Zweck von Cyberversicherungen gesprochen, vor allem darauf hingewiesen, dass eine Cyberversicherung nur ein Teil des Risikomanagements ist – ebenfalls keine Überraschung, wohl aber, dass immer noch weniger als die Hälfte aller Unternehmen eine Cyberversicherung aufweisen.

Hier wie auch in anderen Themen freut mich schon jetzt der Dialog, vielleicht gar die Mithilfe zur Lösung mit Ihnen.



Themen dieser Ausgabe

I. Risiken, hier Gefahren:
- Hochwasserschutz in NRW birgt Risiko – Experten äußern deutliche Kritik
- Die gefährlichsten (und sichersten) Länder 2024

II. Risikomanagement: Risikomanagement bedeutet ständige Wachsamkeit

III. Versicherung
- BDVM sieht keinen Umschwung bei Versichererverhalten
- Warum eine Cyberversicherung nur ein Teil des Risikomanagements ist

I. Risiken

Gefahren

Hochwasserschutz in NRW birgt Risiko – Experten äußern deutliche Kritik

www.tag24.de vom 20.12.24

Langfristig müssten die Ballungsräume zu "Schwammstädten" werden, sagte Frank Obenaus, Vorstand Wassermanagement und Technik bei der Emschergenossenschaft und Lippeverband, am Freitag im WDR.

"Da werden wir aber einen langen Atem brauchen, das sind Projekte, die sicherlich in den nächsten zehn Jahren umgesetzt werden müssen, um dort in Schritten zu mehr Aufnahmefähigkeit der Ballungsräume zu führen."

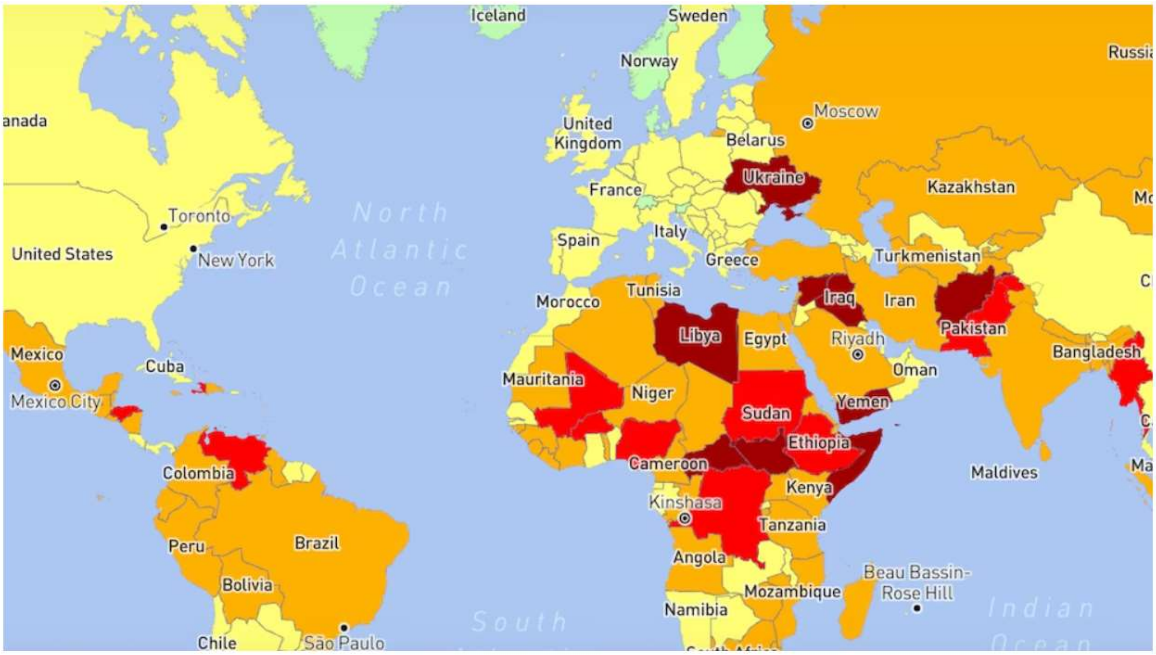
Obenaus sagte, einerseits gebe es die großen technischen Schutzeinrichtungen wie Deiche und Rückhaltebecken für Hochwasserabflüsse. Daneben benötige man "Notpolder", Speicherflächen für das Wasser im Bedarfsfall.

Zudem müsse aber auch die Wasseraufnahme-Kapazität in den Siedlungsgebieten verstärkt werden, und gerade hier müsse in den nächsten Jahren noch viel geschehen. Jede mögliche Fläche zur Versickerung, zum Rückhalt von Regenwasser müsse genutzt werden. "Das passiert, wenn Sie von außen auf die Siedlungsflächen gucken, noch zu wenig", so Obenaus.

Versiegelung müsse hier zurückgenommen werden, neue Speichermöglichkeiten wie begrünte Dächer müssten geschaffen werden. "Das ist durchaus mühsame Kleinarbeit."

Der Aachener Hochschullehrer Holger Schüttrumpf sagte dem WDR, viele Deiche in NRW entsprächen nicht mehr dem Stand der Technik. Es gebe derzeit ja noch keine extrem hohen Wasserstände, und von daher dürften die Deiche eigentlich noch nicht versagen, so der Experte für Wasserwirtschaft. "Es verwundert mich natürlich schon, dass so viele Deiche eigentlich momentan aufweichen." Die Lage zeige, dass die Deiche auf den neuesten Stand gebracht werden müssten. Das sei aber nicht alles: "Wir müssen natürlich Gebäude und Siedlungen schützen. Aber andere Bereiche, die sollten wir dem Fluss zurückgeben." Denn so entstünden Rückhalteräume, die die Wasserstände reduzieren könnten.

Die gefährlichsten (und sichersten) Länder 2024



Die „Risk Map“ zeigt, wo es auf der Welt am gefährlichsten ist und wo Reisende sich sicher wähnen dürfen Foto:

Krieg, politische Unruhen, die Gefahr von Terroranschlägen und Naturkatastrophen sowie eine hohe Kriminalitätsrate bedeuten für Reisende ein hohes Sicherheitsrisiko. Aber auch eine schlechte medizinische Versorgung oder gefährliche Infektionskrankheiten können fatale Folgen haben. Die interaktive Weltkarte „Risk Map“ zeigt, wo auf der Welt Sie 2024 besonders vorsichtig sein müssen.

Wer verreist, möchte in der Regel vorab über die Sicherheitslage im Urlaubsland informiert sein. Welche Länder am gefährlichsten sind und wo die Risiken für Reisende auf der ganzen Welt besonders groß sind, zeigt die „Risk Map“, die von dem Unternehmen „International SOS“ herausgegeben wird.

Die Daten der interaktiven „Risk Map“ setzen sich aus Analysen von 2023 sowie Prognosen für das kommende Jahr zusammen. Nutzer können demnach die Lage auf der Welt hinsichtlich vier verschiedener Kriterien in Erfahrung bringen: Sicherheit, medizinisches Risiko, mentale Gesundheit und Klimawandel. Die jeweiligen Ergebnisse werden in fünf Risikostufen unterteilt: unerheblich (grün), gering (gelb), mittel (orange), hoch (hellrot) und extrem (dunkelrot). Die Einschätzungen richten sich in erster Linie an Geschäftsreisende und Unternehmen, aber auch für Urlauber und Reisende bietet die Weltkarte eine Orientierungshilfe.

Geht es um die Einstufung des Sicherheitsrisikos, spielen Internation SOS zufolge Faktoren wie Terrorgefahr, Krieg, Unruhen, Überfälle, Entführungen und Betrugsvergehen eine Rolle. Aber auch das Risiko von Naturkatastrophen und etwa die Bewertung der Verkehrsinfrastruktur können mit einfließen – insofern deren Risiko-Ausmaß so hoch ist, als dass von etwaigen Folgen ausgegangen werden muss.

„Unerheblich“ ist das Risiko laut der Reisesicherheits-Weltkarte v.a. in Norwegen, Finnland, Dänemark, Island, Luxemburg, der Schweiz, Liechtenstein, Andorra und Slowenien sowie in

Grönland, den karibischen Turks- und Caicosinseln und auf einigen kleinen Inselgruppen in Ozeanien wie den Cook-Inseln, Marshallinseln und Tuvalu.

Die Cookinseln im Südpazifik gelten als besonders sicher Foto: Getty Images
Ein geringes Sicherheitsrisiko gilt auch für den Großteil Europas – mit wenigen Ausnahmen, wie der Türkei mit mittlerem Risiko und der Ukraine mit dem kriegsbedingten, extremen Risiko. Unverständlich ist, dass laut der „Risk Map“ im Kosovo, in Serbien, in der Grenzregion zum Kosovo, sowie in Moldawien nur ein geringes Sicherheitsrisiko gelte. So rät etwa das Auswärtige Amt von Reisen in den Norden Kosovos aufgrund der politischen Zuspitzungen zwischen Kosovo und Serbien weiter ab. Auch bleibt die Sicherheitslage für Moldawien aufgrund des russischen Angriffskrieges gegen die Ukraine laut Auswärtigem Amt in einigen Regionen volatil.

In Nordamerika, Teilen Südamerikas und Mittelamerikas ist das Sicherheitsrisiko laut den Experten gering. Konkret zählen zu diesen Staaten Argentinien, Chile, Paraguay, Uruguay, Suriname, Französisch Guyana, Panama, Costa Rica, Kuba, die USA und Kanada. Ebenfalls sicher sind laut den Experten Australien und Neuseeland sowie China, Japan, Thailand, Vietnam, Malaysia, Brunei, Südkorea, Laos, der Oman und Usbekistan. In Afrika gelten unter anderem Marokko, Namibia, Botswana, Sambia, der Senegal, Malawi und Ghana als Länder mit einem niedrigen Sicherheitsrisiko.

Neben der bereits erwähnten Ukraine wird das Risiko noch in vielen anderen Staaten Asiens, Afrikas und Südamerika als hoch bewertet, in einigen Ländern sogar als extrem. Zu den gefährlichsten Ländern weltweit zählen laut den Experten weiterhin unter anderem Syrien, Afghanistan, Libyen, Jemen und die Zentralafrikanische Republik:
Extrem hohes Sicherheitsrisiko:

- Afghanistan
- Gazastreifen
- Grenzgebiet zwischen Libanon und Syrien
- Teile des Irak
- Libyen
- Jemen
- Teile von Nigeria
- Teile von Pakistan
- Somalia
- Südsudan
- Syrien
- Ukraine
- Zentralafrikanische Republik

Hohes Sicherheitsrisiko:

- El Salvador
- Teile Guatemalas
- Honduras
- Grenzregion zwischen Ecuador und Kolumbien
- Venezuela
- Mali
- Haiti
- Algerien
- Grenzgebiete von Tunesien
- Burkina Faso
- Grenzgebiete der Elfenbeinküste

- Nigeria
- Grenzgebiet des Kamerun
- Teile der Demokratischen Republik Kongo
- Teile Äthiopiens
- Grenzgebiet zwischen Eritrea und Äthiopien
- Grenzgebiet zwischen Eritrea und Sudan
- Teile des Sudans
- Teile des Iraks
- Grenzgebiet zwischen Georgien und Russland
- Teile Pakistans
- Grenzgebiet zwischen Iran und Pakistan
- Myanmar

Die Liste lässt jedoch so einige Länder vermissen. So spricht das Auswärtige Amt aufgrund der innenpolitischen Lage eine Teilreisewarnung für Mosambik aus. Auch für Algerien gilt dem Auswärtigen Amt zufolge weiterhin eine hohe Gefahr durch terroristische Anschläge und Entführungen – es besteht eine Teilreisewarnung.

In Israel, im Gazastreifen und im Libanon wird das Sicherheitsrisiko laut „International SOS“ lediglich als „mittel“ eingestuft. Das ist angesichts des Krieges keinesfalls nachvollziehbar. Auch das Auswärtige Amt warnt vor Reisen nach Israel und in palästinensische Gebiete.

Mit der interaktiven „Risk Map“ können die sichersten und gefährlichsten Länder der Welt außerdem auch hinsichtlich des medizinischen Risikos in Erfahrung gebracht werden. Dieses ist in den folgenden Ländern besonders hoch:

- Afghanistan
- Burkina Faso
- Burundi
- Eritrea
- Gazastreifen
- Guinea
- Haiti
- Irak
- Jemen
- Liberia
- Libyen
- Niger
- Nordkorea
- Somalia
- Sierra Leone
- Sudan
- Südsudan
- Syrien
- Westjordanland
- Zentralafrikanischen Republik

In diesen Ländern ist laut „International SOS“ die Gesundheitsversorgung nicht vorhanden respektive gewährleistet. Auch übertragene Infektionen sind möglich und es kann – etwa wie bei Malaria und Cholera – in einigen Ländern sogar zu größeren Ausbrüchen kommen.

Klimawandel und mentale Gesundheit

Die „Risk Map“ liefert zudem hinsichtlich der Kategorien „Klimawandel“ und „mentale Gesundheit“ eine länderspezifische Risiko-Einstufung. So zeigt die Karte für die Bewertung

der mentalen Gesundheit den Anteil der Bevölkerung, die an einer psychischen Erkrankung leidet. Dazu zählen laut „International SOS“ Depressionen, Angstzustände, Essstörungen, bipolare Störungen und Schizophrenie. Grundlage dafür wären Daten der World Health Organization (WHO).

Vor allem in Grönland, Irland, Australien, Neuseeland, Spanien, Französisch Guyana, sowie im Iran, Westjordanland und im Gazastreifen leiden Menschen der „Risk Map“ zufolge unter mentalen Problemen. Hier sind demnach 17,5 bis 20 Prozent der Bevölkerung betroffen.
In Deutschland gebe es auch ein hohes Risiko: Hierzulande wären etwa 15 bis 17,5 Prozent der Bevölkerung von psychischen Krankheiten betroffen.

II. Risikomanagement

Risikomanagement bedeutet ständige Wachsamkeit

Q: www.risknet.de vom 23.09.2023

Einer gemeinsamen Studie vom Bundesverband Materialwirtschaft, Einkauf und Logistik e.V. (BME) und Expense Reduction Analysts zufolge bedeutet Risikomanagement in Unternehmen ständige Wachsamkeit und Anpassung. Obwohl Verwerfungen im Geschäft nicht immer verhindert werden können, ermöglicht es dem Einkauf, schnell und gezielt zu reagieren.

Die wirtschaftlichen und sozialen Rahmenbedingungen für Unternehmen verändern sich aktuell rapide. Viele können mit diesem Wandel nicht ohne Weiteres Schritt halten. Dies ist eine der Kernaussagen der Studie "Krisenmanagement und Führungskultur – Wie Unternehmen mit der Krise umgehen", die Expense Reduction Analysts zusammen mit dem Bundesverband Materialwirtschaft, Einkauf und Logistik e.V. (BME) durchgeführt hat. 189 Unternehmen haben beantwortet, wie die aktuellen Krisen sie verändert haben und welche Maßnahmen daraus abgeleitet werden.

"Die Studie zeigt, dass nach einer überstandenen Krise mehrheitlich nach den angestammten Mustern weitergearbeitet wird", sagte Matthias Droste, Country Manager DACH der Unternehmensberatung Expense Reduction Analysts (DACH) GmbH. Bei der Führungskultur seien angestammte Muster vorherrschend. Die Nutzung erfolgskritischer Management-Tools, partizipatives Führen oder die Evaluierung neuer Produkte oder alternativer Geschäftsmodelle erfolge mehrheitlich noch nicht.

Für das Top-Management sei die aktuelle Situation eine Herausforderung. Droste: "Die Anforderungen in Bezug auf Kommunikations- und Entscheidungsstärke wie auch Flexibilität sind deutlich gestiegen." Zudem: 72 Prozent der Führungskräfte der zweiten Management-Ebene berichteten von einer Überforderung bei der Entscheidungsfindung unter Zeitdruck.

"Nur jedes zweite befragte Unternehmen hat aus den Krisen wirklich schon Lehren gezogen und daraus Maßnahmen abgeleitet", sagte Droste. So hätten 50 Prozent der Firmen noch immer kein belastbares Krisenmanagementsystem aufgebaut und nur ein Drittel halte die 'Lessons Learned' aus Krisen in Leitlinien und Handbüchern fest. Zudem sei das Krisenmanagement bei über der Hälfte der Unternehmen noch nicht in der Unternehmensstrategie verankert.

"Die deutschen Einkaufsmanager:innen haben gerade in den vergangenen Krisenjahren bewiesen, dass sie auf herausfordernde Situationen reagieren können – sei es durch Naturkatastrophen, die Corona-Pandemie oder geopolitische Veränderungen. Doch trotz dieser Anpassungsfähigkeit zeigt die aktuelle Studie, dass wir noch nicht am Ziel sind", betonte BME-Hauptgeschäftsführerin Helena Melnikov. Risikomanagement in Unternehmen bedeute ständige Wachsamkeit und Anpassung. Es erkenne frühzeitig Veränderungen in wirtschaftlichen, sozialen oder geopolitischen

Rahmenbedingungen. Obwohl Verwerfungen im Geschäft nicht immer verhindert werden könnten, ermögliche gutes Risikomanagement dem Einkauf, schnell und gezielt zu reagieren.

Droste: "Auch bei den operativen Maßnahmen zeigt sich: Unternehmen fokussieren sich noch zu sehr auf das Dringende und nicht auf das Wichtige." Die Sourcing-Strategien würden nur langsam angepasst, Employer Branding als vorherrschende Strategie gegen Hilfs- und Fachkräftemangel eingesetzt und auch beim Thema Digitalisierung gebe es noch viel zu tun.

III. Versicherung

BDVM sieht keinen Umschwung bei Versichererverhalten

Q: www.asscompact.de vom 04.10.2023

Der harte Markt in der Gewerbe- und Industrieversicherung wird bleiben, so der BDVM. Das verlangt Versicherungsmaklern und ihren Mitarbeitern einiges ab. In einem Pressegespräch weiß BDVM-Präsident Thomas Haukje zudem von einer Flut an ausgeschriebenen Flottenversicherungen zu berichten.

Robust – dieses Wort fällt immer öfter, wenn es um das Verhalten der Marktbeteiligten in der Gewerbe- und Industrieversicherung geht. Es bedeutet, dass bei Vertragsverhandlungen die Durchsetzung von Eigeninteressen weit vor dem Finden von Konsenslösungen steht. Und man darf davon ausgehen, dass man den Begriff weiter hören wird, denn eine Entspannung des Marktes ist zumindest in weiten Teilen nicht absehbar.

Am Donnerstag beschrieb Thomas Haukje, seines Zeichens BDVM-Präsident, die Lage aus Sicht der Versicherungsmakler. Versicherer würden weiter Prämien und Verträge anpassen, Risiken ausschließen und Kapazitäten reduzieren. Besonders ärgerlich: kurzfristige Kündigungen vonseiten der Versicherer, die ein geordnetes Renewal kaum möglich machten. Die Gründe seien für die Versicherungsmakler oft nicht nachvollziehbar. Die gängigen Aussagen zu den allgemeinen Rahmenbedingungen wie etwa Inflation und hohe Rückversicherungspreise könnten nicht für alle Anpassungen herhalten. Angesichts der guten Bilanzen der Versicherer fehle auch aufseiten der Versicherungskunden das Verständnis. Haukje sagt, Spartenrentabilität gehe den Versicherern vor Kundenrentabilität. Und: Am Markt gebe es derzeit keinen Wettbewerb um Marktanteile. Gute Bilanzzahlen seien vorerst wichtiger als der Gewinn von Marktanteilen.

Der BDVM als Interessenvertreter der Versicherungsmakler werde sich deshalb weiterhin für eine Verbesserung der Lage einsetzen, sodass Maklerunternehmen auch künftig einen optimalen Versicherungsschutz für ihre Kunden realisieren könnten.

Die größten Sorgen macht den Maklerunternehmen aktuell die Sachversicherung. Kapazitäten werden hier in bestimmten Branchen stark verknappt. Die Anforderungen an technischen Brandschutz etwa steigen stetig und Umsetzungsmaßnahmen werden oft zeitlich bindend vereinbart. Im Bereich von D&O- und Cyberversicherung gibt es dagegen Lichtblicke.

In der Kfz-Versicherung wiederum tobe der „wilde Sanierungsteufel durch die Lande“, erklärt Haukje. Aufgrund der hohen Reparatur- und Ersatzteilkosten in den Werkstätten erwarten im Grunde alle Marktbeteiligten deutliche Prämiensteigerungen. Die Folge: Ein Großteil der Flotten wird dieses Jahr aufgrund der Sanierungsforderungen vonseiten der Versicherer ausgeschrieben. Der BDVM berichtet, dass die Kfz-Flottenversicherer zwei- bis fünfmal so viele Ausschreibungen wie in den Vorjahren auf dem Tisch hätten. Nur höre man leider nichts von den Versicherern, so Haukje. Die Flut sei bei den Versicherern kaum zu bewältigen, hier würden sich die Folgen des Ressourcen- und Fachkräftemangels zum Jahresende schmerzhaft für alle Beteiligten zeigen.

Die aktuelle Marktsituation sei nichts für schwache Nerven, sagt der BDVM-Präsident, der im November erneut für den BDVM-Vorstand, aber nicht mehr für das Präsidentenamt kandidieren wird. Der Aufwand im Maklerunternehmen für das Halten des eigenen Servicelevels nehme weiter zu. Auch für die Mitarbeiter und Mitarbeiterinnen erhöhten sich dadurch die Anforderungen. Es brauche resiliente und engagierte Leute, die den Herausforderungen standhielten. Die BDVM-Mitglieder würden zwar konstant 12.000 Mitarbeiter auf sich vereinigen, aber auch hier werde es schwerer, Fachkräfte zu gewinnen und auch zu halten.

Haukje vermutet, dass der „harte Markt" in der Gewerbe- und Industrieversicherung anhalten werde. Seiner Ansicht nach wird der „harte Markt" schlicht der „neue Markt" sein. Der Umgang miteinander wird wohl robust bleiben. (bh)

Warum eine Cyberversicherung nur ein Teil des Risikomanagements ist

www.ey.com/de aus November 2023

Immer mehr Unternehmen schließen sie ab – doch noch mehr sollten sie haben: ein Interview über Sinn und Zweck von Cyberversicherungen.

Seit nunmehr etwa elf Jahren gibt es spezielle Versicherungsprodukte auf dem deutschen Markt, mit denen sich Unternehmen im Fall eines Cyberangriffs vor allem vor den akuten finanziellen Folgen schützen können. Laut der Datenklaustudie 2023 von EY stieg der Anteil der Unternehmen mit einer Cyberversicherung im Vergleich zur Vorstudie von 2011 von 36 auf 46 Prozent; jedes dritte Unternehmen, das noch keine solche Versicherung abgeschlossen hat, plant dies noch zu tun. Cyber Incidents nehmen nicht nur zahlenmäßig, sondern auch an Raffinesse zu – und damit die Bedrohung. Bodo Meseke und Thomas Koch, beide Partner der Forensic & Integrity Services bei EY, sowie Jens Krickhahn, Practice Leader Cyber & Fidelity bei Allianz Commercial, beleuchten im Interview Zweck und Bedingungen einer Cyberversicherung: eines komplexen Produkts, das immer nur ein Baustein des Risikomanagements und der Vorbereitung auf Cyberangriffe sein kann und darf. EY ist seit mehreren Jahren einer der designierten Dienstleistungspartner der Allianz Commercial im Bereich Cyberversicherungen. So können Kunden des Versicherers bei Bedarf die Cyber-Response-Dienstleistungen von EY zu vordefinierten Konditionen abrufen.

Herr Krickhahn, Herr Meseke, Herr Koch: Wem würden Sie eine Cyberversicherung empfehlen?
Jens Krickhahn: Das ist immer eine Kosten-Nutzen-Abwägung für ein Unternehmen. Hält es aufgrund des Geschäftsmodells viele personenbezogene Daten vor oder verwendet es in der Produktion viel Operational IT, sollte man im Risikomanagement über eine Cyberversicherung nachdenken.
Bodo Meseke: Sinnvoll ist eine Cyberversicherung mittlerweile eigentlich für jeden, sie ist allerdings nicht für jeden finanziell darstellbar. Und nicht jedes Unternehmen hat den notwendigen Reifegrad, um überhaupt eine Police zu bekommen. Gerade die kleineren haben ihn oft nicht. Wer sich eine Cyberversicherung nicht leisten kann oder will, muss technisch vorbeugen und auch Rücklagen bilden, um den potenziellen Schaden selbst finanziell abmildern zu können. Denn irgendwann kann es jeden, auch kleine Unternehmen, treffen. Mit diesem Risiko müssen heute leider alle leben.

Was bedeutet in diesem Zusammenhang „Reifegrad"?
Krickhahn: Um einen Versicherungsschutz anbieten und gewährleisten zu können, haben wir insgesamt zwölf Kernkriterien benannt, die mögliche Versicherte erfüllen müssen. Das bedeutet: Wir prüfen prozessuale und technische Bereiche, ob beispielsweise Awareness-Trainings gemacht werden, ob Mitarbeiter für den Umgang mit Daten sensibilisiert sind und so weiter.
Auf der technischen Seite spielen unter anderem Patch-Management und eine vernünftige Backup Policy eine große Rolle. Wichtig sind für den Fall eines Cyberangriffs Krisenpläne, die regelmäßig mit dem kompletten Krisenstab geübt werden. Die Cyberversicherung kann immer nur ein Teil des

Risikomanagements sein. Sich in Friedenszeiten auf den Ernstfall vorbereiten – das ist es, was Unternehmen tun müssen. Je besser und gründlicher sie das hinbekommen, desto höher der Reifegrad.
Thomas Koch: Die Versicherung ist ja nicht die Gegenreaktion auf eine Cyberattacke, sondern sie bezahlt die Gegenmaßnahmen. Es ist per se allerdings nicht zielführend, über die Versicherung zwar die finanziellen Mittel verfügbar zu haben, jedoch kein Konzept, wie ich als Unternehmen im Ernstfall auf einen Cyberangriff reagieren soll.
Ähnlich verhält es sich mit präventiven Investitionen in Cybersicherheit: Sie bringen an der falschen Stelle schlicht gar nichts. Die meisten Schwachstellen finden sich nicht einmal im technischen Bereich, sondern sind ganz praktischer Natur: Es sind in der Regel menschliche Fehler und mangelndes Risikobewusstsein, die erfolgreiche Cyberattacken ermöglichen.

Welche Schäden beziehungsweise Gegenmaßnahmen deckt eine Cyberversicherung ab?
Krickhahn: Eine Cyberversicherung ist eine Kombination aus unterschiedlichen traditionellen Sparten, dazu gehören zum Beispiel Haftpflichtkomponenten im Falle einer Datenschutzverletzung. Einer der relevantesten Treiber ist allerdings der Betriebsunterbrechungsschaden inklusive der damit zusammenhängenden Kosten: für IT-Forensiker, für Rechtsanwälte, für PR-Fachleute oder auch für Beratungsdienstleistungen, für die Wiederherstellung der Systeme und so weiter. All das umfasst die Cyberpolice bis zu den Grenzen, die im Vertrag unter anderem als Versicherungslimits geregelt sind.
Koch: Ergänzend dazu: Die technische Aufarbeitung von Cyberangriffen ist erfahrungsgemäß nicht der primäre Kostentreiber. In vielen Fällen ist diese nach wenigen Tagen bis Wochen abgeschlossen. Doch auch wenn Unternehmen die gestohlenen Daten – gegebenenfalls nach Zahlung eines Lösegeldes – entschlüsselt und damit wieder in ihrem Besitz haben, muss die Infrastruktur neu aufgebaut werden. Die operative Nutzung einer einmal kompromittierten Umgebung ist zwangsläufig nur ratsam, wenn betroffene Segmente oder die gesamte Infrastruktur gründlich untersucht und nachweislich nicht mehr infiltriert sind. Das sind schließlich die signifikanten Kostenblöcke.

Das Stichwort „Lösegeld“, das in vielen Fällen von Cyberangriffen gegen die Entschlüsselung von Daten erpresst wird, scheint in dieser Rechnung nicht aufzutauchen …
Krickhahn: Prinzipiell müssen sich Versicherer an die gesetzlichen Vorgaben halten. Es gibt Länder, die die Versicherung von Lösegeld verbieten, und solche, die sie erlauben. In Deutschland gibt es weder ein Verbot noch eine offizielle Erlaubnis.
Meseke: Ich würde erwarten, dass Versicherer sich künftig beim Thema Lösegeld eher zurücknehmen, weil das ein Risiko ist, das sich versicherungsmathematisch nicht mehr so einfach bestimmen lässt. Die Lösegeldforderungen – und hierdurch getrieben dann die Schadensummen – sind in den letzten Jahren immer weiter gestiegen.

Welche sind die momentan größten Cyberbedrohungen?
Meseke: Der Platzhirsch ist weiterhin Ransomware, diese wird uns auch noch lange Zeit begleiten. Hier werden nicht nur die Methoden, sondern auch die Erpressungsmodelle perfider. Betroffene Unternehmen sollen nicht mehr nur ihre Daten zurückkaufen, sondern zusätzlich dafür zahlen, dass diese nicht veröffentlicht werden, und womöglich ein drittes Mal, um zu verhindern, dass ihre Kunden auch noch direkt erpresst werden.
Krickhahn: Ich kann Bodo Meseke nur zustimmen, da schon lange Ransomware as a Service im Darknet als Dienstleistung zu kaufen ist. Da werden dem Erpresser Tools zur Verfügung gestellt, und sollte er die nicht beherrschen, gibt es sogar eine Hotline zur Hilfestellung. Das ist ein Geschäftsmodell. Man findet heute aber im Netz auch schon Bewertungen, welche Hackergruppen zuverlässig den Schlüssel nach Lösegeldzahlungen liefern und welche nicht.
Meseke: Die zweite wesentliche Bedrohung – gerade im Kontext von Cyberversicherungen – ist der Business E-Mail Compromise (BEC), insbesondere der CEO Fraud. Ziel des BEC ist es, Zahlungen auszulösen oder umzuleiten, sodass die Angreifer finanziell profitieren. Dem geht gute Vorbereitung voraus: Die Hacker spionieren aus, wer im Unternehmen wofür verantwortlich ist, und basteln plausible Stories zusammen, damit eine Zahlung freigegeben wird.

Wird die Cyberversicherung für Unternehmen einmal so selbstverständlich wie die private Haftpflichtversicherung für Bürger?
Krickhahn: Bei vielen Unternehmen hat sie bereits einen hohen Stellenwert im Versicherungsportfolio, andere wollen den Preis nicht zahlen oder haben noch nicht den nötigen Reifegrad erzielt. Wiederum andere glauben: „Mir passiert schon nichts." Die Cyberversicherung ist noch nicht dort angekommen, wo sie sein sollte und könnte. Aber wir sind auf einem guten Weg.

Seit 2019 haben die Cyber Incidents und damit auch die Anfragen nach Cyberversicherungen zugenommen. Wie ist das profitabel zu managen?
Krickhahn: Teilweise kamen in dieser dynamischen Zeit tatsächlich mehr Schäden als Neuabschlüsse rein. Wir hatten daher keine Zeit, ein Portfolio aufzubauen, und konnten entsprechend aus keinem schöpfen. Reagieren mussten wir dennoch. Das war dann auch der Start für eine viel tiefere Risikoanalyse als zuvor, um eine bessere Qualifizierung vornehmen zu können. In Branchen mit schweren Risiken, den kritischen Infrastrukturen (KRITIS) zum Beispiel, fordern wir noch mehr Informationen, bevor wir dann sagen: damit können wir jetzt leben. Tatsächlich hat die Identifizierung der Schwachstellen seit 2019 dazu geführt, dass die Informationstiefe, aber auch die Risikoqualität bei heutigen Anfragen insgesamt besser ist. .
Meseke: Nicht nur die Technik, die Cybersecurity und die Cyberversicherungen entwickeln sich weiter, die Cyberkriminalität tut es leider auch. Wir sehen immer neue Bedrohungslagen, immer raffiniertere Angreifer und können darum immer nur wiederholen: Technische Sicherheit zu hinterfragen ist wichtig, aber mindestens ebenso wichtig ist es, auch die Prozesse zu üben, zu üben, zu üben. Wenn ein Krisenmanagementteam im Ernstfall zum allerersten Mal zusammenarbeitet, ist es eigentlich schon zum Scheitern verurteilt.
Wenn ein Krisenmanagementteam im Ernstfall zum allerersten Mal zusammenarbeitet, ist es eigentlich schon zum Scheitern verurteilt.

Welche sind die momentan größten Cyberbedrohungen?
Meseke: Der Platzhirsch ist weiterhin Ransomware, diese wird uns auch noch lange Zeit begleiten. Hier werden nicht nur die Methoden, sondern auch die Erpressungsmodelle perfider. Betroffene Unternehmen sollen nicht mehr nur ihre Daten zurückkaufen, sondern zusätzlich dafür zahlen, dass diese nicht veröffentlicht werden, und womöglich ein drittes Mal, um zu verhindern, dass ihre Kunden auch noch direkt erpresst werden.
Krickhahn: Ich kann Bodo Meseke nur zustimmen, da schon lange Ransomware as a Service im Darknet als Dienstleistung zu kaufen ist. Da werden dem Erpresser Tools zur Verfügung gestellt, und sollte er die nicht beherrschen, gibt es sogar eine Hotline zur Hilfestellung. Das ist ein Geschäftsmodell. Man findet heute aber im Netz auch schon Bewertungen, welche Hackergruppen zuverlässig den Schlüssel nach Lösegeldzahlungen liefern und welche nicht.
Meseke: Die zweite wesentliche Bedrohung – gerade im Kontext von Cyberversicherungen – ist der Business E-Mail Compromise (BEC), insbesondere der CEO Fraud. Ziel des BEC ist es, Zahlungen auszulösen oder umzuleiten, sodass die Angreifer finanziell profitieren. Dem geht gute Vorbereitung voraus: Die Hacker spionieren aus, wer im Unternehmen wofür verantwortlich ist, und basteln plausible Stories zusammen, damit eine Zahlung freigegeben wird.

Wird die Cyberversicherung für Unternehmen einmal so selbstverständlich wie die private Haftpflichtversicherung für Bürger?
Krickhahn: Bei vielen Unternehmen hat sie bereits einen hohen Stellenwert im Versicherungsportfolio, andere wollen den Preis nicht zahlen oder haben noch nicht den nötigen Reifegrad erzielt. Wiederum andere glauben: „Mir passiert schon nichts." Die Cyberversicherung ist noch nicht dort angekommen, wo sie sein sollte und könnte. Aber wir sind auf einem guten Weg.

Kontakt: heroldconsult
c/o Prof. Dr. Bodo Herold
herold@heroldconsult.com
www.heroldconsult.com
Pfarrstr. 5, D 51399 Burscheid