RISK REPORT
Ausgabe XII
Ihr Magazin für Chance und Wagnis von Risk Experts

Risiko Geschäfts-führung

Wie Paragraphen, ausufernde Dokumentationspflichten und Klagsdrohungen den Job an der Spitze zum Wagnis werden lassen.

WKO-Chef Mahrer im Gespräch:

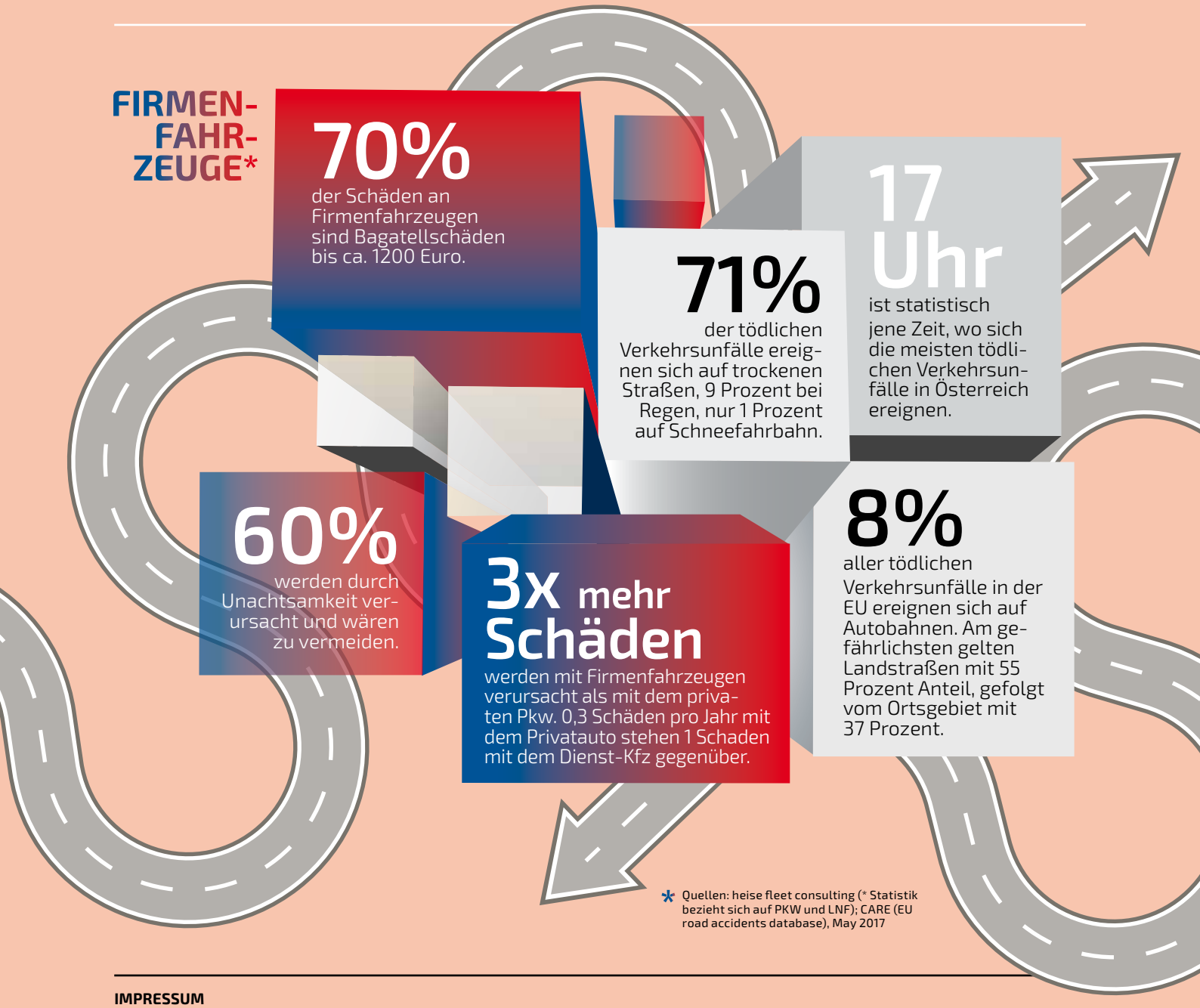
„Ohne Risiko kein Unternehmertum“

Roboter statt Berater?

Der Mensch sei nicht zu ersetzen, sagen Experten.

GEFÄHRLICHE STRASSE

UNFÄLLE UND SCHÄDEN



* Quellen: heise fleet consulting (* Statistik bezieht sich auf PKW und LNF); CARE (EU road accidents database), May 2017

IMPRESSUM

Herausgeber, Medieninhaber und Verleger: Risk Experts Risiko Engineering GmbH, Schottenring 35/2, 1010 Wien **Für den Inhalt verantwortlich:** DI Gerhart Ebner, Geschäftsführender Gesellschafter **Konzeption, redaktionelle Mitarbeit:** Heidi Brukner, Mag. Daniel Brandtmayer von Risk Experts **Projektleitung und Redaktion:** WEKA Industrie Medien GmbH, Mag. Margret Handler, Dresdner Straße 45, 1200 Wien **Art Direction:** Nicole Fleck **Grafik&Layout:** Sarah Güttinger **Druck:** „agensketterl" Druckerei GmbH, Druckhausstr. 1, 2540 Bad Vöslau

Erstellt unter Mitarbeit und aufgrund von Inputs des gesamten Risk Experts-Teams; Die Beiträge wurden sorgfältig ausgearbeitet, dennoch können wir keine Haftung für Richtigkeit der Angaben übernehmen. Alle verwendeten geschlechtsspezifischen Formulierungen meinen die weibliche und männliche Form.

Kontakt für Feedback: media@riskexperts.at

Coverfoto: Fotolia

LIEBE LESERIN, LIEBER LESER

Ja, Manager geraten immer mehr unter Druck. Geschäftsführung ist mittlerweile ein Drahtseilakt, der mit einer zunehmenden Anzahl an Risiken behaftet ist. Damit betiteln wir nicht nur die Covergeschichte der XII Ausgabe des Risk Reports, sondern haben dazu einige interessante Führungspersönlichkeiten befragt, Fakten zusammengetragen und analysiert, die in Summe belegen: Leichter geworden ist es an der Spitze in den vergangenen Jahren nicht.

Wer könnte zum Thema „Risiken beim Wirtschaften" ein besserer Gesprächspartner sein als Wirtschaftskammerpräsident Harald Mahrer? In der Reihe „Ebner diskutiert" hat er sich als spannender Gesprächspartner präsentiert und aus dem Nähkästchen geplaudert.

Außerdem haben wir uns ein derzeit sehr brisantes Thema der Branche angesehen: Cyberattacken auf Unternehmen. Die Fakten dazu sprechen für sich. Nämlich, dass es immer mehr Betroffene gibt. Was die aktuellen Daten der Polizeistatistik sagen und womit wir in Zukunft noch rechnen müssen, haben wir in einer Geschichte zum Thema recherchiert.

Wir wünschen Ihnen ein spannendes Lesevergnügen mit diesen und anderen Artikeln im aktuellen Heft.

Ein starkes Team für Sie

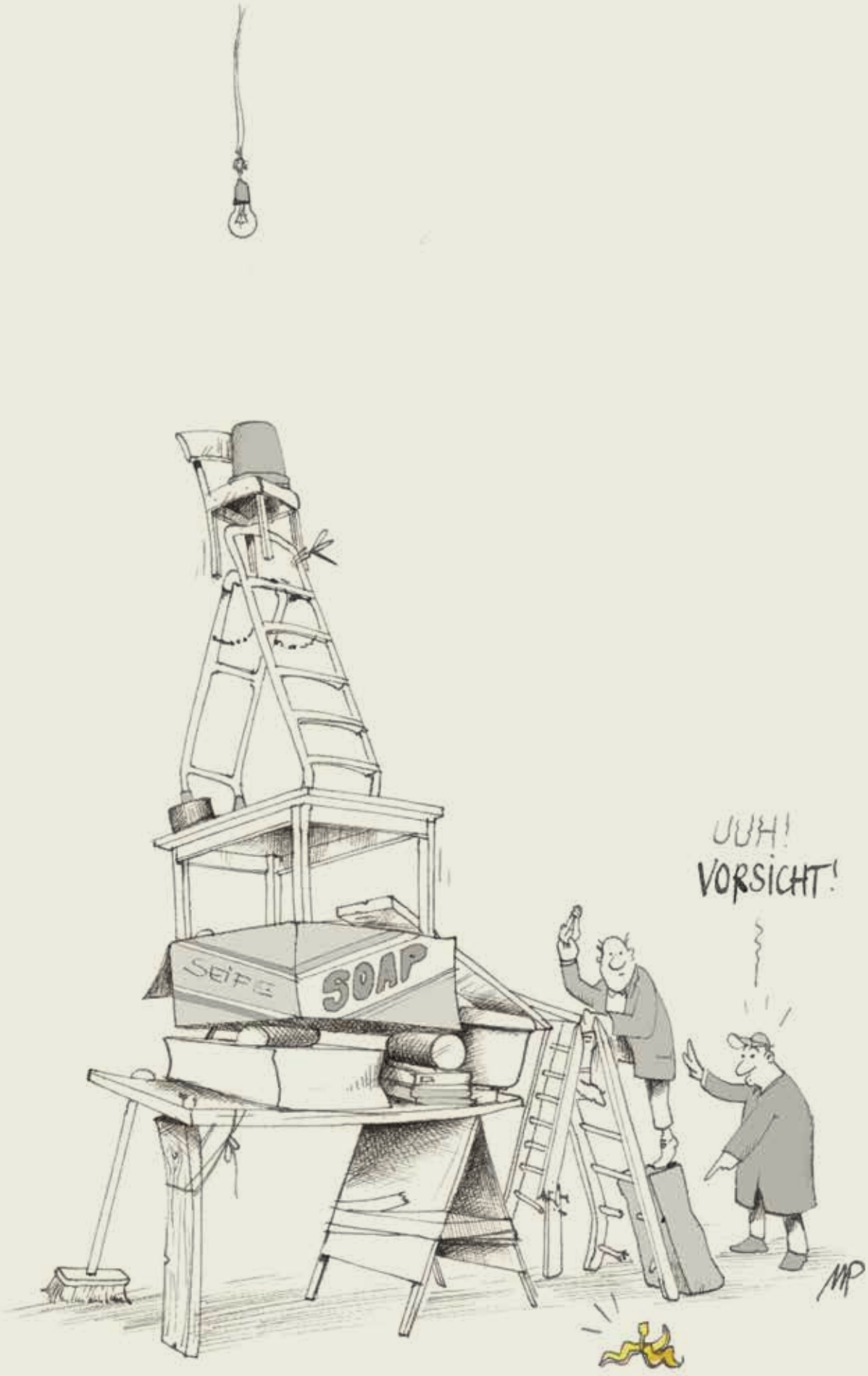
Mit der Kombination aus breitem und interdisziplinärem Know-how sowie der langjährigen Erfahrung unserer Mitarbeiterinnen und Mitarbeiter an unseren Standorten in Wien, Kufstein, Warschau, Bratislava, Bukarest, Sofia und Istanbul können wir Sie bestmöglich unterstützen. Gut ausgebildete Fachleute vor Ort, ein Know-how-Pool in Österreich und unsere webbasierte Experten-Software bieten Unternehmen und Organisationen ein schnelles, kompetentes Netzwerk für Ihre Risikomanagement-Herausforderungen.

Wenn Sie Fragen oder Projekte haben, schreiben Sie uns unter **office@riskexperts.at,** oder rufen Sie uns an unter **+43-1-713 50 96** und in dringenden Fällen unter der 24-Stunden-Hotline **+43-676 88 626 676.**

Ing. Mag. Gerald Netal, MBA

DI Gerhart Ebner

Fotos: Weinkirn


SEIFE
SOAP
UUH!
VORSICHT!

Josef Zotter fürchtet sich nicht vor Risiken.

Harald Mahrer und Gerhart Ebner diskutieren über aktuelle Herausforderungen im Unternehmertum.

INHALT

Fotos: Zotter Presse Fotos | Thomas Topf

WALDBRÄNDE

Österreich verzeichnete 2018 einen Sommer der Extreme. Die Waldbrandsaison ging mit 63 Bränden zu Ende, 42 davon gab es alleine im August. Müssen wir uns künftig vermehrt an Naturkatastrophen gewöhnen?

Auf den heißesten Mai seit 150 Jahren folgte 2018 ein Sommer der Extreme: Hitze, Trockenheit, daneben Starkregen und Überschwemmungen. Dass Österreich von den Folgen des Klimawandels immer mehr betroffen ist, belegen diese Zahlen: In der Alpenrepublik sind die Durchschnittstemperaturen in den vergangenen 140 Jahren um zwei Grad gestiegen, weltweit hingegen nur um 0,9 Grad. Das bleibt nicht ohne Folgewirkung für die Natur. In der heurigen Waldbrandsaison wurden 63 Brände gemeldet, wie das Institut für Waldbau der Boku Wien berichtet. Der größte Waldbrand des Jahres ereignete sich am 21. August im südlichen Oberösterreich. Oberhalb von Hallstatt geriet ein steiles Waldgebiet in Brand und konnte erst nach vier Tagen endgültig gelöscht werden.

Foto: Fotolia

NEUGRÜNDUNGEN

Nur 50 Prozent bestehen länger als fünf Jahre

Lediglich jede zweite neugegründete Firma im Bereich Finanz- und Versicherungs-Dienstleistungen hält sich länger als fünf Jahre am Markt. Das zeigen aktuelle Daten der Statistik Austria. Positiv sticht der Energiesektor mit der größten Überlebensrate hervor.

Viele Unternehmen gibt es nur wenige Jahre. Versicherungsmakler, Fondsmanager, Gutachter: 565 Firmen sind u. a. in diesem Tätigkeitsbereich im Jahr 2011 neugegründet worden. Ihre Überlebensrate lag fünf Jahre später nur noch bei 51,5 Prozent, wie die Statistik Austria in ihrem aktuellen Bericht zur Unternehmensdemografie aufzeigt.

Die Überlebensrate einer Gründungskohorte fällt naturgemäß von einem Jahr aufs andere. Im Wirtschaftsbereich insgesamt beträgt die Überlebensrate von neugegründeten Unternehmen nach einjähriger Tätigkeit 87,9 Prozent (beispielhaft hier das Jahr 2011-2012). Die Zweijahresüberlebensrate (von 2011-2013) beträgt laut Statistik Austria 72,9 Prozent, nach vier Jahren sinkt diese auf 55,5 Prozent und liegt nach fünf Jahren bei 50,2 Prozent. Das heißt: Jedes zweite 2011 gegründete Unternehmen war 2016 nicht mehr am Markt.

Energiebranche mit hohen Raten

Besonders hohe „Fünfjahresüberlebensraten“ haben Gründungen im Bereich „Energieversorgung“ – drei von vier 2011 gegründeten Firmen in diesem Bereich waren 2016 noch tätig. Dahinter rangiert „Wasserversorgung und Abfallentsorgung“ mit 68,9 Prozent sowie „Herstellung von Waren“ mit 61,8 Prozent. Unterdurchschnittliche Raten weisen die Sparten „Beherbung und Gastronomie“ (45 Prozent) oder Verkehr (42,2 Prozent) auf.

Die besten Überlebenschancen waren bei Beschäftigtengrößen von „zehn und mehr unselbstständig Beschäftigten“ gegeben (61,7 Prozent). Im Bundesländervergleich stechen Vorarlberg, Tirol und Salzburg mit hohen Fünfjahresüberlebensraten hervor, während Wien, das Burgenland und Kärnten unter dem Durchschnitt liegen.

Der Fokus der Statistik zur Unternehmensdemografie liegt auf Neugründungen und Schließungen sowie dem Überleben von Unternehmen, heißt es von der Statistik Austria. Aus diesen Daten werden Indikatoren wie Neugründungs-, Schließungs- und Überlebensraten abgeleitet. Keine Aussage wird darin über Umstrukturierungen (z. B. Fusionen und Übernahmen), Insolvenzen oder Betriebsnachfolgen getroffen.

Foto: Fotolia

Cyber-Security-Hotline der WKO

Soforthilfe für Betriebe: Unter der Hotline 0800 888 133 steht von Cyberkriminalität betroffenen Unternehmen ab sofort eine kostenlose telefonische Notfallhilfe zur Verfügung. Die Nummer ist rund um die Uhr, sieben Tage die Woche besetzt. Für Hilfe darüber hinaus sorgt von Montag bis Freitag jeweils von 8 bis 18 Uhr ein ebenfalls neu eingerichteter Bereitschaftsdienst von IT-Security-Experten. KMU und Unternehmensbereiche wie die Personalabteilung und der Vertrieb gelten als besonders verwundbar, da sie regelmäßig E-Mails von fremden Personen mit unbekannten Anhängen oder Links erhalten.

49 %
der Unternehmen weltweit wurden in den vergangenen zwei Jahren Opfer von Wirtschaftskriminalität, berichtet das Beratungsunternehmen „PwC".

62 %
und somit am stärksten betroffen davon ist das Versicherungswesen, gefolgt von Agrarindustrie und Kommunikationsbranche.

VERSICHERUNG

Anstieg des Prämienvolumens

Österreichs Versicherungsunternehmen haben im zweiten Quartal 2018 einen Anstieg des Prämienvolumens um 3,5 Prozent auf 4,14 Milliarden Euro erzielt. Das geht aus dem aktuellen Bericht der Finanzmarktaufsichtsbehörde (FMA) hervor. Wachstum gab es in den Sparten Schaden/Unfälle (+4,94 Prozent), in der Krankenversicherung (+4,31 Prozent) und in der Lebensversicherung (+0,86 Prozent). Der Solvabilitätsgrad der österreichischen Versicherungsunternehmen war zur Jahresmitte 2018 zufriedenstellend: Mehr als die Hälfte der Unternehmen hatten einen SCR-Solvabilitätsgrad von mehr als 220 Prozent und verfügten somit über doppelt so hohe Eigenmittel wie erforderlich.

Fotos: Fotolia

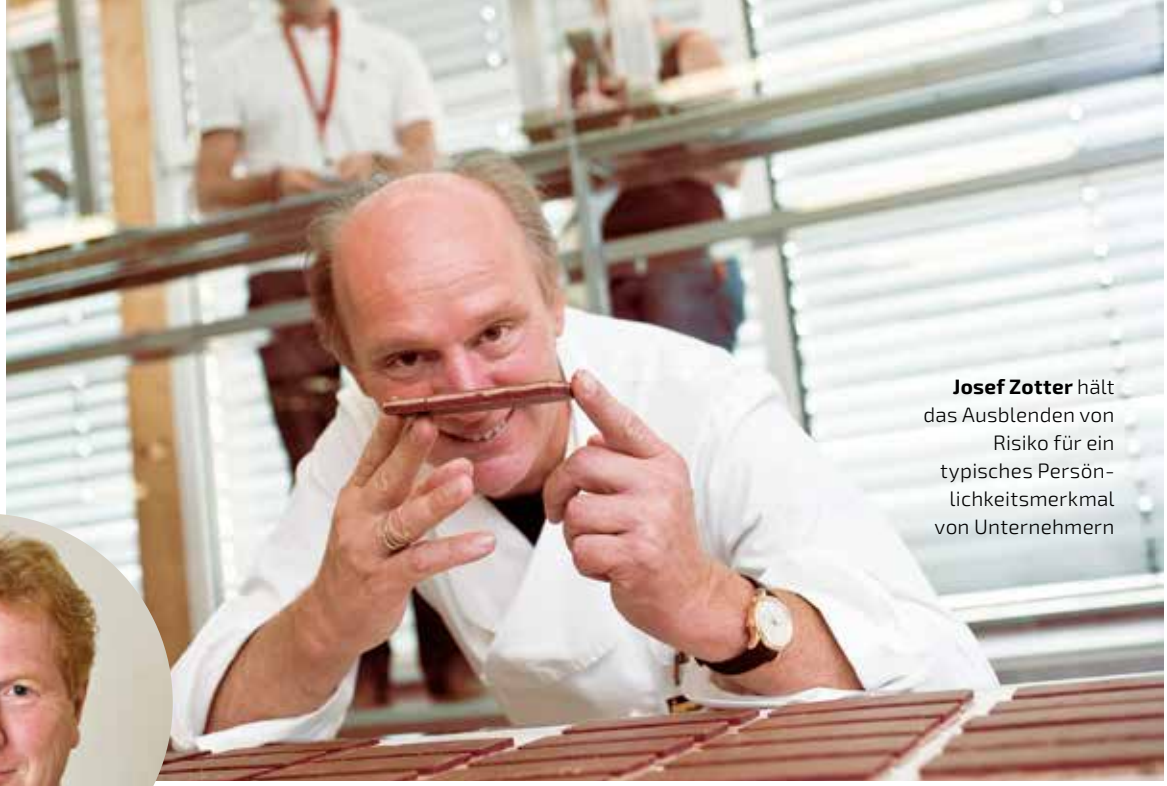
OGH-Urteil im Nachbarschaftsstreit

Die intensive Blendung durch eine Solaranlage am Dach des Nachbarn muss nicht hingenommen werden, zu diesem Schluss kommt der Oberste Gerichtshof (OGH). Zur Vorgeschichte: Ein Grundstücksbesitzer montierte auf seinem Wintergarten zwei Solarkollektoren, die in den Sommermonaten intensive Blendungen auf Balkon und Terrasse eines Nachbarn hervorriefen. Dieser klagte, weil ein Aufenthalt ohne Sonnenschutz auf Balkon und Terrasse zu bestimmten Uhrzeiten nicht mehr möglich war. Das Erstgericht befand den Beklagten für schuldig. Das Berufungsgericht hingegen wies die Klage ab mit dem Argument, der geblendete Kläger könne sich durch Sonnenschirme schützen. Schließlich schloss sich der OGH in seinem Urteil dem Erstgericht an: „…ortsunübliche und wesentliche, die Nutzung seines Grundstücks beeinträchtigende Immissionen vom Nachbargrundstück" seien nicht hinzunehmen.

DRAHTSEILAKT GESCHÄFTS-FÜHRUNG

Foto: Fotolia

Manager unter Druck. Die Liste der Pflichtverletzungen, für die Geschäftsführer haften, wird jedes Jahr länger. Egal ob Datenlecks, Verstöße gegen das Arbeitsrecht oder Korruptionsvorwürfe – am Ende ist immer der Chef schuld. Mit diesem Risiko umzugehen erfordert viel Mut und Wissen. Ein Blick auf die Erfahrungen von Risikoforschern und Piloten kann helfen, das zu meistern.



Josef Zotter hält das Ausblenden von Risiko für ein typisches Persönlichkeitsmerkmal von Unternehmern

Foto: Zur Verfügung gestellt | Zotter PR

Heimo Gruber ist Experte für Haftpflichtfragen und Internationales bei Risk Experts

Der Weg an die Spitze endet oft mit einer Überraschung. Sobald sie nach Jahren harter Arbeit in der Vorstandsetage angekommen sind, merken Manager, dass die Welt ein Ort voll Paragraphen ist. Von einem Tag auf den anderen sind sie für Dinge verantwortlich, deren Existenz sie früher nicht einmal ahnten: die Einhaltung von komplexen Feuerschutzbestimmungen zum Beispiel. Oder von Vorgaben darüber, wie jede einzelne Kachel in der Betriebskantine normgerecht zu verlegen ist. Dass Geschäftsführer auch für alle kaufmännischen Fehlentscheidungen mit ihrem persönlichen Vermögen haften, erscheint angesichts der unzähligen anderen juristischen Bedrohungen fast schon als eine Kleinigkeit. Bald, sagen Beobachter hinter vorgehaltener Hand, werde es daher kaum noch Leute geben, die sich den Geschäftsführerjob überhaupt noch antun.

„Jammern ist des Unternehmers Gruß. Und des Österreichers sowieso", sagt Josef Zotter, wenn man ihn auf solche Prophezeiungen anspricht. Der steirische Top-Chocolatier denkt gern gegen den Strich und spricht es auch aus. Nach dem Risiko, das er als Chef eines Betriebs mit 21 Millionen Euro Jahresumsatz trägt, gefragt, antwortet er daher: „Es ist nicht so, dass ich Selbstmordgedanken bekomme, weil Unternehmertum so riskant geworden wäre. Klar, wenn ich anfange darüber nachzudenken, was alles schiefgehen kann, dann brauch ich den ganzen Tag, um das aufzuschreiben, und werde trotzdem nicht fertig. Aber ich mach das nicht."

Trotzdem muss auch der notorische Optimist Zotter, der das Ausblenden von Risiko für ein typisches Persönlichkeitsmerkmal von Unternehmern hält, zugeben, dass sich die juristische Bedrohungslage geändert hat. Nicht zum Besseren: „Heute wird bei Schwierigkeiten viel schneller mit Klage gedroht", sagt er.

Christian Knill, CEO der Knill Energy Holding, macht ähnliche Erfahrungen: „Immer mehr gesetzliche Auflagen bedeuten auch immer mehr Risiken, mit denen sich Geschäftsführer konfrontiert sehen." Anfütterungsparagraph, Datenschutzgrundverordnung, ausufernde Dokumentationspflichten – die Liste ist heute schon endlos und wird dennoch von Jahr zu Jahr länger. Kein Wunder, dass Geschäftsführer heute sehr stark darauf drängen würden, dass für sie entsprechende D&O-Versicherungen abgeschlossen werden, sagt Knill. „Noch vor zehn Jahren war das in diesem Ausmaß nicht der Fall."

Heimo Gruber, Experte für Haftpflichtfragen und Internationales bei Risk Experts, bestätigt die zunehmende Sensibilität: „Ich weiß nicht, ob der Job eines Geschäftsführers heute gefährlicher ist als vor fünfzehn Jahren. Die meisten Geschäftsführer sind sich aber der persönlichen Haftung mit ihrem gesamten Privatvermögen bewusst. Das war früher nicht so selbstverständlich."

Warum Klagen immer häufiger werden

Doch dass Geschäftsführer für immer mehr Sachverhalte haften, ist nur ein Teil der Geschichte. Der andere besteht in einer Eskalationsspirale, die zwar vermutlich nicht gewollt war, die aber trotzdem kaum noch aufzuhalten ist. Denn die Tatsache, dass heute fast alle Unternehmen D&O-Versicherungen für ihr Management abgeschlossen haben, hat inzwischen zu einer deutlich höheren Bereitschaft geführt, Ansprüche vor Gericht durchzusetzen – in der durchaus berechtigten Annahme, bei der gegnerischen Versicherung könnte es etwas zu holen geben.

Doch damit es noch vertrackter wird: Selbst wenn ein Geschäftsführer gerne darauf verzichten würde, bei Streitigkeiten mit der ganzen Palette der rechtlichen Möglichkei-

ten aufzufahren – er kann sich das de facto nicht erlauben. Denn versäumt er es, berechtigte Forderungen einzuklagen, kommt er selbst in die Haftung. In die er übrigens auch ohne direktes eigenes Verschulden gelangen könne, wie Heimo Gruber erklärt: „Bei Unternehmen mit mehreren Geschäftsführern oder Vorständen kommt das Prinzip der solidarischen Haftung zum Tragen. Das heißt, jeder Vorstand haftet im Prinzip auch für die Fehler seiner Kollegen."

Die gestiegene Bereitschaft zu klagen zieht logischerweise auch einen höheren Prozentsatz an ungerechtfertigten Forderungen nach sich. „Eine wichtige Funktion von D&O-Versicherungen besteht daher darin, solche Ansprüche abzuwehren. Das können auch Ansprüche der eigenen Gesellschaft sein. Um das zu tun, fallen ja häufig hohe Anwaltskosten an, auch Kosten für Sachverständige. Ohne eine entsprechende Versicherung kann sich ein einzelner Geschäftsführer diese Kosten unter Umständen gar nicht leisten, selbst wenn er im Recht ist", sagt Gruber.

Risikomanagement als Teil der Betriebskultur

So unverzichtbar D&O-Versicherungen sind, letztlich bieten sie nur ein allerletztes Back-up, das zumindest den finanziellen Verlust für die haftende Person eingrenzt. Risikominimierung im Vorfeld wirkt besser. Hier können Unternehmen nach wie vor viel aus den Erfahrungen jener Branchen lernen, in denen Fehler unmittelbare Lebensgefahr bedeuten: Der Luftfahrt, der Medizin, manchen Risikosportarten, aber auch aus bestimmten Bereichen des Bauwesens.

Piloten zum Beispiel werden darauf trainiert, ihre Entscheidungen so strukturiert wie nur möglich zu treffen. Dazu dienen nicht nur die berühmten Checklisten, auf denen jede denkbare Situation abgebildet ist, bis hin zur Frage, ob die Crew vor der Landung das Fahrwerk ausgefahren hat. Bei jeder Entscheidung an Bord werden außerdem zunächst einmal alle denkbaren Alternativen durchgegangen, ihre Folgen abgeschätzt und erst dann fällt die Entscheidung, die dann laufend darauf geprüft wird, ob sie unter eventuell geänderten Bedingungen noch immer richtig ist.

Der Pilot von heute dreht also nicht ständig an irgendwelchen Knöpfen herum, der Hauptteil seiner Arbeit ist das Durchdenken von Szenarios, auch solcher, die hoffentlich nicht eintreffen werden: Was tun wir, wenn ein Triebwerk ausfällt? Fliegen wir weiter oder kehren wir um, wenn ein Passagier über dem Atlantik ernsthaft krank wird? Bis wohin würde der aktuell vorhandene Treibstoff reichen?

Unternehmen handeln ähnlich, doch nicht immer konsequent genug. Nicht immer wird wirklich die gesamte Organisation auf etwaige Risikoquellen durchleuchtet, nicht immer werden alle Folgen von Entscheidungen bedacht. Sehr häufig ist von solchen blinden Flecken der IT-Bereich betroffen, in dem Administratoren naturgemäß weitreichende Zugriffsrechte haben: „Hier ist es erforderlich, sie in entsprechende Kontrollsysteme einzubinden", sagt Gruber.

Ortwin Renn, einer der bekanntesten deutschen Risikoforscher, Gründungsdirektor am Zentrum für Interdisziplinäre Risiko- und Innovationsforschung der Universität Stuttgart und wissenschaftlicher Direktor am Institute for Advanced Sustainability Studies in Potsdam, nennt noch einen weiteren Grund, warum Risiken nicht erkannt werden: Selbstüberschätzung. „Eine der größten Gefahren besteht darin, die eigene Fähigkeit, mit einer Risikosituation fertigzuwerden, zu überschätzen", sagt er. Als simples, aber wirksames Gegenmittel empfiehlt Renn, nicht immer nur auf die eigene Stimme zu hören.

Etwas, was in der Luftfahrt seit dem Unglück von Teneriffa (1977), bei dem 583 Menschen starben, weil ein Kapitän die Bedenken seines ersten Offiziers überhörte, Standard ist. Nicht nur aus Sicherheitsgründen empfiehlt Andreas Rieckert, Senior First Officer bei der Lufthansa und zugleich auch Master of Business Administration, Managern bei Entscheidungen auch die Meinung ihrer Teams einzuholen: „Ein Unternehmenschef, der niemanden anhört, bringt sich oft um die besten Ideen."

Unschuld beweisen können

Wahr ist freilich auch: Selbst das beste Risikomanagement, kann keine hundertprozentige Sicherheit bringen. Josef Zotter führt dafür ein überaus plakatives Beispiel ins Feld: „Wir haben für unseren essbaren Tiergarten eine Waffe, weil ja der dazu ausgebildete Mitarbeiter zu gegebenem Zeitpunkt auf die Weide geht, um ein Tier zu schießen. Die Waffe ist in einem sicheren Schrank verwahrt und nur die berechtigte Person darf sie entnehmen. Aber ich kann nicht den ganzen Tag danebenstehen und verhindern, dass er sie nicht an jemand anderen weitergibt oder gar wild um sich schießt. Andererseits weiß ich, dass ich mein Bestmögliches getan habe, um jemanden für diesen Job zu finden, der das mit nahezu hundertprozentiger Sicherheit nicht tun wird."

Nach bestem Wissen und Gewissen zu handeln, sei neben Versicherungen, die „grundsätzlich durchaus Sinn machen", auch für Andreas Fill, Geschäftsführer und Eigentümer des gleichnamigen oberösterreichischen Maschinenbauunternehmens, der beste Weg, um als Unternehmer für juristisch schwierige Situationen gerüstet zu sein. Als besonders gefährlich empfindet Fill seinen Job übrigens nicht: „Da gibt es sicher ganz andere Risikoberufsgruppen."

Anders als noch vielleicht vor fünfzehn Jahren kommen Geschäftsführer heute allerdings nicht darum herum, ihr Handeln nach bestem Wissen und Gewissen auch penibel zu dokumentieren. „Im Schadensfall muss ein Manager beweisen können, dass er seiner Sorgfaltspflicht nachge-

kommen ist, dass er das Risiko analysiert hat, dass er alle Organe, die bei wichtigen Entscheidungen informiert werden sollten, tatsächlich informiert hat, sich im Gegenzug aber auch ausreichend informieren hat lassen", sagt Risiko-Profi Gruber.

Galt einst die launige Feststellung „Jedes Schriftl ist a Giftl" unter manchen Managern als oberste Handlungsmaxime, so hat sich die Situation inzwischen völlig gedreht: „Wer nicht sorgfältig das Wesentliche dokumentiert, kann sich im Fall des Falles auch nicht freibeweisen, zumal die Beweislast, dass alles ordnungsgemäß abgelaufen ist, auf Seite des in Anspruch Genommenen liegt", erklärt Gruber.

Deshalb kann es auch nicht schaden, bei heiklen Entscheidungen belegen zu können, dass man im Vorfeld die Expertise von unabhängigen Sachverständigen und Rechtsanwälten in Anspruch genommen hat. Erstens, um den wichtigen Blick von außen zu bekommen, aber auch weil sie im Schadensfall entlastend wirken. Wenn ein externer Jurist eine Konstruktion für gesetzlich korrekt befunden hat, hat das eine andere Aussagekraft, als wenn eine solche Aussage von jemanden kommt, der im Haus tätig ist und womöglich in einem Netz von Abhängigkeiten und Rücksichten agieren muss.

Vorsicht DSGVO

Freude mit der Notwendigkeit, jeden einzelnen Schritt penibel und nachvollziehbar dokumentieren zu müssen, haben die meisten Manager nicht. Christian Knill ärgert sich vor allem über jene Dokumentationspflichten, denen er keinen Sinn abgewinnen kann: „Als Geschäftsführer der Holding bin ich unter anderem mit Finanzierungsfragen beschäftigt. Und hier fällt mir schon auf, dass wir mittlerweile, nur um rechtlich abgesichert zu sein, regelrechte Papierberge produzieren müssen, die eigentlich verzichtbar wären." Einen ähnlichen Effekt, sagt er, habe die DSGVO. „Da hat mir ohnehin bislang niemand schlüssig erklären können, welchen Vorteil die haben soll."

Tatsache ist allerdings, dass die DSGVO zwei wichtige neue Fakten schafft, die Unternehmen dazu zwingen, die Verordnung exakt einzuhalten. Zum einen legt sie für Vergehen eine klare strafrechtliche Verantwortung fest, gegen die man sich, wie gegen jedes andere strafrechtliche Risiko auch, nicht versichern kann. Andererseits ist es nicht auszuschließen, dass in Zukunft einzelne Personen bewusst darauf spekulieren, dass ein Unternehmen Daten, über die es laut DSGVO auskunftspflichtig ist, nicht parat hat, um mit Klagsdrohung Abschlagzahlungen zu erreichen – ein weiteres Szenario, das Unternehmer, gleich Piloten, im Voraus bedenken sollten, obwohl die Eintrittswahrscheinlichkeit nicht übermäßig hoch ist.

INTERVIEW

„WER GAR KEIN RISIKO EINGEHT, ERSTARRT."

Der Risikoforscher Ortwin Renn erklärt, warum Risiko sinnvoll sein kann und nicht-existierende Freunde, Sicherheit geben.

Teilen Sie das Urteil, dass wir – und hier meine ich vor allem den deutschsprachigen Raum – risikoaverser geworden sind?

ORTWIN RENN: Ob wir generell risikoscheuer geworden sind, kann ich nicht sagen, weil sich mit der Zeit ja auch die Art der Risiken ändert. Was aber auf jeden Fall stimmt ist die Tatsache, dass wir uns vor Dingen, die uns heute viel weniger bedrohen als noch vor zwanzig oder dreißig Jahren, mehr fürchten als damals.

Hätten Sie da ein Beispiel?

RENN: Nehmen Sie die Kriminalität, die seit Jahren eher abnimmt bzw. auf gleichem Niveau bleibt, vor der sich die Menschen aber dennoch immer mehr fürchten. Oder chemische Zusätze in Lebensmitteln: Die waren früher viel häufiger und auch viel gesundheitsgefährdender als heute und trotzdem ist die Angst vor Chemie im Essen heute so groß wie noch nie.

Unternehmer sprechen in diesem Zusammenhang gern von einer Regulierungswut, die ohnehin minimale Gefahren noch weiter minimieren will.

RENN: Wir hatten früher in Deutschland über 5.000 tödliche Betriebsunfälle, heute sind es 375. Hier und in vielen anderen Bereichen haben Regulierungen also einen wichtigen Beitrag zur Risikoreduktion geliefert. Inzwischen sind wir aber an einem Punkt angelangt, wo der Grenznutzen immer geringer wird. Mit immer größerem finanziellen und bürokratischen Aufwand erreichen wir nur noch minimale Verbesserungen.

Dass man das trotzdem tut, liegt vermutlich an der Vorstellung, hundertprozentige Sicherheit wäre möglich.

RENN: Ja, denn diese Vorstellung ist in unserem Alltagsdenken sehr stark verankert. Wenn Sie über eine

Ortwin Renn gilt als der bekannteste deutsche Risikoforscher

Foto: Zur Verfügung gestellt

Brücke fahren, wollen Sie, dass diese Brücke sicher ist. Sie kommen gar nicht auf die Idee zu überlegen, dass es unter einer bestimmten Belastung die Wahrscheinlichkeit gibt, dass die Brücke einstürzt, diese Wahrscheinlichkeit aber so gering ist, dass Sie trotzdem über die Brücke fahren. Es ist auch sehr verwirrend zu erfahren, dass ein Lebensmittel zu neunzig Prozent gesund ist, man aber unter bestimmten Umständen davon Krebs bekommen kann. Zumindest in der Wissenschaftstheorie ist es aber seit der stochastischen Wende unumstritten, dass es weder hundertprozentige Sicherheit noch hundertprozentige Unsicherheit gibt. Ebenso wenig ist etwas hundertprozentig gesund oder ungesund. Es geht immer um Wahrscheinlichkeiten.

Die Tatsache, dass man Risiken nicht auf null drücken kann, ist ein pragmatischer Grund, sie bis zu einem bestimmten Grad in Kauf zu nehmen. Gibt es aber nicht auch ein per se gutes Risiko?

RENN: Wir sprechen nicht zufällig von Risiko und das verträgt sich nicht wirklich mit dem Adjektiv gut. Aber natürlich geht es immer um eine Risiko-Nutzen-Abwägung, selbst in so heiklen Bereichen wie der Gesundheit. Ein einfaches Beispiel: Wenn Sie in ein fremdes, exotisches Land fahren, haben Sie ein erhöhtes Risiko zu erkranken. Trotzdem nehmen es viele von uns in Kauf, weil der Gewinn, der mit einer solchen Reise verbunden ist, mehr wiegt. Noch deutlicher ist das im Finanzbereich, wo nur derjenige gewinnen kann, der auch etwas riskiert. Und generell gilt: Wenn Sie gar kein Risiko mehr eingehen, das Haus nicht mehr verlassen, dann sind Sie de facto erstarrt, Sie können sich nicht weiterentwickeln. Da gilt tatsächlich der Spruch: Zu Tode gefürchtet, ist auch gestorben.

Wie komme ich aber zu einer guten Risikoeinschätzung?

RENN: Da gibt es sehr viele Faktoren, die entscheidenden Punkte sind aber immer das mögliche Schadensausmaß und die Eintrittswahrscheinlichkeit. Wenn der größtmögliche Schaden der Verlust von fünf Euro ist, werde ich ganz andere Eintrittswahrscheinlichkeiten akzeptieren, als wenn es um mein ganzes Vermögen oder gar meine Gesundheit geht.

Kritisch sind allerdings die Entscheidungen, wo ich zwar das mögliche Schadensausmaß kenne, nicht aber die Eintrittswahrscheinlichkeit.

RENN: Ja, das ist schwierig und das kommt häufig vor. Hier kann ich versuchen herauszufinden, wie das Risiko verteilt ist und mich danach richten. Bei linear ansteigendem Risiko kann ich dann dynamisch vorgehen: also ein Stück in das Risiko hineingehen und je nachdem, wie die Rückmeldung ausfällt, dann noch ein weiteres Stück. Dort, wo es einen Schwellenwert gibt, ab dem das Risiko-Ereignis in vollem Ausmaß eintritt, hilft mir diese Vorgangsweise allerdings wenig. Unabhängig davon besteht die größte Gefahr aber ohnehin darin, die eigene Fähigkeit, mit einer Risikosituation fertigzuwerden, zu überschätzen. Sie wissen ja: 80 Prozent der Deutschen halten sich für bessere Autofahrer als der Durchschnitt. Das kann aber rein rechnerisch nicht funktionieren.

Und wie schütze ich mich vor Selbstüberschätzung?

RENN: Da gibt es ein sehr hilfreiches Gedankenexperiment. Überlegen Sie, bevor Sie ein Risiko eingehen, ob Sie einem Freund empfehlen würden, dieses Risiko einzugehen. Wenn Sie zu der Antwort kommen, dass Sie einem Freund abraten würden, aber glauben, das Risiko aufgrund Ihrer Fähigkeiten oder Ihres Wissens trotzdem eingehen zu können, dann ist das der Moment zu prüfen, ob Sie wirklich um so viel besser sind als der imaginäre Freund oder ob Sie sich vielleicht doch überschätzen.

FAKTEN ZU D&O VERSICHERUNGEN

1-2
Seiten hatten D&O-Polizzen vor 30 Jahren.

25 UND MEHR
Seiten haben D&O-Polizzen heute.

20%
der Geschäftsführer waren bereits mit konkreten Haftungsansprüchen konfrontiert.

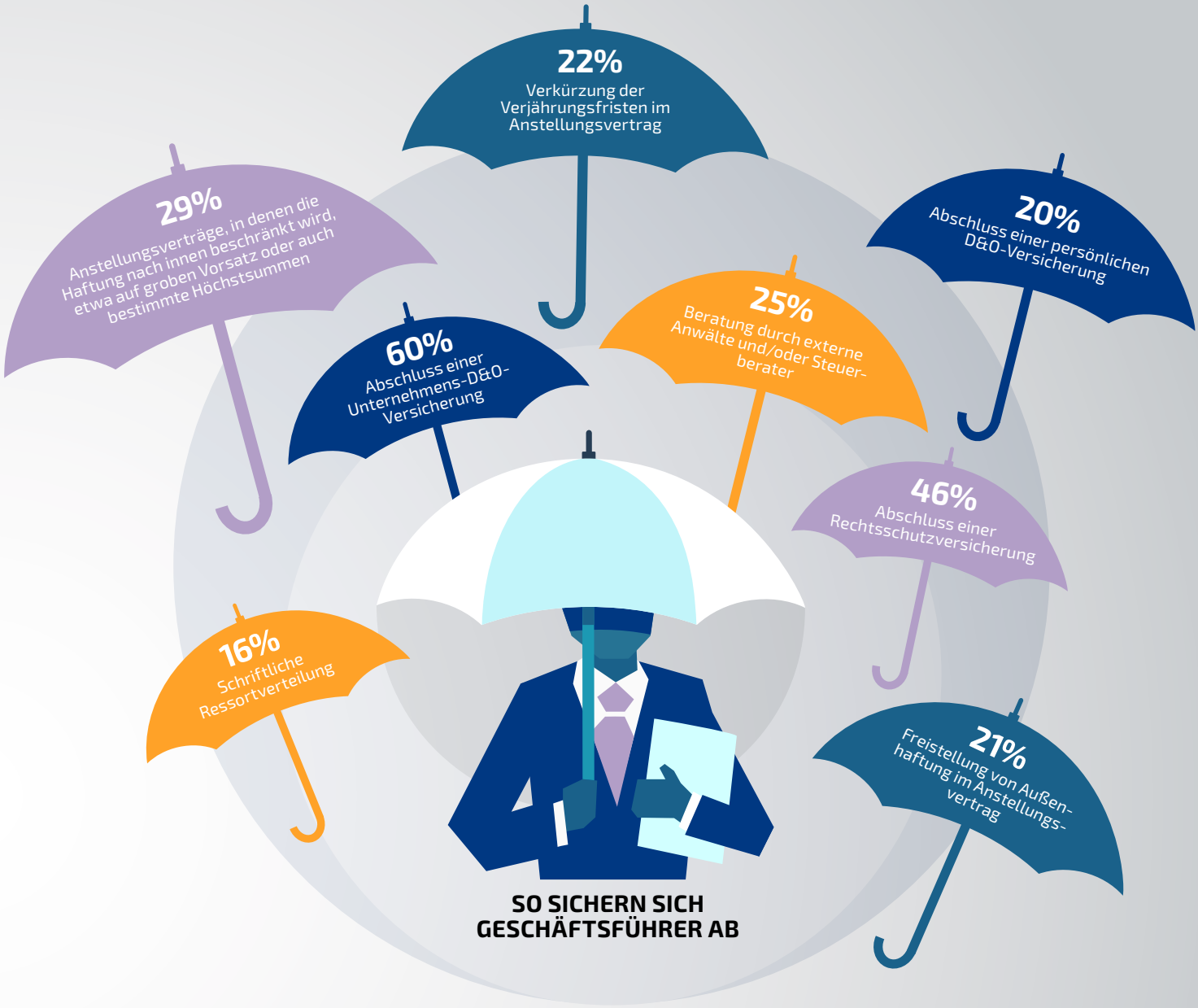
60%
der Geschäftsführer haben eine D&O-Versicherung.

2,3
Milliarden – Marktvolumen für D&O-Versicherungen europaweit

VERURTEILT!

900
MIO. EURO FÜR EINEN SATZ:
Weil er die Kreditwürdigkeit des Medienunternehmers Leo Kirch in einem Interview bezweifelt hatte, wurde ein ehemalige Manager der Deutschen Bank von Kirchs Erben auf diese Summe geklagt.

815.000
EURO STRAFE FÜR BIERBRAUER:
Diese Summe musste der Geschäftsführer einer Brauerei bezahlen, weil er sich nicht auf das Kerngeschäft des Bierbrauens beschränkte und dabei Verluste einfuhr.



SO SICHERN SICH GESCHÄFTSFÜHRER AB

90%

der Finanzvorstände finden, dass das Haftungsrisiko vor fünf Jahren niedriger war.

72%

der Finanzvorstände glauben, dass Versicherungen allein nicht reichen, um ihr Haftungsrisiko zu minimieren.

SO EMPFINDEN MANAGER IHR HAFTUNGSRISIKO

Quellen: Finaccord D&O Studie 2014, VOV D&O-Studie 2014, Aichinger 2016, Finance CFO)

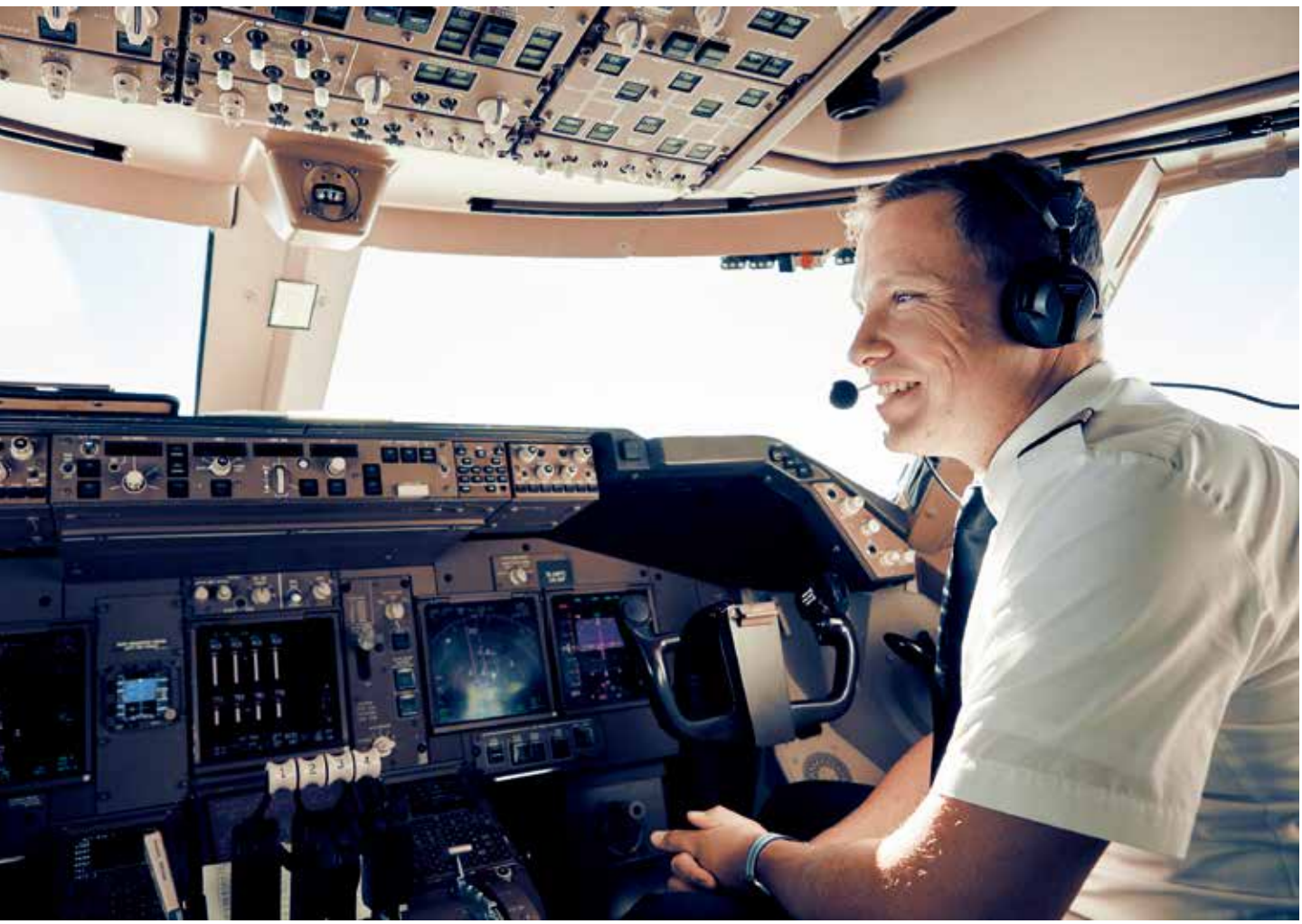


Foto: Zur Verfügung gestellt

INTERVIEW

„EIN EINZELNER FEHLER FÜHRT SELTEN ZUR KATASTROPHE“

Andreas Rieckert, First Senior Office bei der Lufthansa, verrät, was Manager von Piloten lernen können.

Was können Piloten bezüglich Risiko besser als Manager?

ANDREAS RIECKERT: Für den Einzelfall kann man das natürlich nicht sagen. Worin die Luftfahrt aber sehr gut ist, ist die Fehleranalyse. Weil in der Fliegerei Unfälle fast immer ein sehr großes Schadensausmaß bedeuten, sind wir dazu gezwungen, auch bei kleinsten Fehlern, die wir erkennen, den Kreis zu schließen und Vorkehrungen zu treffen, damit derselbe Fehler unter gleichen Umständen nicht noch einmal passiert. Denn ein einzelner Fehler führt selten zur Katastrophe, es sind fast immer ganze Fehlerketten. Und die gilt es von Beginn an zu durchbrechen. In gewissem Sinn haben wir es aber auch leichter als Manager, weil bei uns Sicherheit immer die absolute Priorität hat. Bei einem Unternehmer sind die Prioritäten weniger klar. Manchmal ist es auch die Sicherheit, ein anderes Mal Innovation und noch ein anderes Mal Gewinnmaximierung. Solche Entscheidungen müssen Piloten nicht fällen.

Gesetzt den Fall, die Prioritäten sind bereits klar gesetzt, wie komme ich dann, oft unter Druck und mit beschränkten Ressourcen, zu möglichst guten Entscheidungen?

RIECKERT: Indem ich so strukturiert wie möglich vorgehe. Da gibt es von der NASA ein sehr gutes Modell, das im Wesentlichen darauf basiert, zunächst einmal alle möglichen Handlungsalternativen zu sammeln, dann deren möglichen Folgen abzuschätzen und auf dieser Basis die Entscheidung für eine der Optionen zu treffen. Dazu kommen dann aber noch zwei weitere sehr wichtige Elemente: die ständige Evaluation der getroffenen Entscheidung, das heißt das ständige Überlegen, ob zum Beispiel ein wegen Schlechtwetters gewählter Ausweichflughafen immer noch die beste Lösung ist. Und schließlich eine klare Kommunikation über den Entscheidungsprozess.

Mit den beiden letzten Punkten haben Unternehmen allerdings recht häufig Probleme. Da wird eine einmal gefasste Entscheidung ohne Rücksicht auf Verluste durchgezogen und kommuniziert wird sie auch nicht immer eindeutig.

RIECKERT: Das ist in der Fliegerei früher auch vorgekommen. Nach der bisher schwersten Katastrophe der zivilen Luftfahrt ohne terroristischen Hintergrund, dem Unfall von Teneriffa im Jahr 1977, bei dem 583 Menschen ums Leben kamen, hat man aber erkannt, dass schlechte Kommunikation und das Festhalten an einer einmal gefassten Entscheidung letztlich die Hauptursachen für die Katastrophe waren. Da war ein Kulturwandel unumgänglich.

Und er hat auf Anhieb funktioniert?

RIECKERT: Es ging natürlich nicht von heute auf morgen. Aber heute hat sich bei allen großen Fluggesellschaften eine Fehlerkultur entwickelt, bei der man für Fehler, die man nicht bewusst herbeigeführt hat oder sie aus Bequemlichkeit bzw. Ignoranz machte, nicht bestraft wird. So ist es überhaupt erst möglich, über Fehler offen zu reden und Maßnahmen zu treffen, die den gleichen Fehler in Zukunft verhindern. Die zweite große Lehre aus Teneriffa war, dass man Hierarchiestrukturen abgeflacht hat. Heute sind Kapitäne darauf trainiert, ihre Crew so zu führen, dass jeder Einwände äußern kann, wenn er meint, der Chef hätte einen Fehler gemacht oder etwas übersehen. Wäre ein solches Verhalten schon damals auf Teneriffa Standard, hätte man den Unfall wahrscheinlich verhindern können. Denn der erste Offizier eines der damals verunglückten Flugzeuge hat sehr wohl versucht, seinen Chef auf dessen Fehler aufmerksam zu machen, kam damit aber nicht durch.

In Industrieunternehmen soll das auch heute noch vorkommen.

RIECKERT: Ja, vor allem in familiengeführten Unternehmen gibt es manchmal immer noch den Patriarchen, dessen Wort Gesetz ist. Nach allem, was wir aus der Fliegerei wissen, wirkt eine solche Konstellation aber massiv risikotreibend. Außerdem bringt sich ein Unternehmenschef, der niemanden anhört, oft um die besten Ideen.

Fehlerkultur, Kommunikation auf Augenhöhe, radikale Analyse auch von scheinbar belanglosen Fehlern – was könnten Industriemanager sich noch von der Luftfahrt abschauen?

RIECKERT: Bei sicherheitskritischen und sich stets wiederholenden Aufgaben sind verbindliche Checklisten eine sehr gute Maßnahme, um das Risiko zu senken. Boeing hat schon 1930 das erste Flugzeug mit einer Checkliste ausgeliefert. Da stand dann unter anderem: Vor der Landung Fahrwerk ausfahren. Jetzt würde man meinen, das weiß doch jeder Pilot. Ja, und doch gab es eine ganze Reihe von Unfällen, wo die Piloten bei schlechten Bedingungen so sehr auf andere Dinge fixiert waren, dass sie das vergessen haben. Dass Checklisten auch in anderen Bereichen das Risiko massiv senken können, zeigt übrigens die Medizin. Da hat die WHO 2008 ebenfalls begonnen, mit Checklisten zu arbeiten. Auf denen steht so Banales, wie dass eine Operation nicht begonnen werden darf, bevor sich nicht alle die Hände gewaschen haben. An Krankenhäusern, die diese Checkliste konsequent verwenden, hat man die Anzahl von operationsbedingten Infektionen halbiert.

IM GESPRÄCH

„COWBOYS HABEN IMMER SAISON“

Wirtschaftskammer-Präsident Harald Mahrer traf Risk Experts-Gründer Gerhart Ebner zum Gespräch über die Risikobereitschaft von Österreichs Unternehmern in Zeiten der Digitalisierung.

Harald Mahrer: „Schaffen wir mehr Freiräume, steigen die Risiken.“

Fotos: Thomas Topf

RISK REPORT: Herr Mahrer, Herr Ebner, wir sitzen hier in der Wirtschaftskammer, um über die Digitalisierung und ihre Auswirkungen zu diskutieren. Vorweg: Beschäftigen wir uns im geschäftlichen Tun genug mit den Risiken und zu wenig mit Chancen?

GERHART EBNER: Ich habe inzwischen fast aufgegeben, der positiv besetzten „Fiktion Sicherheit“ die Realität „Risiko und Chance“ gegenüberzustellen. Trotzdem kommt die Beschäftigung mit Risiko und Chance auch außerhalb des angelsächsischen Bereichs in Mode, und das ist gut so.

HARALD MAHRER: Ich sehe hier ein anderes Gegensatzpaar, das auch in der Wirtschaftspolitik eine Rolle spielt. Nämlich Freiheit und Sicherheit versus unternehmerische Chance und Risiko. Die große Geschichte ist: Schaffen wir mehr Freiräume, steigen die Risiken. Die Digitalisierung hat in diesem Zusammenhang auch für den Einzelnen ganz neue Themen mit sich gebracht. In einer Welt, in der vom Bankomaten über den Zahlungsverkehr bis zur Energiewirtschaft wirklich alles digital gesteuert wird, ist vielen gar nicht so bewusst, was Systemausfälle für Auswirkungen haben

können. Diese Realität wird sehr treffend im Buch „Blackout“ des österreichischen Autors Marc Elsberg beschrieben.

RISK REPORT: Würden Sie beide sagen, dass die Digitalisierung ein unkalkulierbares Risiko ins Wirtschaften gebracht hat?

EBNER: Nein.

MAHRER: Nein. Man muss auch dazu sagen, dass wir disruptive Veränderungen wie die Digitalisierung in der Geschichte bereits erlebt haben. Es gab in den vergangenen 170 Jahren mehrere technologische Sprünge, die eine ähnliche Qualität hatten und damals extrem dramatisch für die Leute waren. Die industrielle Revolution, die Einführung des elektrischen Stroms in den Städten, die ersten Maschinenfabriken. Auch bei der Einführung des Automobils gab es Leute, die sagten, das setzt sich nie durch. Meine Großmutter erzählte mir, als damals die Waschmaschine kam, demonstrierten in den Städten die Wäschermädel dagegen. Der Unterschied zu bisherigen Technologieentwicklungen: Im Moment passieren die Dinge extrem schnell und in vielen Bereichen gleichzeitig.

EBNER: Und trotzdem werden wir über dieses heute so extrem empfundene Tempo morgen lachen. Fast jeder technologischen Veränderung geht ein 20-jähriger Entwicklungsprozess voraus, man muss eigentlich nur die Augen aufmachen. Es ist ja auch nicht disruptiv, wenn der Mond am anderen Ende des Firmaments steht, nur weil man inzwischen geschlafen hat.

RISK REPORT: Was würde man dann sehen?

EBNER: Wir machen operatives Risk Management. Eines der gängigsten Risiken ist die Betriebsunterbrechung. Wie der Umgang mit Risiken von der Perspektive abhängt, zeigt, dass in der Finanzwirtschaft eine Eintrittswahrscheinlichkeit von 1:100 oft ein akzeptables Risiko darstellt. Für die meisten operativen Risiken ist das ein No-Go. Bei 2.000 betreuten Unternehmen tritt ein Ereignis mit dieser Wahrscheinlichkeit ja 20-mal im Jahr ein.

Gerhart Ebner: „Die Chance liegt darin, Digitalisierung nutzbar zu machen.“

RISK REPORT: Sie beide haben in Ihren Funktionen mit unzähligen Unternehmen zu tun. Wie hat sich Ihrer Einschätzung nach die Risikobereitschaft von Unternehmern entwickelt?

MAHRER: Es gibt kein Unternehmertum ohne Risiko. Bestimmte Dinge sind nicht beherrschbar. Ich kann für ein neues Produkt noch so viele Marktstudien machen, Kundenakzeptanz ermitteln und die Preisakzeptanz erforschen – irgendwann muss ich damit auf den Markt hinaus und erfahre die Wahrheit. Angenommen ich habe eine tolle Idee in meiner Garage, weiß ich trotzdem nicht, was in der Garage auf der anderen Straßenseite passiert. Was heute anders ist: Diese Garage kann auch in Singapur, Shenzhen oder Kuala Lumpur stehen. Damit ist ein massives Risiko verbunden.

EBNER: Auf den großen Risikomanagement-Konferenzen wird immer analysiert: Wann hat welche Aktie durch welches Ereignis an einem Tag zwanzig Prozent oder mehr verloren? Diese Ereignisse waren immer die Folge von unternehmerischen Entscheidungen, die nicht aufgegangen sind. Aber dabei übersieht man gerne, welchen Nutzen Unternehmen aus solchen Entscheidungen ziehen.

RISK REPORT: Also ist die Risikobereitschaft wie eh und je?

MAHRER: Das hängt sicherlich davon ab, ob ich Unternehmer oder angestellter Manager bin, der für seine Entscheidungen anders haftet als der Eigentümer. Hier hat die gesamte Regulatorik enorm angezogen. Compliance, Haftungsvorschriften, man denke an die gesamten Veränderungen im Finanzbereich. Das Korsett ist hier deutlich enger geworden und beeinflusst das Handeln immens. Es werden auch eine ganze Reihe von Entscheidungen nicht getroffen, weil inzwischen Haftungsfragen im Vordergrund stehen.

EBNER: Ja. Das merkt man auch an der gestiegenen Anzahl der D&O-Schäden. Man trifft heute leider viele Entscheidungen, von denen später gesagt wird: Das war wohl State of the Art, so zu entscheiden. Dadurch gehen aber auch sehr viele Chancen verloren.

MAHRER: Das ist sicher der Unterschied zwischen jungen Unternehmen, die wie Schnellboote sind, und etablierten Tankern. Die Entscheidungswege auf den Schnellbooten sind nicht nur kürzer. Auf den Tankern sind im Vorfeld viel mehr Berater involviert, die versuchen, Entscheidungen zu objektivieren.

Das ist heute Standard, Entscheidungen so abzusichern. Ich glaube, vor 25 Jahren haben sich Manager eher bei unterschiedlichen Ansichten Expertise von außen geholt. Aber alleine das Involvement von Externen verlangsamt alles dramatisch.

RISK REPORT: Ist vielleicht jetzt wieder die Zeit der wilden Hunde gekommen, die sagen: „Ich trau mich, das jetzt zu entscheiden, obwohl ich dafür haften könnte, obwohl ich nicht alle Aspekte durch meine Stäbe habe prüfen lassen, aber dafür entscheide ich es jetzt und gehe das Risiko ein, bevor es ein anderer macht"?

MAHRER: Ich glaube, man muss die wilden Hunde ein bisschen entmystifizieren. Cowboys haben immer Saison, wenn das Wetter für sie passt. Sie können aber auch in ein Tal hineinreiten, in dem eine Indianerhorde wartet und das war es mit den Cowboys. Entscheidend bleibt immer die Balance: Was kann ich auf der strategischen, auf der Marktebene an Risiko nehmen und was bin ich auf der operativen Seite bereit zu investieren?

Manchmal braucht es einen Cowboy, der wild entschlossen ist, manchmal einen besonnenen Herzchirurgen, der fein säuberlich mit Ultramikrospezialistentum das eine kleine Teilchen für den Erfolg verändert.

EBNER: Mut ist nicht, dass man wie ein Cowboy irgendwo hineinreitet, sondern auch bereit ist, die negativen Konsequenzen auf sich zu nehmen. Die Ulanen, die mit Speeren gegen Panzer gekämpft haben, waren nicht mutig. Sie waren eigentlich nur „uninformiert".

MAHRER: Aber sagen Sie, Herr Ebner, was ist Ihrer Ansicht nach das größte Risiko für unsere Volkswirtschaft? Was ist ein Risiko, das wir jetzt in einer gemeinsamen Anstrengung beherrschen könnten?

EBNER: Wenn ich mir die nächsten Jahre ansehe, dann sind es ganz klar qualifizierte Mitarbeiter, die Ausbildung und fehlende Skills. Ich sehe ein großes Problem: Wir lernen nicht, nicht-linear zu denken. Aber das wird in fünf bis zehn Jahren ganz entscheidend sein: zwei nicht-lineare Entwicklungen intuitiv zu verknüpfen. Am ehesten lernt man das noch in komplexen Spielen.

MAHRER: Das würde ich zu hundert Prozent unterschreiben. Die Frage der Qualifikation ist das ungelöste Zukunftsthema. Hier werden wir auch sehr ungewöhnliche Dinge in den kommenden Jahren machen und unkonventionell schnell Maßnahmen ergreifen müssen. Sonst wird mangelnde Qualifikation die größte Wachstumsbremse für unsere Wirtschaft sein. Ich stimme Ihnen auch zu, dass wir uns sehr stark an Gamification orientieren müssen. Wir haben erst wieder in Asien gesehen, wie intuitiv der Wissenserwerb erfolgen kann.

EBNER: Das wird ein Wettlauf mit der Zeit.

RISK REPORT: Zum Abschluss: Wird Digitalisierung in Österreich zu sehr als Chance oder in richtigem Maß als Risiko wahrgenommen?

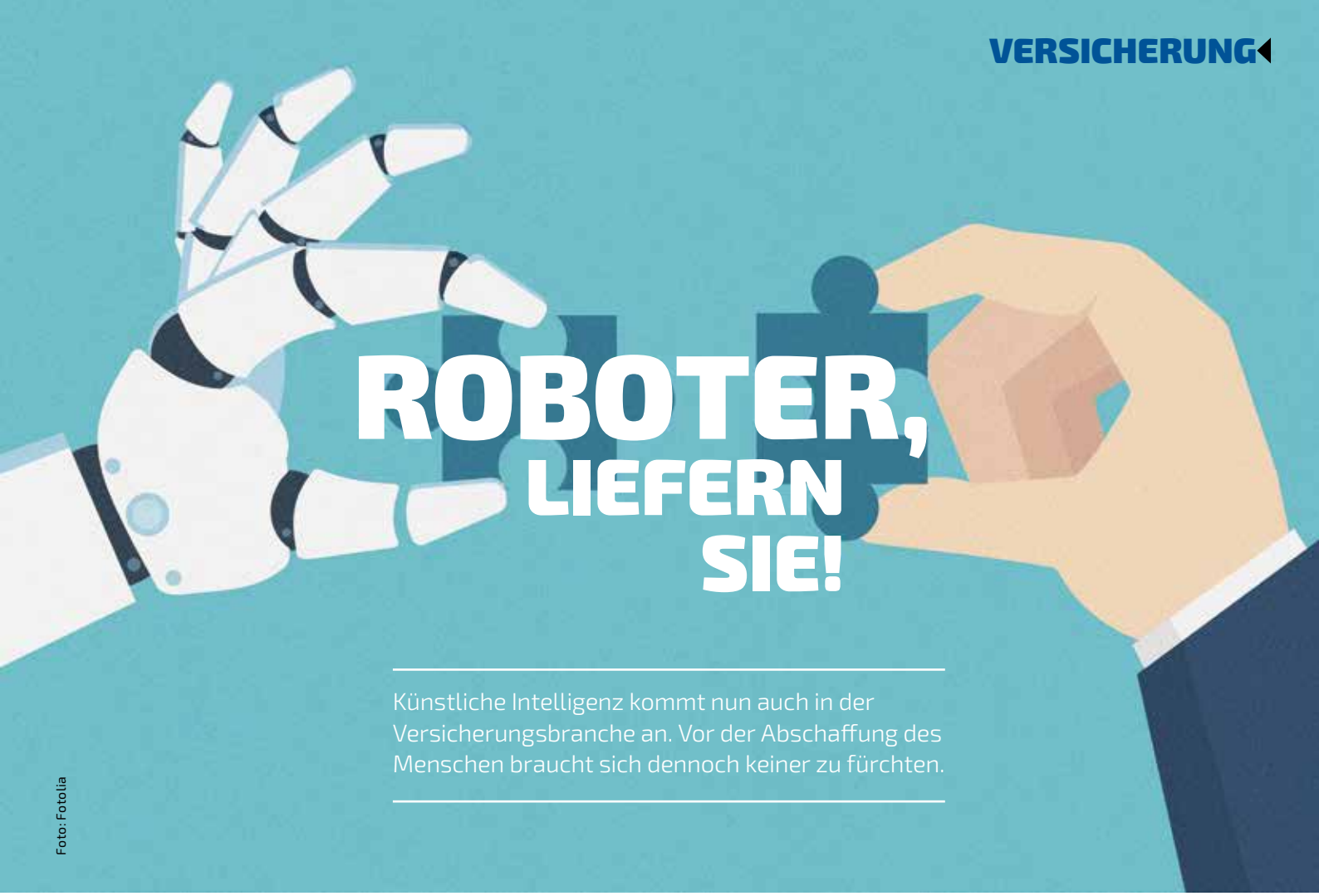
EBNER: Im Mainstream wird Digitalisierung eigentlich vorwiegend als Risiko wahrgenommen. Die Chance freilich liegt darin, Digitalisierung nutzbar zu machen.

MAHRER: Natürlich ist die Digitalisierung eine technologische Veränderung, die unsere Generation und die unserer Eltern so noch nicht erlebt hat. Dieser technologische Fortschritt wird in vielen Bereichen einsetzen. Im Moment sehen wir erst – in einer Restaurantterminologie ausgedrückt – den Gruß aus der Küche. Das mehrgängige Hauptmenü kommt erst. Da ist man natürlich gut beraten, sich darüber den Kopf zu zerbrechen.

EBNER: Ich habe den Eindruck, dass wir in Österreich mit unserer vorsichtigen Mentalität, bei der sich alles ganz sicher rechnen muss, dabei ein bisschen ins Hintertreffen geraten werden.

MAHRER: Ja, aber ich verstehe unseren Ansatz auch. Bei einer derart hohen Unternehmensbesteuerung und einem derart engen bürokratischen Korsett habe ich Verständnis dafür, dass die Risikobereitschaft in manchen Teilen der Wirtschaft weniger stark ausgeprägt ist. Wenn der finanzielle Spielraum einfach nicht da ist, fällt es schwer, ein Risiko zu nehmen. Ich denke, das zu ändern ist wohl die derzeit größte Aufgabe für die Politik.

RISK REPORT: Wir danken für das Gespräch.



ROBOTER, LIEFERN SIE!

Künstliche Intelligenz kommt nun auch in der Versicherungsbranche an. Vor der Abschaffung des Menschen braucht sich dennoch keiner zu fürchten.

Foto: Fotolia

Die Vorstellung ist den meisten Menschen nach wie vor unheimlich: Algorithmen sollen in Zukunft über unsere Sicherheit entscheiden – in selbstfahrenden Autos, in Lufttaxis und nun auch in der Versicherungsbranche. Eigentlich sind solche Systeme aber auch jetzt schon im Einsatz: Flugzeuge können heute nahezu vollautomatisch landen, die unzähligen Assistenzsysteme im Auto fallen uns kaum noch auf und natürlich schließen wir simple Versicherungen per Mausklick im Internet ab.

Ist Künstliche Intelligenz also das nächste große Ding oder doch eine alte Bekannte? Beides. Denn selbst unter Fachleuten herrscht alles andere als Übereinstimmung darüber, was denn überhaupt als Künstliche Intelligenz zu werten ist: schon das Smartphone, das den Weg zum nächsten Café weist? Oder erst ein Cyborg, der sich vom Menschen nur noch darin unterscheidet, dass er kein Bewusstsein hat? Oder muss er Bewusstsein auch noch haben?

KI als Chamäleon

„Es gibt sicher an die hundert Definitionen von Künstlicher Intelligenz", sagt dementsprechend ein Mann, der es wissen muss: Andreas Klug, Vorstand bei ITyX, einem der Pioniere in der Entwicklung von KI-Software. Ihm persönlich sei jene Definition am liebsten, sagt Klug, die Künstliche Intelligenz als das Lernen von Arbeitsschritten durch einen Computer sieht, ohne dass man dafür ein dediziertes Skript schreiben muss. „Stattdessen legt man der Maschine Beispiele vor und sagt: Genauso sollst du das in Zukunft auch tun." Computer, die Muster erkennen, könnten dann zum Beispiel Versicherungsbetrug in Echtzeit aufdecken, indem sie Alarm schlagen, sobald sie Abweichungen zwischen der Schadensmeldung und der dazugehörigen Reparaturabrechnung bemerken.

Doch noch sind solche Anwendungen mehr Wunschdenken denn Realität. „Heute sehen wir vor allem simple Automatisierung, echte KI wird noch nicht eingesetzt", sagt Jobst Landgrebe. Der Arzt und Mathematiker hat vor fünf Jahren in Köln Cognotekt gegründet, ein Unternehmen, das unter anderem auch Versicherungen dabei unterstützt, Künstliche Intelligenz zu implementieren.

Die Wiener TU-Professorin und Vorsitzende des österreichischen Robotik-Rats Sabine Köszegi sieht Künstliche Intelligenz in der Versicherungsbranche ebenfalls recht engen Einschränkungen unterworfen: „Sobald Sie keine Standardsituation haben, ist der Mensch unersetzbar. Eine Betriebsausfallversicherung ist zum Beispiel so individuell, dass eine persönliche Beratung absolut nötig ist, weil viel Kontextwissen erfragt und verarbeitet werden muss: der persönliche Hintergrund des Versicherten, Fakten zum Betrieb. KI-Systeme darauf zu trainieren wäre viel

zu aufwendig und es würde möglicherweise auch gar nicht funktionieren."

Daten, Daten, Daten

Und dann ist da noch die Sache mit den Daten. Um autonom Entscheidungen treffen zu können, müssen Computer zunächst mit Daten gefüttert werden, anhand derer sie lernen können, wann eine Position korrekt ist und wann nicht oder welche Konstellationen als risikobehaftet gelten und welche nicht. „Theoretisch kann man auch", sagt Sven Krüger, CEO beim Digitalisierungsanbieter Eucon, „anhand von Informationen zum Objektalter, seinem Zustand, der Schadenshäufigkeit und der Schadensart auch eine Prognose über die Schadenswahrscheinlichkeit machen, aber diese Daten hat schlichtweg niemand."

Sein Unternehmen beschäftige sich allerdings ohnehin primär mit der durchgängig digitalisierten Schadensregulierung. Und hier baue man vor allem darauf, dass Software die korrekten Fälle erkennt und so die Bearbeitungszeit erheblich beschleunigt. „Wir nutzen KI für das Schadenmanagement. So prognostizieren wir anhand der vorliegenden Daten, ob ein Schadensfall einfach ausgezahlt werden kann oder in die Detailbetrachtung muss."

Dass auf diesem Weg immense Zeiteinsparungen möglich sind, gilt als unumstritten. Schätzungen zufolge ist rund die Hälfte der bei Versicherungen eingereichten Versicherungsfälle sowohl sachlich als auch formal korrekt. Schaffen Unternehmen es, diese weitgehend automatisiert abzuwickeln, kommen Kunden schneller zu ihrem Geld und sind dementsprechend zufriedener.

Innovation kommt

Damit Versicherungsanbieter die Vorteile der Digitalisierung voll ausschöpfen, müssen sie allerdings noch einiges an Aufbauarbeit leisten. „Als man daran ging, die Archive zu digitalisieren, hat das vor allem darin bestanden, existierende Akten zu scannen und als PDF-Dateien zu speichern. Das erleichtert zwar die Arbeit, ist aber für ernsthaften Einsatz von Künstlicher Intelligenz völlig ungeeignet. Denn die so digitalisierten Daten liegen völlig unstrukturiert vor", erzählt der Mathematiker Landgrebe. Sie in eine strukturierte Form zu überführen, sei daher die nächste große Aufgabe, die auf die Branche zukommt. „Dann können wir von Digitalisierung reden. Bisher gab es vielfach eher etwas, das die Bezeichnung Fehldigitalisierung verdient."

Dass der Digitalisierungshebel nicht in dem Ausmaß genützt wird, in dem das möglich wäre, sieht Landgrebe aber auch als ein strukturelles Problem. „Nach der Marktkonsolidierung der 80er- und 90er-Jahre sind vor allem Anbieter am Markt geblieben, die erfolgreich EDV-Eigensysteme eingeführt haben. Diese Systeme haben nun aber Altlasten und man ist bei der Digitalisierung langsamer als andere Branchen."

Neue Impulse werden daher vor allem von außen, aus der Start-up-Welt kommen. Und hier ist inzwischen auch einiges in der Pipeline: Plattformen, die nicht nur beim Versicherungsabschluss helfen, sondern auch bei der Risikoeinschätzung. Portale, auf denen mehrere sicherheitsrelevante Dienste zusammengefasst werden und die aktives Risikomanagement durch Alerts betreiben, die bei entsprechender Bedrohung auf das Smartphone des Kunden kommen.

Noch sind solche Projekte klein und betreffen vor allem Individualkunden. In Zukunft könnte sich auch das ändern. Denn Beispiele von Technologien, die ursprünglich für den B2C-Bereich entwickelt und dann ins B2B-Geschäft transferiert wurden, gibt es in anderen Branchen mehr als genug.

INTERVIEW

„DER MENSCH BLEIBT UNERSETZBAR"

Foto: Zur Verfügung gestellt

Sabine Köszegi, Professorin an der TU Wien und Vorsitzende des österreichischen Robotik-Rates, über Versicherungen, Künstliche Intelligenz und die spezifischen Fähigkeiten des Menschen.

Zunächst einmal die unvermeidbare Frage an eine KI-Expertin: Wie sehr müssen wir uns davor fürchten, dass Roboter die Herrschaft über uns übernehmen?

SABINE KÖSZEGI: Wenn Sie die Frage so stellen, dann ist die Antwort absolut eindeutig: gar nicht. Das wird in der Zeitspanne unseres Lebens und wahrscheinlich auch in der Zeitspanne des Lebens unserer Kinder nicht passieren. Auch wenn wir in der Entwicklung von Künstlicher Intelligenz riesige Fortschritte gemacht haben, so sind lernfähige, autonome Systeme heute immer

noch auf ganz spezifische Fähigkeiten trainiert, in denen sie Menschen vielleicht sogar übertreffen können. Wir halten im Allgemeinen aber Menschen dann für intelligent, wenn sie neuartige Situationen und Problemstellungen verstehen und lösen können. Diese Form genereller Intelligenz ist derzeit für KI-Systeme noch undenkbar.

Für die Versicherungsbranche bedeutet das: Es macht nur Sinn jene Aufgaben zu automatisieren, die sehr häufig sind, denn da zahlt sich das Programmieren wenigstens aus?

KÖSZEGI: Ja, bei Standardfällen mit geringeren Schadenssummen, die häufig vorkommen und wo genügend Erfahrung und Daten aus der Vergangenheit vorliegen, an denen man ein KI-System trainieren kann, ist es vorstellbar, dass die Schadensabwicklung komplett automatisiert wird. Ein Beispiel wären Meldungen über Fahrraddiebstähle oder Glasschäden im Haushalt. Bei sehr individuellen Situationen und für komplexere Versicherungsprodukte wird es aber immer den menschlichen Sachbearbeiter brauchen, der berät, unterstützt und entscheidet. Denkbar ist allerdings, dass er in seiner Arbeit von künstlich intelligenten Systemen unterstützt wird, die Daten sammeln, analysieren und aufbereiten.

Und auf der Produktseite? Wird es je den digitalen Versicherungsberater geben?

KÖSZEGI: Bei simplen Anwendungen gibt es ihn schon heute. Nehmen Sie Reiseversicherungen, die man online abschließen kann, oder KFZ-Versicherungen, wo Sie online Parameter eingeben und das System dann ein entsprechendes Angebot zusammenstellt. Wenn der Verzicht auf den menschlichen Berater günstigere Prämien bedeutet, werden solche Angebote gern angenommen. Doch auch hier gilt: Sobald Sie keine Standardsituation haben, ist der Mensch unersetzbar.

Man erwartet auch, dass Maschinen beim Erkennen von Versicherungsbetrug effizienter sein könnten als Menschen, weil sie die dazugehörigen Muster zuverlässiger erkennen. Eine falsche Hoffnung?

KÖSZEGI: Solche Anwendungen sind grundsätzlich möglich. Die große Herausforderung dabei ist allerdings, dass die Qualität des Algorithmus, der die Betrugsmuster erkennen soll, von der Qualität und vom Umfang der Daten abhängt, die als Basis dienen, um den Algorithmus zu trainieren. Denn damit ein Computer Muster erkennen kann, müssen Sie ihm zunächst als Trainingsmaterial eine große Anzahl von Fällen aus der Vergangenheit vorlegen und kennzeichnen, welche davon Betrugsfälle waren und welche nicht. Wenn die Daten selbst falsch sind, weil die menschlichen Bearbeiter in der Vergangenheit Betrugsfälle nicht erkannt haben oder korrekte Angaben als Betrugsversuch klassifizierten, dann lernt das System diese Fehler mit. Vor allem aber: Sie brauchen wirklich große Datenmengen von guter Qualität, damit Sie einer KI das Erkennen von Muster beibringen können.

Sabine Köszegi: „Sobald Sie keine Standardsituation haben, ist der Mensch unersetzbar.

Sind die Erwartungen, die heute in die Künstliche Intelligenz gesetzt werden, am Ende also zu hoch gegriffen?

KÖSZEGI: Im Moment gibt es um Künstliche Intelligenz, Robotik und Digitalisierung einen unglaublichen Hype. Er wird auch medial davon befeuert, dass Ideen, die sich gerade einmal in der Entwicklungsstufe befinden, völlig unkritisch bereits als fertige und serientaugliche Lösungen dargestellt werden. Seit 2015 haben wir in der KI-Forschung zwar einige wichtige Durchbrüche erlebt, die auch medial sehr präsent sind, wie etwa Watson oder AlphaGo, aber für konkrete Anwendungen dieser Technologien in der Praxis ist oft noch ein deutlicher Entwicklungsbedarf gegeben.

Außerdem fehlen Robotern immer noch viele mechanische Fähigkeiten.

KÖSZEGI: Bei sogenannten „embodied" KI-Systemen, die also nicht rein digital sind, sondern in physischen Komponenten eingebettet sind, wird es tatsächlich noch einmal komplizierter. Und da geht es nicht nur um Mechanik und Sensorik wie beim nach wie vor schwierigen Problem des richtigen Greifens. Aktuell wird beispielsweise bei uns an der TU Wien daran geforscht, wie gemeinsame Aufmerksamkeit von Roboter und Mensch auf ein Objekt hergestellt werden kann. Menschen stellen gemeinsame Aufmerksamkeit ganz selbstverständlich her, indem sie zum Beispiel den Blick auf einen Gegenstand richten und auf ihn zeigen. Dass ein Roboter der Aufforderung nachkommen kann: „Bring mir diesen Becher dort!", ist alles andere als trivial und beginnt schon damit, dass Menschen Becher, Tasse oder vielleicht auch Häferl synonym verwenden, auch wenn es streng genommen unterschiedliche Gefäße sind. Auch die Bezeichnung „dort" wird vielleicht mit einer Geste verdeutlicht, die eine Maschine erst richtig interpretieren können muss.

Wofür KI am häufigsten eingesetzt wird

1 *Virtuelle persönliche Assistenten*
2 *Automatisierte Datenanalyse*
3 *Automatisierte E-Mail-Kommunikation*
4 *Automatisiertes Reporting*
5 *Automatisierte Effizienzanalyse*
6 *Predictive Maintenance*
7 *Direkte Unterstützung bei Entscheidungen*
8 *Robotik-Anwendungen*
9 *Automatisierte Verkaufsanalyse*
10 *Machine Learning*

FEUERWERK DER IDEEN

Unternehmenserfolg heißt: die besten Ideen haben, ihr Potenzial nutzen und dadurch Wettbewerbsvorteile erschließen. Innovationsmanagement lautet das Stichwort. Doch ohne Mut, passende Firmenkultur und Risikofreude können Innovationen nicht gedeihen.

Wer denkt, Innovationen sind gefährlich, sollte es mal mit Routine versuchen: Die ist tödlich“, schreibt Christian Müller-Roterberg in seinem neuen Management-Handbuch „Innovation“. Und tatsächlich kommt in der hart umkämpften Geschäftswelt heute der Qualität des Innovationsmanagements eine ganz besondere Schlüsselrolle zu. Von der Idee zum Markterfolg braucht es nicht nur Strategie, sondern auch Organisation. Dabei stellt sich schnell die Frage: Innovationsmanagement selber machen oder an externe Dienstleister vergeben?

Innovation mag keine Routine

Gleich vorweg: Wer sich überlegt, Innovation intern zu managen, muss die entsprechenden Rahmenbedingungen schaffen. „Dazu braucht es drei Elemente: Mitarbeiter dürfen sich mit Innovation beschäftigen. Sie müssen dazu befähigt sein. Und sie müssen es wollen“, sagt Michael Putz, Chef der auf Innovationsmanagement spezialisierten Lead Innovation.

Das bedeutet auch, dass sich die Tätigkeit als Innovationsmanager nur schwer mit einer anderen kombinieren lässt. Ein Mitarbeiter, der nebenbei noch andere Routineaufgaben in der Firma hat, wird schwer kreativ sein können. Denn bei der einen Tätigkeit gibt es sichere Wege, die zum Erfolg führen, bei der anderen – der kreativen – nicht. Ebenfalls wichtig im Vorfeld: Der interne Innovationsmanager braucht die Rückendeckung der Chefetage und muss direkt dem obersten Management unterstellt sein. Neuerungen bedeuten immer Veränderung und die stößt intern schnell auf Widerstand. Ist dieser Grundstein gelegt, dann spricht einiges dafür, internes Innovationsmanagement zu betreiben.

internes Innovationsmanagement

+ Erschaffung und Umsetzung von Innovationen ist zur Königsdiszplin geworden. Diese direkt im Haus zu haben, scheint für Unternehmen überlebenswichtig zu sein. Internes Innovationsmanagement bringt das Unternehmen auf Touren und sorgt nachhaltig für intrinsische Motivation, ohne dass es dafür ständige Anstöße von außen braucht.
+ Der interne Innovationsmanager kennt die Kollegen und weiß, wie das Unternehmen tickt. Widerstände gegen Neuerungen, die von einem Externen („der nicht weiß, wie der Laden hier läuft") kommen, fallen meist größer aus, als wenn sie von einem Kenner der Firma stammen.
+ Innovationsmanagement ist weit mehr als das bloße Finden und Unterstützen von Ideen; es geht immer auch um einen kulturellen und organisatorischen Wandel. Den möchte man von innen heraus steuern und kontrollieren.
+ Internes Management lässt dem Unternehmen auch die Zügel in der Hand, was die Auswahl und Vorbereitung der richtigen Mitarbeiter für eine Innovationsstrategie betrifft.
+ Ein hauseigner Mitarbeiter führt die Idee bis zur Marktreife. Die Beratung des Externen ende oft mit einem Konzept, dessen Umsetzung Sache des Unternehmens bleibt. Dort fühlt sich dann jedoch häufig keiner zuständig und die Innovation landet in der Schublade.

internes Innovationsmanagement

- Jeder Anfang ist schwierig: Unternehmen, die hinsichtlich neuer Ideen Aufholbedarf haben oder unter Zeit- und Erfolgsdruck stehen, brauchen voraussichtlich Starthilfe. „Wenn es große Innovations- und Technologiesprünge geben soll, macht externes Innovationsmanagement Sinn", sagt Michael Putz von Lead Innovation.
- Wer das Unternehmen gut kennt, hat meistens auch schon einen gewissen Tunnelblick. Dabei werden Entwicklungen aus anderen Wirtschaftsbereichen, die das eigene Problem vielleicht lösen könnten, schnell übersehen. Der Blick über den Tellerrand fällt einem externen Innovationsmanager leichter, weil er meist für unterschiedliche Branchen tätig ist.
- Angst vor dem Scheitern ist ein Hemmnis. „Je radikaler die Innovation, desto größer die Erfolgspotenziale und desto größer auch die damit einhergehenden Risiken", erläutert WU-Professor Nikolaus Franke, Leiter des Instituts für Entrepreneurship und Innovation. Wenn die Bereitschaft, sich auf ein Wagnis einzulassen, im Unternehmen gering ist, kann externes Management der richtige Wege sein.
- Externes Management kostet spürbar Geld. Das kann als Treiber für die rasche Umsetzung eines Projekts hilfreich sein.
- Die Belegschaft akzeptiert einen Außenstehenden oft schneller als Innovationsexperten als einen Kollegen, der bisher vielleicht eine ganz andere Tätigkeit hatte.

Sinn kann es aber auch machen, internes und externes Innovationsmanagement zu kombinieren. Etwa indem man die Nähe zu Start-ups sucht und deren Innovationskraft nutzt. „Start-ups sind wie Schnellboote. Etablierte Unternehmen sind im Vergleich eher Tankschiffe, ihr natürlicher Vorteil sind die Ressourcen und ihre Stabilität", sagt Nikolaus Franke. Eine Kombination von beidem wäre daher vorteilhaft. Ob Kooperation mit jungen Unternehmen oder andere Formen der Anbindung – lernen können etablierte Firmen von ihnen auf jeden Fall. Das frische Herangehen an Märkte, der unverkrampfte Zugang zu radikalen Ideen, das Fehlen erstickender Bürokratie sind Eigenschaften, die sich so manche Firmenchefs wünschen würden.

Fotos: Fotolia

INTERVIEW

„ECHTE UNTER-NEHMER TREIBEN INNO-VATION VORAN“

Lucanus Polagnoli ist Partner bei Speedinvest, einem Finanzierer von Start-ups. Im Interview spricht er über Start-ups als Vorbild und welche Mentalität entscheidend ist.

Hinter dem Begriff Innovation kann vieles stecken – was bedeutet er für Sie?

LUCANUS POLAGNOLI: Im Venture Capital suchen wir nach Innovationen, die disruptiv und game-changing sind. Oft geht es aber um ganz traditionelle Bereiche, die völlig neu gedacht werden.

Haben Sie ein Beispiel?

POLAGNOLI: Als Beispiel kann AirBnB genannt werden: In einer fremden Stadt ein Zimmer anzumieten ist wenig innovativ – es geht vielmehr um eine völlig neue Art und Weise, wie durch digitale Innovation neue Angebote für diese immer schon bestehende Nachfrage zustande kommen.

Innovation wird oft mit Start-ups in Verbindung gebracht. Wie funktioniert Innovation aber in etablierten Unternehmen?

POLAGNOLI: Ich glaube, dass große Unternehmen einen hohen Innovationsgrad erreichen können. Wenn Unternehmen von Start-ups lernen wollen, dann sehe ich die besten Lösungen meist in Partnerschaften. Da lernen beide Seiten voneinander. Weniger häufig funktioniert ein Einkauf von Innovation durch eine Übernahme von Start-ups. Hier sehen wir eher Erfolge auf Eigentümer-Ebene, wenn der Unternehmer direkt oder indirekt etwa über einen Fonds in Start-ups investiert. Da gibt es eine hohe Lernkurve, ohne dass die unterschiedlichen Ziele von traditionellen Unternehmen und Start-ups unter einen Hut gebracht werden müssen.

Nikolaus Franke: „Wenn ein Anfänger sagt, dass er Skifahren lernen, aber niemals in den Schnee fallen will, dann wird er nie vom Idiotenhügel runterkommen. So ist das auch mit Innovationen“

Ist eine Start-up-Mentalität erforderlich, um Innovation voranzutreiben?

POLAGNOLI: Aus meiner Sicht sind Start-ups dann besonders erfolgreich, wenn sie sich voll und ganz darauf konzentrieren, ein Problem zu lösen und damit auf den Nutzen des Kunden fokussieren – auch wenn dies ein hohes Risiko mit sich bringt. Gepaart mit agilem Projektmanagement bedeutet das für mich nichts anderes als Unternehmertum – und echte Unternehmer sind immer schon diejenigen gewesen, die Innovation vorantreiben.

Was bedeutet Start-up-Mentalität?

POLAGNOLI: Auch wenn das für viele seltsam klingen mag, aber aus meiner Sicht ist die Start-up-Mentalität einfach eine Unternehmer-Mentalität. Vielleicht ist diese manchen älteren, etablierten Unternehmen verloren gegangen.

Falsch gedacht

Beispiele für Innovationen, die in der Vergangenheit falsch eingeschätzt wurden:

- *Das Internet wird kein Massenmedium – weil es in seiner Seele keines ist. (Matthias Horx, 2001)*
- *Solange die Menschen Mobiltelefone kaufen, auf denen Nokia steht, werden wir nichts an unserer Strategie ändern. (Nokia-Top-Manager, als 2007 das erste iPhone auf den Markt kam)*
- *Das Auto ist fertig entwickelt. Was kann noch kommen? (Karl Benz, um 1920)*

Event

electronica 2018
Komponenten | Systeme | Anwendungen | Lösungen
Weltleitmesse und Konferenz der Elektronik
Messe München | 13.–16. November 2018 | electronica.de

Sicherheit ist das wichtigste Leistungsmerkmal von elektronischen Systemen und Produkten. Im Rahmen der Electronica in München vom 13. bis 16. November 2018 findet das Cyber Security Forum statt. Fachleute aus den Bereichen Software und Halbleiter sowie Test- und Messgeräte präsentieren ihre Lösungen und Ideen dazu. Ein zentrales Thema des Cyber Security Forums ist die Embedded-Sicherheit. Experten erläutern skalierbare und sichere Lösungen für unterschiedlichste Produkte und Systeme. Dabei thematisieren sie auch die sichere Kommunikation zwischen Home-Gateways und Servern.

Warnung per App

KATWARN Österreich/Austria ist eine Service-App des Innenministeriums zur Übermittlung von Gefahren- und Katastrophenwarnungen innerhalb Österreichs. Die App gewährleistet ortsbasierte Benachrichtigungen über Gefahrenmeldungen wie Großbrände oder Extremwetter und bietet dabei die Möglichkeit, sich immer für den aktuellen Standort und zusätzlich für sieben weitere, frei wählbare Orte informieren zu lassen. Diese Auswahl kann jederzeit aufgehoben, angepasst und bei Bedarf ausgeschaltet werden. Durch Verwendung der energieeffizienten Ortung über Basisstationen und WLAN-Zugangspunkte (und nicht über GPS) wird der Akku nur geringfügig belastet.

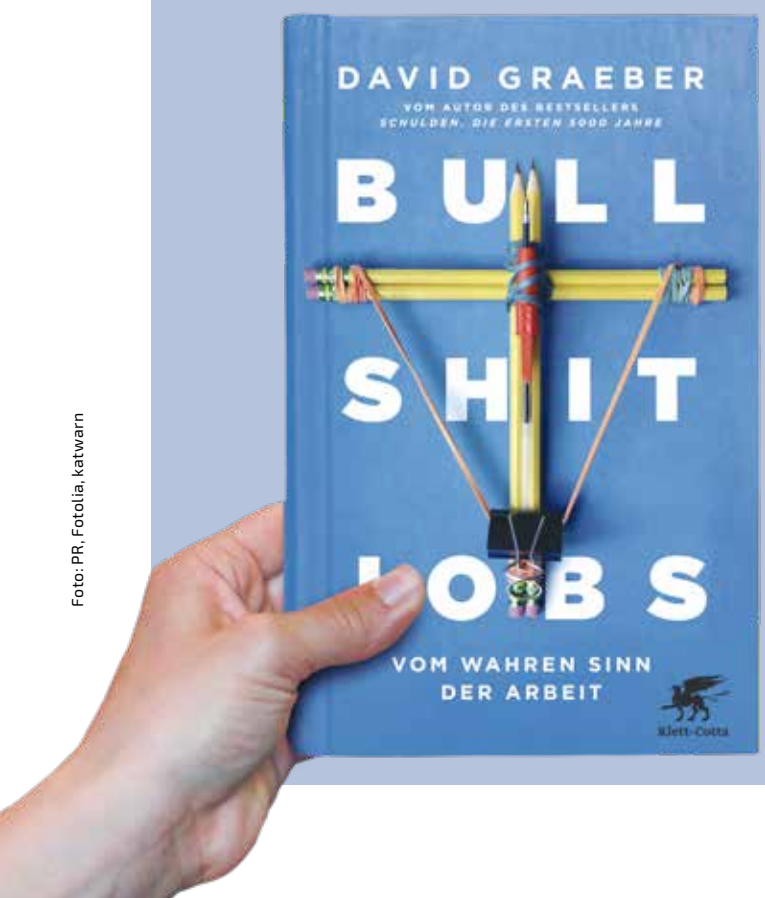


Foto: PR, Fotolia, katwarn

Buchtipp

Millionen Menschen sind in Bullshit-Jobs gefangen. Zu diesem Schluss kommt David Graeber, Anthropologe und Vordenker der Occupy-Bewegung, in seinem neuen Buch mit dem gleichnamigen Titel „Bullshit Jobs". Gemeint sind Jobs, die zwar gut bezahlt sind, aber keinen gesellschaftlichen Mehrwert bieten. Kritiker sagen: Statt methodisch sauberer Analyse präsentiert Graeber intellektuellen Populismus und lässt dabei zentrale Fragen ungeklärt.

David Graeber: Bullshit Jobs, a Theory (aus dem Englischen von Sebastian Vogel), Klett Cotta Verlag, 2018, 464 Seiten, ISBN: 978-3-608-98108-7, 26 Euro

IM VISIER DER CYBER-KRIMINELLEN

Zwei von drei österreichischen Unternehmen sind im vergangenen Jahr Opfer eines Cyberangriffs geworden. Vielen von ihnen fehlt das Risikobewusstsein dafür, wie leicht man Ziel einer Attacke werden kann. Dabei steht viel auf dem Spiel: neben Kapital vor allem das gute Image.

30 Prozent. Das ist der Wert um den kriminelle Machenschaften aus dem Internet laut aktueller Statistik des Bundeskriminalamts (BK) österreichweit binnen eines Jahres gestiegen sind. Kein Deliktsbereich hat ähnliche Wachstumsraten. Die Opfer sind häufig Unternehmen. Was sich bei näherer Analyse zeigt: Vor allem (kleinere und mittelständische) Betriebe wissen um ihr Risikopotenzial kaum Bescheid.

Das Thema ist längst kein länderspezifisches: Die Fälle von Cybercrime steigen weltweit. Dabei werden die Angriffsszenarien technisch immer raffinierter, wie das BK in seinem Jahresbericht zur Internetkriminalität meldet. Die Arbeit für die Strafverfolger wird dadurch immer schwieriger.

Heimische Unternehmen im Visier

Die Zahlen sprechen für sich: Fast zwei Drittel (61 Prozent) der heimischen Unternehmen gerieten laut einer Studie der Unternehmensberatung KPMG im Jahr 2017 ins Visier von Cyberkriminellen. Im Jahr davor waren es sogar 72 Prozent. PricewaterhouseCoopers (PwC) hat erhoben, dass Cyberkriminalität im Bereich der Wirtschaftskriminalität an zweiter Stelle hinter Unterschlagung liegt – mit dem Potenzial Rang eins zu erobern, denn das Risiko wächst weiter.

Besonders der Tatbestand der Datenbeschädigung wurde 2017 laut Polizeistatistik häufig angezeigt, hier gab es eine Steigerung der Anzeigen um 80 Prozent. Die Kriminalisten sehen die Ursache dafür in der weltweit zunehmenden Verbreitung von Ransomware. Damit werden Daten im IT-System durch einen Trojaner unbrauchbar gemacht. Die Täter versuchen dann für die Entschlüsselung Lösegeld in Form von Bitcoins zu erpressen.

Auch was die zukünftigen Trends angeht, bleibt Ransomware ganz oben auf der Liste der Kriminalitätsbekämpfer. „Hier ist eine zunehmende Spezialisierung auf bestimmte Ziele und Zielgruppen wie Personalabteilungen, Klein- und Mittelbetriebe usw. feststellbar“, heißt es im Bericht des Bundeskriminalamts. Kriminelle würden virtuelle Zahlungsmittel wie Bitcoins immer häufiger dazu verwenden, kriminelle Geldflüsse und Gewinne vor den Ermittlungsbehörden zu verschleiern. Das Darknet habe hier die Entstehung krimineller Dienstleister begünstigt und beschleunigt.

Hohe Dunkelziffer

Als wäre die Zahl der bekannten Fälle nicht ohnehin schon groß, wird dennoch von einer hohen Dunkelziffer ausgegangen. Laut KPMG-Studie erstatten nur rund ein Drittel (31 Prozent) der Betroffenen Anzeige. Zu groß ist die Angst vor einem vermuteten Reputationsverlust.

Ein Umstand, den auch Rene Forsthuber, Leiter International Development bei Risk Experts, bestätigen kann. „Imageverlust ist der gefürchtetste Schaden von Unternehmen, besonders in Folge eines Verlusts von Kundendaten. Denn sind die Daten weg, muss ich in vielen Fällen den Kunden darüber informieren. Und das vermittelt, dass man nicht gut genug auf seine Daten aufgepasst hat, nachlässig war, sich zu wenig gekümmert hat“, sagt er. Mit dem Imageschaden geht ein Vertrauensverlust einher. Je größer das Unternehmen, umso relevanter wird das. „Aufwände von hunderttausend Euro sind da schnell beisammen, wir kennen aber auch Fälle mit Schäden in Millionenhöhe“, sagt er.

Neben dem Imageschaden sind auch Angriffe gefürchtet, die eine Betriebsunterbrechung hervorrufen. Gerade in der automatisierten Produktion ist mit einem sehr hohen Profitentgang zu rechnen, wenn der Betrieb tagelang stillsteht.

Risikoeinschätzung mangelhaft

Was aber weit mehr ins Auge sticht: Fast die Hälfte der von PwC Befragten weltweit gab an, dass ihr Unternehmen keine Risikoeinschätzung im Bereich der Wirtschaftskriminalität durchgeführt hat. Zu den am häufigsten betroffenen Branchen von Wirtschaftskriminalität allgemein zählen Versicherungswesen (62 Prozent), Agrarindustrie (59 Prozent), Kommunikationsbranche (59 Prozent), Finanzdienstleistungen (58 Prozent), Einzelhandel und Konsumgüter (56 Prozent) sowie Immobilienbranche (56 Prozent). Mehr als zwei Drittel der Cyberangriffe werden durch Phishing (33 Prozent) und Schadsoftware (36 Prozent) verursacht.

Besonders Ransomware macht kaum vor jemandem Halt. Bevorzugt bedroht sind kleine und mittlere Unternehmen (KMU). 2016 rangierten unter den Opfern an vorderster Stelle Autohäuser, öffentliche und gemeinnützige Betriebe, Getränkehändler, Notare und Rechtsanwälte.

Doch warum blenden Unternehmen das Thema trotz steigender Fallzahlen immer noch aus? „In Österreich gab es den Super-Gau noch nicht und viele Angriffe gehen gerade noch glimpflich aus“, analysiert Forsthuber. „Doch niemand weiß, wann der Angriffs-Fall passiert oder ob man nicht schon längst Opfer ist. Denn es gibt kriminelle Energien, die sich schon lange vorher in das IT-System einschleichen und monatelang ihr Ziel ausspähen. Wer überweist die großen Geldbeträge? Wie sind die Abläufe im Unternehmen? All das wird ausgeforscht. Die Kriminellen warten auf den passenden Moment, während der Unternehmer gar nicht weiß, dass er schon betroffen ist.“

Krisenmanagement für den Ernstfall

Das, was Versicherungen für diese Fälle bieten, sind Cyberversicherungen, welche neben der Abdeckung von Eigen- und Drittschäden auch

Foto: Unsplash

Cybercrime – was ist das?

Der Begriff Cybercrime ist recht umfassend. Eine allgemein gültige Definition gibt es nicht. Er beschreibt Straftaten, die „unter Ausnutzung der Informations- und Kommunikationstechnik (IKT) oder gegen diese begangen werden". Im polizeilichen Bereich wird zwischen Cybercrime im engeren und Cybercrime im weiteren Sinn unterschieden. Im engeren Sinn werden Straftaten umfasst, bei denen Angriffe auf Daten oder Computersysteme (Datenbeschädigung, Hacking, DDoS-Attacken) begangen werden. Im weiteren Sinn meint Delikte, wo die IKT zur Planung, Vorbereitung und Ausführung für herkömmliche Kriminaldelikte eingesetzt wird (Betrug, Kinderpornografie, Cybermobbing).

eine Krisenmanagement Komponente beinhalten. Diese besteht je nach Produkt aus Forensik, Rechtsbeistand, IT-Securityfirmen und PR-Agenturen, die sich etwa um den Imageschaden kümmern. „Da gibt es für jeden Gewerbetreibenden bis zum großen Konzern mittlerweile gute Produkte auf dem Markt", so Forsthuber. Entscheidend sei jedoch, das für sich Passende zu finden. „So einfach wie mit einer Kfz-Versicherung ist es leider nicht."

Das, was diese Versicherungen dabei für sich beanspruchen, ist, die Situation für den Versicherungsnehmer nach dem Schadensfall wieder so herzustellen, als ob der Schaden gar nie eingetreten wäre. „Außerdem haben viele Versicherungen Assistance-Dienstleistungen. Das heißt ab dem Moment, wo der Bildschirm schwarz wird und Erpressungshinweise auftauchen, kann man sich gleich telefonisch an die Versicherungshotline wenden und sich erste Tipps geben lassen bis hin zur Unterstützung durch Fernwartung oder Kontakt vor Ort", so Forsthuber. Zu seinem Job gehört es, Unternehmen dahingehend zu analysieren, wie sie in Bezug auf Bedrohungen aus dem Netz aufgestellt sind. „Wenn wir in unseren Risikoanalysen Schwachstellen entdecken, dann können wir beraten, wie man sich richtig schützen kann." Und dahingehend kommt in den nächsten Jahren noch einiges auf Geschäftstreibende – aber auch Private zu.

Immer mehr Geräte online

Experten zufolge wird das „Internt der Dinge" in diesem Zusammenhang von besonderer Bedeutung sein. Denn Prognosen sagen, dass bis 2020 rund 20 Milliarden Geräte mit dem Internet verbunden sein werden. Die meisten davon ungeschützt.

Ein prominentes Beispiel dafür, welches Gefahrenpotenzial durch das IoT (Internet of Things) lauert, ist die DDoS-Attacke im Herbst 2016 mit dem „Mirai-Botnet" auf das US-Unternehmen „DynDNS".

Zur Erinnerung: 2016 gab es mehrere Angriffswellen auf die Server von Dyn. Es handelte sich um sogenannte „Distributed-Denial-of-Service"-Angriffe (DDoS). Dabei werden so viele gleichzeitige Anfragen von vielen verschiedenen Geräten auf einen oder mehrere Server geschickt, bis diese schlicht überlastet sind. Interessant war in der anschließenden Analyse, woher die IP-Adressen kamen. Teilweise nämlich waren es vernetzte Haushaltsgeräte, also aus dem sogenannten Internet of Things (IoT): Kühlschränke, Thermostate etc., die womöglich dazu geführt haben, dass Nutzer in den USA Netflix oder Spotify nicht mehr erreichen konnten.

Glossar

BotNet
oder auch Roboter-Netzwerk genannt, meint einen Verbund von fernsteuerbaren Computersystemen, auf die sich widerrechtlich Zugang verschafft wurde. Die Kontrolle über die Systeme wird durch Würmer oder Trojanische Pferde erlangt, die auf Anweisungen des kontrollierenden Servers warten.

Phishing
ist eine Form des Trickbetrugs im Internet. Die Täter versuchen per E-Mail den Empfänger zur Herausgabe von Zugangsdaten und Passwörtern zu bewegen. Meistens in Bezug auf Online-Banking oder andere Bezahlsysteme.

DDoS-Attacke
ist ein Angriff auf die Verfügbarkeit der Ressourcen und Dienste eines IT-Systems mit dem Ziel, diese zu blockieren und regulären Benutzern keinen Zugriff mehr zu ermöglichen. Oft wird der Angriff von vielen Rechnern gleichzeitig aus durchgeführt.

Ransomware
bezeichnet „bösartige" Software, die zur Erpressung genutzt wird, indem sie die Funktionalität des Systems des Opfers einschränkt und eine Geldzahlung fordert, um diese Einschränkung wieder aufzuheben.

PREMIERE

Risk Experts am asscompact-Trendtag

Mit 70 Ausstellern und 3000 Besuchern ist der asscompact-Trendtag der Branchentreff für die Versicherungs- und Finanzbranche. Heuer ist Risk Experts erstmals als Aussteller am 18. Oktober in der Pyramide Vösendorf vor Ort. Zu finden sind die Risk Experts mit einem Stand in der Futurzone im Zentrum der Ausstellung - gemäß ihrem Motto: „Two Steps ahead". Der Trendtag findet bereits zum 12. Mal statt.

Fachvorträge **Two Steps ahead**

Aufgrund der großen Nachfrage wird Risk Experts seine kostenlose Fachvortragsreihe für Versicherer, die vergangenen Herbst gestartet wurde, weiter fortsetzen. Frei nach der Risk Experts-Vision „Two Steps ahead" werden die Chancen und Risiken von Themen behandelt, die für die Zukunft eine wichtige Rolle spielen. Sobald die Termine und Themen für die kommenden Fachvorträge feststehen, finden Sie die aktuellen Informationen auf der Risk Experts-Homepage. Ein regelmäßiger Besuch auf **www.riskexperts.at** ist deshalb immer empfehlenswert.

Fotos: AssCompact GmbH | Unsplash

EINBRUCHSCHUTZ EINST & JETZT

Ca. 600 bis 1500 n. Chr.
Im Mittelalter dienen Fenstergitter, Verriegelungen und mechanische Klingeln dazu, das eigene Heim zu schützen. Daneben sorgt das aufgeregte Geschnatter von Gänsen oder das Bellen des Wachhundes dafür, ungebetene Gäste zu vertreiben.

1853
lässt der Tüftler Augustus Russell Pope die erste elektro-magnetische Alarmanlage patentieren. Sie reagiert auf das Schließen eines Stromkreislaufes: Türen und Fenster sind mittels Parallelschaltung verbunden. Wird eines von beiden geöffnet und so der Stromkreislauf geschlossen, versetzt der Stromfluss einen Magneten in Vibration. Diese Schwingungen werden auf einen Hammer übertragen, der eine Messingglocke anschlägt.

1857
kauft Edwin Holmes die Rechte an Popes Erfindung. Der Geschäftsmann gilt als kluger Stratege und setzt für die Verbreitung seines Einbruchsalarmtelegrafen klassische Werbemittel ein. Bald gehören berühmte Schmuckgeschäfte wie Tiffany oder Lord & Taylor zu seinen Kunden.

1860
Ein Alarmsystem, das Hilfe holen kann: Edward A. Calahan setzt einen weiteren Meilenstein in der Geschichte moderner Alarmanlagen. Er teilt New York in einzelne Distrikte auf, die jeweils mit einer zentralen Notrufstelle verbunden sind. Die Notrufkästen vom Typ Calahan werden schnell zum Standard im Polizei- und Feuerschutz, aber auch Nachrichtendienste nutzten sie.

1970
Werden die ersten Bewegungsmelder in Alarmsysteme integriert.

1980er-, 1990er-Jahre
Alarmanlagen gehören zunehmend zum Standard in der Gebäudesicherung. Die ersten Funkalarmanlagen kommen auf den Markt.

Heute
können selbst unübersichtliche Grundstücke durch den Einsatz von modernen Bewegungsmeldern, elektronischen Detektoren und hochauflösender Videoüberwachungstechnik fast lückenlos abgesichert werden. Laut Österreichischer Datenschutzbehörde (DSB) müssen private Videoüberwachungsgeräte dieser gemeldet werden, weil Daten identifizierbarer Personen verarbeitet werden.

Foto: Unsplash

NEU – INDIVIDUELLE SCHULUNGSANGEBOTE FÜR INDUSTRIE UND GEWERBE

Fokussierte Weiterbildung für Unternehmen aus Industrie, Handel und Gewerbe

THEMENAUSZÜGE

SACH- UND BETRIEBSHAFTPFLICHTVERSICHERUNG – KOMPAKTES BASISWISSEN FÜR VERSICHERUNGSVERANTWORTLICHE IN UNTERNEHMEN

Versicherungsbeauftragten und –verantwortlichen in Unternehmen soll im Rahmen des Seminars ein praxistaugliches Basiswissen zu den Grundzügen der Sach- und Haftpflichtversicherung vermittelt werden, um Deckungskonzepte und deren Kosten plausibilisieren zu können, aber auch Klarheit über Rechte und Pflichten, die mit Versicherungsverträgen verbunden sind, zu gewinnen.

FEUERRISIKEN UND BETRIEBSGEFAHREN

Kern des Seminars bildet ein Experimentalvortrag zur praktischen Veranschaulichung von Brandgefahren. Zusätzlich können Sie nach Bedarf und Interesse aus folgenden Themenmodulen auswählen:

- Feuerrisiken und Betriebsgefahren
- Brandrauch und seine gefährlichen Bestandteile
- Feuer, Explosion und andere Katastrophen, nicht nur der Flash-Over ist gefährlich
- Risikomanagement – Traditionelle Schutzkonzepte auf dem Prüfstein
- Business Continuity Planning – Wenn nichts mehr geht, Grundlagen und Praxisworkshop
- Gefahrenquelle Öl im Betrieb
- Dämmstoffe zur Gebäudeisolierung, Brandgefahren und Feuerrisiken durch Wärmedämmung
- Lithium-Batterien – Brandgefahren und Sicherheitsrisiken bei Lagerung, Produktion und Transport

UNTERWEISUNGEN UND INFORMATION

Mit unserem breiten Erfahrungsspektrum erstellen wir an die Arbeitssituation Ihrer Dienstnehmer angepasste Unterweisungen, die sowohl theoretische als auch praktische Aspekte umfassen – auf Wunsch auch mit Abschlussprüfung. Neben einer Teilnahmebestätigung erhalten die Teilnehmer eine übersichtliche Zusammenfassung und Merkblätter. Gerne halten wir erforderliche Wiederholungen von Unterweisungen für Sie in Evidenz.

- Umgang mit brennbaren Arbeitsstoffen – VbF
- Umgang mit Zündquellen, Raucherregelung
- Umgang mit Abfällen
- Verhalten im Brandfall (Rettungskette, Löschmittel)
- Maschinensicherheit – CE-Konformitätserklärungen

Zur Beratung und Gestaltung Ihrer maßgeschneiderten Schulungen kontaktieren Sie:

Heidi Brukner unter
academy@riskexperts.at.
Wir beraten Sie gerne!

Factbox

Das Angebot der **Risk Experts Academy** umfasst Vorträge, Grundlagenlehrgänge, Spezialisten-Ausbildungen und Expertentrainings mit Workshops, Fallstudien und Exkursionen. Die Inhalte kombinieren Themen aus dem Bereich Schadenverhütung und Risikomanagement und können auf die Bedürfnisse und Vorkenntnisse der Teilnehmer zugeschnitten und als Vortrag, Fachseminar oder als komplettes Ausbildungsprogramm gestaltet werden.

RISK EXPERTS

UNSERE KOMPETENZ FÜR IHREN ERFOLG

- Risikoanalyse und Risikobewertung
- Risiko- und Sicherheitsberatung
- Sachverständigenleistungen
- Schadenmanagement
- Wertermittlung
- Enterprise Risk Management
- Risk Experts Academy
- Expertensoftware

Risk Experts Risiko Engineering GmbH
Schottenring 35/2, 1010 Wien, office@riskexperts.at, +43 1 713 50 96, www.riskexperts.at

Geschäftsführer/Management:
DI Gerhart Ebner, Ing. Mag. Gerald Netal

WIEN KUFSTEIN BRATISLAVA WARSCHAU BUKAREST SOFIA ISTANBUL

24-STUNDEN-EMERGENCY-HOTLINE:
+43 676 88 626 676