Digitalisierung, Cyberrisk & KI: Wandel gestalten

Fakten & Meinungen zur
DAV/DGVFM-Jahrestagung 2019

DAV
DEUTSCHE
AKTUARVEREINIGUNG e.V.

DGVFM
DEUTSCHE GESELLSCHAFT
FÜR VERSICHERUNGS- UND
FINANZMATHEMATIK e.V.

INHALT

IMPRESSUM

Herausgeber:
Deutsche Aktuarvereinigung e.V.
Hohenstaufenring 47–51
D-50674 Köln
Telefon 0221/912554-231
Telefax 0221/912554-9231
presse@aktuar.de - www.aktuar.de

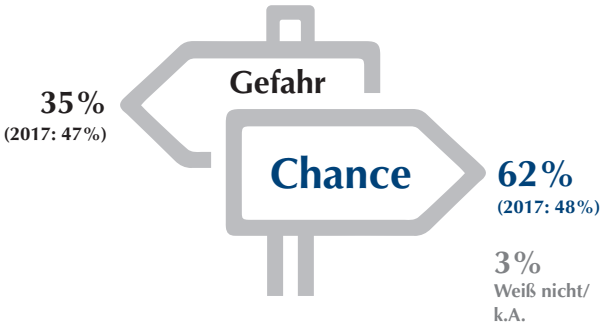
Redaktion:
Birgit Kaiser (verantwortlich)
Erik Staschöfsky

Foto:
S. 11: Marlene Bleicher; Büro Schipanski; Kerstin Bänsch, PHOTOdesign

April 2019

Sehen Sie Künstliche Intelligenz als Chance oder Risiko?

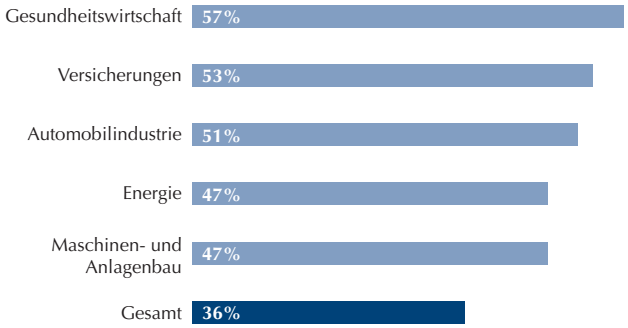
Repräsentative Befragung der Bundesbürger



Basis: Alle Befragten (2018: n=1.007 | 2017: n=1.006) |
Quelle: Bitkom Research 2018

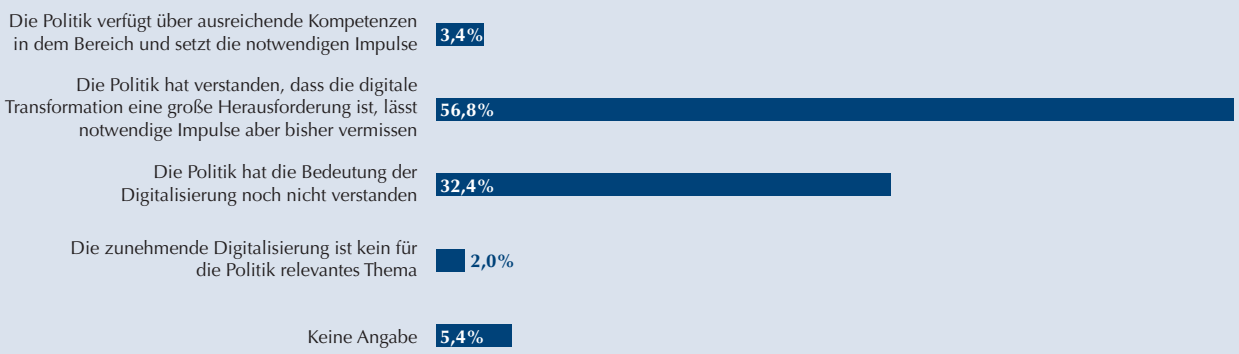
Einsatz von Big-Data-Lösungen in verschiedenen Branchen

2017



Quelle: KPMG / Bitkom Research 2017 | Studie „Mit Daten Werte Schaffen“

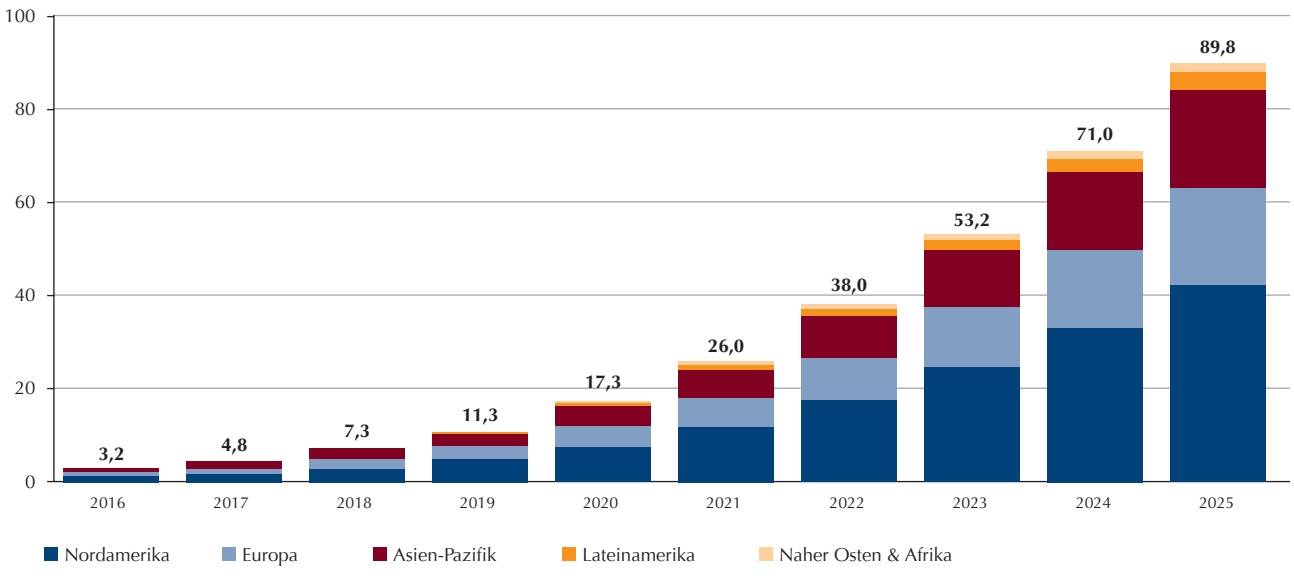
Deutsche Wirtschaftselite sieht Politik nicht für digitale Transformation gerüstet



Quelle: Roland Berger und WELT-Gruppe, www.leaders-parliament.com | 2015

Prognostizierter weltweiter Umsatz mit Künstlicher Intelligenz

Angaben in Milliarden Dollar



Quelle: Tractica

Im Gespräch mit Dr. Andreas Weigend

„Wir müssen den digitalen Analphabetismus überwinden!“

INTERVIEW

Daten sind das Öl des 21. Jahrhunderts. Das spiegelt sich nicht nur in den Börsen-Notierungen der Unternehmen wider, sondern auch im Machtgefüge der Volkswirtschaften. Große Industrienationen wie Deutschland droht der schleichende Abstieg. Um dieser Entwicklung entgegenzuwirken, braucht es nach Überzeugung von Digitalexperte Dr. Andreas Weigend dringend tief greifende Reformen, ein ganz neues Mindset hinsichtlich der Chancen der Digitalisierung und neue Strukturen in der Bundesregierung. Ohne diese Änderungen hat das Mitglied des Digitalrats der Bundesregierung wenig Hoffnung für die Zukunft der deutschen Digitalwirtschaft. Skeptisch beurteilt der ehemalige Chef-Wissenschaftler von Amazon die Pläne für eine nationale oder internationale Digitalsteuer. Sinnvoller sind nach seiner Überzeugung „synthetische Daten“: Die Digitalunternehmen, wie Facebook und Google, sollten einen Teil ihrer Daten so gut wie möglich anonymisiert in einen großen Datenpool geben, auf den auch Wettbewerber zugreifen könnten. Davon könnten die europäische Wirtschaft und vor allem die Start-up-Szene stärker profitieren als von Steuern.

Herr Dr. Weigend, ein Blick auf Ihre Webseite verrät einem sehr gut, wo Sie gerade sind, mit welchem Flieger Sie aktuell unterwegs sind oder wo Sie aktuell Vorträge halten. Das ist eine große Offenheit mit eigentlich sehr persönlichen Daten. Ist das direkt Ihr Statement zu Ihrer These, dass es Privatsphäre gar nicht mehr gibt?

Genauso ist es. Für mich ist es eine Frage der Geisteshaltung: Entweder wir geben uns der Illusion hin, dass es noch so etwas wie Privatsphäre gibt, oder wir erkennen die Realität an und hinterfragen, wie wir aus diesen Gegebenheiten für uns selbst die größten Vorteile ziehen können. Dabei geht es für mich aber nicht nur um finanzielle Aspekte. Sondern ich frage mich vielmehr, wie wir die Datenraffinerien nutzen können, um für uns bessere Entscheidungen zu treffen.

Nichtsdestotrotz sprechen Sie in Ihrem Buch „Data for the People“ davon, dass Daten einen konkreten Wert haben. Wie bemisst sich dieser?

Lassen Sie mich zunächst etwas philosophisch werden: Im Deutschen gibt es den wunderbaren Ausdruck „etwas preisgeben“. Dafür kennt die englische Sprache leider kein Pendant. Aber diese Redewendung trifft den Kern der digitalen Welt. Denn im Internet geben wir den Datenraffinerien unsere Informationen und dafür sollte ein Preis festgelegt werden. Und der Wert unserer Daten bemisst sich nach meiner Überzeugung daran, welchen Einfluss unsere Daten auf Entscheidungen haben.

Die europäischen Staaten wollen die Bigtechs stärker zur Kasse bitten. Frankreich hat Anfang März angekündigt, notfalls im Alleingang eine Digitalsteuer einzuführen. Wie bewerten Sie das?

Ich halte das für den falschen Weg. Ich denke nicht, dass wir die großen Firmen zu einer finanziellen Steuer verpflichten sollten. Viel sinnvoller wäre es, wenn die Datenraffinerien unter Beachtung der EU-Datenschutzgrundverordnung einen Teil ihrer Daten in einen großen Datenpool geben müssen, auf den dann auch Wettbewerber zugreifen können. Davon würden die europäische Wirtschaft und vor allem die Start-up-Szene viel stärker profitieren als von Steuern. Denn das größte Hemmnis für Unternehmen, bspw. bei der Entwicklung guter Künstlicher Intelligenz (KI), ist das Fehlen von entsprechenden Datenmengen.

Und die Daten liegen bei den Digitalunternehmen. Einst waren Versicherungen die marktbeherrschenden Datenfirmen, doch sie haben diesen Vorsprung im digitalen Zeitalter verloren. Heute ist Google der alles beherrschende Player und jeder weiß: Gegen diesen Giganten hat niemand eine Chance. Wenn Google sich überlegt, eine Versicherung zu gründen, dann werden alle Konkurrenten das Nachsehen haben. Denn selbst Versicherungen wissen im Vergleich zu Google fast gar nichts.

Sie sprachen gerade das Thema KI an, mit dem viele Bürger auch ethische Fragen verbinden. Was entgegnen Sie denen, die Angst vor einer maschinenbestimmten Zukunft haben, in der primär Algorithmen die Entscheidungen treffen?

Das ist eine nicht unberechtigte Angst. Deshalb braucht es eine strenge Aufsicht, deren Ziel es ist, zu verhindern, dass Daten gegen uns verwendet werden können. Genauso wie

es Wirtschaftsprüfer gibt, die die Bücher der Unternehmen prüfen, braucht es im Digitalzeitalter unabhängige Prüfer für die genutzten Algorithmen. Hier sehe ich noch entsprechendes Entwicklungspotenzial. Darüber hinaus sehe ich großen Bedarf für eine umfassende Studie über die wirklichen Datenängste der Bürger. Sie haben gerade eine Angst beschrieben. Aber welche Ängste gibt es daneben noch? Meine persönlich größte Angst ist, dass jemand auf Grundlage (falscher) Daten über mich meine persönlichen Freiheiten beschneidet.

Lassen Sie uns zu Ihrer Arbeit im Digitalrat der Bundesregierung kommen. Deutschland hat einen Topruf als Industrienation. Die Digitalisierung scheint man hierzulande aber vielfach verschlafen zu haben. Was muss passieren, dass in Deutschland oder zumindest in Europa ein Global Player für den Digitalmarkt erwächst?

Zu Beginn meiner Arbeit im Digitalrat im August 2018 hatte ich tatsächlich noch die Hoffnung, dass wir auch in Europa einen Global Player im Digitalmarkt aufbauen können. Inzwischen ist diese Hoffnung aber ein gutes Stück weit geschwunden. Denn uns fehlen schlichtweg die Strukturen. Nach meiner Überzeugung braucht es auch in Deutschland einen Chief Technical Officer (CTO) in der Regierung, wie es ihn unter der Obama-Administration in den USA gab. Und diese Position muss mit erfahrenen Experten aus der Wirtschaft besetzt werden, die sowohl eine große Expertise als auch Durchsetzungsvermögen mitbringen. Letzte CTO unter Obama war beispielsweise mit Megan Smith eine langjährige Google-Managerin. Das ist hierzulande leider anders.

Das klingt aber machbar. Sind das in Ihren Augen die einzigen Probleme?

Nein, bei Weitem nicht. Das größte Problem ist für mich, dass wir zu viele digitale Analphabeten haben und wir dieses Problem nicht konsequent bekämpfen. Während Lesen- und Schreibenlernen für die meisten Menschen selbstverständlich sind, fristet der richtige Umgang mit Daten ein Schattendasein. Das halte ich für sehr gefährlich. Deshalb braucht es in der Schule dringend das Fach Datenkunde, wie es längst Tier-, Pflanzen- oder Erdkunde gibt. Für mich als Physiker gehört dazu, oft wie ein Physiker zu denken: Wissen, was wahrscheinlich, unmöglich, unwahrscheinlich oder unmöglich ist. Schüler, Verbraucher, Bürger und Wähler müssen ein Gefühl für Größenordnungen bekommen.

Sie sind im Digitalrat dafür mitverantwortlich, das Mindset der Deutschen zum Thema Digitalisierung zu verändern. Sie haben kürzlich in einem Interview gesagt, dass die Deutschen vor allem die negativen Aspekte der Digitalisierung sehen, die Amerikaner hingegen vor allem die positiven. Wie kann hierzulande ein Umdenken stattfinden?

Ehrlich gesagt habe ich mittlerweile wenig Hoffnung, dass wir mit den aktuellen Strukturen das Mindset der Deutschen wirklich ändern können. Anders verhält es sich beispielsweise in Frankreich: Dort hat Präsident Macron die Digitalisierung zu einer wirklichen Chefsache gemacht und treibt den Mindset-Wandel voran. Er lebt den digitalen Wandel, was sich auch in seinen Interviews widerspiegelt. Diese behandeln zum Teil wichtigere Aspekte als die offiziell verabschiedeten Strategiepapiere der deutschen Bundesregierung und ihrer vielen Räte beziehungsweise Gremien zum Thema Künstliche Intelligenz.

Das ist ein vernichtendes Urteil für den Digitalstandort Deutschland. Was muss in Ihren Augen geschehen, um hier gegenzusteuern?

In der Welt entstanden und entstehen viele Gründungen aus der Not heraus, weil vorher etwas nicht funktioniert hat oder katastrophal endete. Eines der besten Start-ups der letzten 100 Jahre ist die BRD. Aus dem Nichts wurde dieses Land einschließlich seines großartigen Grundgesetzes geschaffen. Dagegen ist doch Facebook eine Puppe. Aber heutzutage haben die meisten Deutschen nicht den (wirtschaftlichen) Druck, etwas Neues zu tun. Vielen geht es einfach zu gut, sie wurschteln so vor sich hin und bauen ihre kleinen Sandburgen, so wie im Digitalrat. Ganz anders ist die Einstellung von Gründern in den USA oder auch in China: Make new mistakes every day. Als Experimentalphysiker stehe ich voll hinter diesem Ansatz. Aber wie viele Deutsche würden diesen Satz unterschreiben? Selbst bei Amazon haben wir nur dank zahlloser Experimente und oftmals Zufällen neue Wege und neuen Lösungen gefunden.

Jetzt sind wir neugierig. Was heißt das genau?

Dass Amazon angefangen hat, Waren versandkostenfrei zu liefern, beruht – wie man sich erzählt – auf einem Fehler eines Amazon Softwareentwicklers in Frankreich. Er soll seinerzeit schlichtweg in einer Programmierung die Portokosten vergessen haben. Dadurch wurde ein regelrechter Run auf Amazon in Frankreich ausgelöst. Dieser Zufall war der Ausgangspunkt für unsere umfangreichen Untersuchungen bei Amazon, ab welchem Einkaufswert wir die kostenlose Lieferung anbieten wollten. Experimente und Zufällen sind meine persönliche Grundhaltung: „Embrace the noise“. Jeder sollte die Bereitschaft haben, Zufälle zu akzeptieren und davon zu lernen. Auch das gehört dazu, das Datenanalphabetentum zu überwinden.

Arne Schönbohm

Cybersicherheit made in Germany

Die Digitalisierung ist ein großes Versprechen insbesondere für die Wirtschaft. Sie bietet ökonomische Chancen, Effizienzvorteile und kann uns allen im Beruflichen wie Privaten den Alltag erleichtern. Klar ist aber auch, dass sie uns als Gesellschaft und unser Wirtschaftssystem verwundbarer macht. Als die nationale Cyber-Sicherheitsbehörde hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) in den vergangenen Jahren eine neue Qualität der Cyber-Angriffe festgestellt.

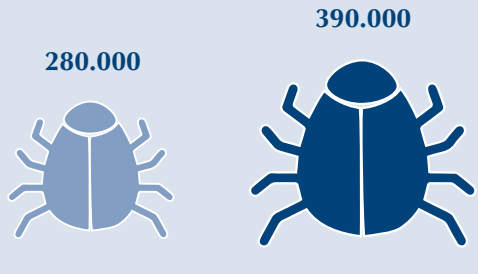
Nicht nur hat sich die Angriffsfläche durch die fortschreitende Vernetzung vergrößert, auch die Art der Angriffe und die ausgewählten Ziele heben die Gefährdungslage auf ein neues Niveau. Durch WannaCry und NotPetya kam es 2017 zu Produktionsausfällen und Schadenssummen, die einzelne Unternehmen mehrere Hundert Millionen Euro gekostet haben. Anfang 2018 wurden Schwachstellen in Hardwareprodukten veröffentlicht – sie werden uns über Jahre begleiten, insbesondere im Virtualisierungsumfeld. Nicht zuletzt wird die unter dem Namen Emotet bekannt gewordene Schadsoftware noch ausgefeilteren CEO-Fraud und gefährliche Phishing- und Spam-Mails ermöglichen. Das Auslesen von Kontaktbeziehungen und die Möglichkeit, auf das Opfer angepasste Schadsoftware wie Ransomware oder Banking-Trojaner nachzuladen, machen Emotet zu einer ernsten Bedrohung, die bereits Ende 2018 für Produktionsausfälle und damit für Millionenschäden in deutschen Unternehmen gesorgt hat.

Dabei ist das Potenzial der Digitalisierung nahezu unbegrenzt. Bis zum Jahr 2025 kann Europa insgesamt bis zu 1,25 Billionen Euro zusätzliche industrielle Wertschöpfung erzielen, wie eine durch den BDI beauftragte Studie 2015 ergeben hat. Längst laufen viele Prozessschritte in der Industrie voll automatisiert ab. Neu ist dabei die digitale Vernetzung der Maschinen. Maschinen und Produkte kommunizieren miteinander und die Flexibilität der Produktion nimmt erheblich zu. Diese digitale Vernetzung ist ein wichtiger Faktor für die Produktivität und das wirtschaftliche Wachstum in Deutschland. Die steigende Anzahl von „Smart Factories“ und vernetzten Objekten wird aber die Anfälligkeit der Wirtschaft für Hackerattacken und Cyber-Angriffe weiter erhöhen. Industrieunternehmen sind zudem häufig Opfer von komplexeren Cyber-Vorfällen. Dies sind Herausforderungen, denen wir uns als nationale Cyber-Sicherheitsbehörde und auch als Gesellschaft stellen müssen.

Cyber-Sicherheit muss Chefsache sein

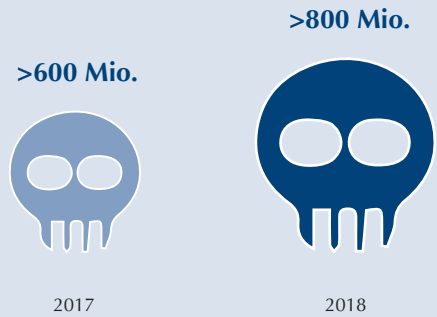
All dies verdeutlicht eines: Cyber-Sicherheit ist die Voraussetzung für eine erfolgreiche Digitalisierung in Staat und Gesellschaft und insbesondere auch in der Wirtschaft. Sie ist keine Innovationsbremse, sondern vielmehr ein Innovationsgarant, wenn die strategischen politischen und unternehmerischen Entscheidungen für die Zukunft der Digitalisierung die Cyber-Sicherheit bereits berücksichtigen. Die Si-

Neue Schadprogramm-Varianten pro Tag



Quelle: Bundesamt für Sicherheit in der Informationstechnik | Die Lage der IT-Sicherheit in Deutschland 2018

Schadprogramme im Umlauf



Quelle: Allianz für Cyber-Sicherheit | Ergebnisse der Cyber-Sicherheits-Umfrage 2017

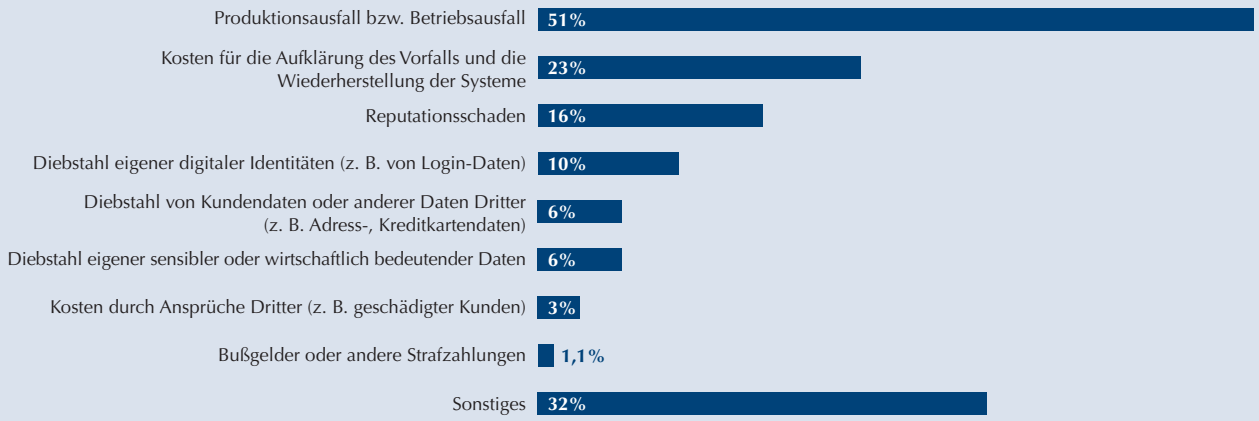
cherheitsarchitektur von computergestützten Arbeitsplätzen und Unternehmensabläufen muss ebenso grundlegend neu gedacht werden wie die IT-Sicherheit von Produkten und Dienstleistungen. Dabei muss die Sicherheit der eingesetzten Systeme durch „Security by design“ und „Security by default“ von vornherein gewährleistet sein. Dies im Sinne des Unternehmenserfolgs strategisch und nachhaltig umzusetzen, ist Chefsache.

Das BSI hat bereits wichtige Schritte unternommen und Impulse gesetzt, um in der Wirtschaft sowohl das Bewusstsein für die Gefährdungen zu erhöhen als auch die Unternehmen bei der Bewältigung der Herausforderungen konkret zu unterstützen. Das BSI verfügt auf Basis seiner technisch tiefgehenden Expertise schon heute über eine integrierte Wertschöpfungskette der Cyber-Sicherheit – von der Cyber-Abwehr über die Beratung und Entwicklung sicherheitstechnischer Lösungen bis hin zur Standardisierung und Zertifizierung. Mit der Allianz für Cyber-Sicherheit (ACS) hat das BSI das größte Selbsthilfe-Netzwerk der deutschen Wirtschaft initiiert und bietet über die ACS praxisnahe Hilfestellungen für die Analyse von Cyber-Risiken und die Umsetzung geeigneter Schutzmaßnahmen. Dabei arbeitet die ACS eng mit Partnern aus Wirtschaft und Forschung sowie Multiplikatoren zusammen. Mit dem Zentralverband des Deutschen Handwerks und dem Handelsverband Deutschland konnten wichtige strategische Partnerschaften initiiert und durch die Unterzeichnung formaler Absichtserklärungen bekräftigt werden. Und mit dem modernisierten IT-Grundschutz bietet das BSI Anwendern aus Wirtschaft und Verwaltung ein fundiertes und praktisches Managementsystem für Informationssicherheit. Ein Erfolgsmodell ist zudem der C5-Standard, der Anwendern ebenso wie Diensteanbietern eine gute und verlässliche Orientierung zur Sicherheit bei Cloud-Diensten verschafft. Neben den großen internationalen Anbietern haben auch deutsche Anbieter diese Testierung durchlaufen und ermöglichen den Unternehmen so, die Sicherheitseigenschaften von Cloud-Services in die Beschaffungsentscheidung einfließen zu lassen.

Absicherungen von vornherein mitdenken

Deutschland als Wirtschafts- und Innovationsstandort muss Vorreiter einer Digitalisierung sein, die Absicherungen von vornherein mitdenkt: Informationssicherheit ist das neue „Made in Germany“ in der Digitalisierung. Dies in Staat, Wirtschaft und Gesellschaft zu gestalten, ist und bleibt Aufgabe des BSI. Als Kompetenzzentrum für Cyber-Sicherheit beschäftigt sich das BSI daher selbstverständlich intensiv mit zukunftsträchtigen Themen, etwa dem maschinellen Lernen oder der Sicherheit der Blockchain-Technologie. Im aktuellen Koalitionsvertrag sind dem BSI weitere wichtige Aufgaben wie zum Beispiel der digitale Verbraucherschutz und der Ausbau der Beratung für die Wirtschaft zugewiesen worden. Aufgaben, die das BSI neben seinen bestehenden gesetzlichen Aufgaben als die in Deutschland zuständige Stelle für Cyber-Sicherheit gern annimmt. Der Dreiklang der Digitalisierung, der zunehmenden Vernetzung und der extrem hohen Innovationsgeschwindigkeit macht es umso wichtiger, dass es auch in Zukunft für das Thema Informationssicherheit einen zentralen Ansprechpartner für Behörden, Unternehmen und Gesellschaft gibt: die nationale Cyber-Sicherheitsbehörde, das BSI. Aus diesem Selbstverständnis heraus gestalten wir auch in Zukunft die Informationssicherheit in der Digitalisierung für Staat, Wirtschaft und Gesellschaft. So wird Digitalisierung made in Germany ein Erfolgsmodell mit Vorbildcharakter für die internationale Gemeinschaft.

Art der Schäden durch erfolgreiche Cyber-Angriffe
Anteile in Prozent an allen Befragten, Mehrfachantworten möglich



Quelle: Allianz für Cyber-Sicherheit | Ergebnisse der Cyber-Sicherheits-Umfrage 2017

Jürgen Reinhart

Cyber – Komplexes Risiko mit Potenzial

Mit der voranschreitenden Digitalisierung und der allumfassenden Konnektivität wachsen auch Cyberrisiken. Die vergleichsweise neuen, komplexen und sich ständig weiterentwickelnden Gefährdungsprofile erfordern Ansätze, die weit über die klassische Versicherung hinausgehen. Gerade für Unternehmen ist Cyber eines der größten Risiken unserer Zeit.

Selbstlernende Maschinen, Cloud Computing, digitale Ökosysteme: Im wachsenden Internet der Dinge steht jedes Objekt mit anderen im Austausch. Waren 2017 noch weltweit 27 Milliarden Geräte online, wird sich ihre Anzahl bis 2030 knapp verfünffacht haben, auf dann 125 Milliarden Geräte[1].

Wachsende Gefährdung

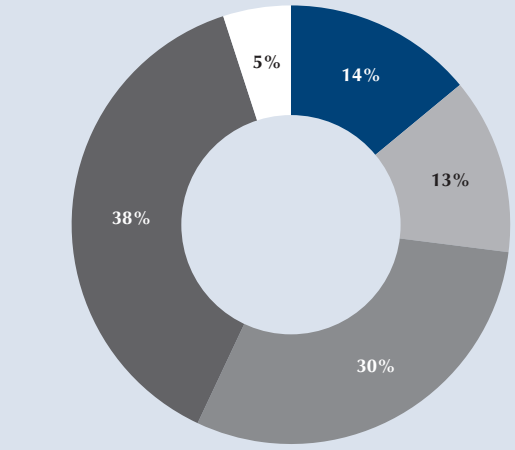
Den Vorteilen der zunehmenden Vernetzung stehen auch Risiken gegenüber. Es ist heutzutage beinahe unmöglich, die einhundertprozentige Sicherheit von digitalen Daten zu garantieren. Das bedeutet, dass Unternehmen beim Auf- und Ausbau einer digitalen Infrastruktur auch permanent in Know-how über Datensicherheit sowie in technische Sicherheitssysteme investieren müssen, nicht zuletzt für die Abwehr von Cyberangriffen. Das wurde deutlich, als die Ransomware-Attacken durch WannaCry und NotPetya weltweit zu Betriebsunterbrechungen und Produktionsstopps führten und die dadurch entstandenen Kosten alle Befürchtungen übertrafen.

2018 dominierten Datenlecks und Datendiebstähle die öffentliche Wahrnehmung: gehackte Infotainment-Systeme in Autos, gleich mehrere Datenskandale eines der weltweit größten sozialen Netzwerke, mehrere Hundert Millionen gestohlene personenbezogene Datensätze. Phishing, also das Abgreifen von sensiblen Personen- und Zugangsdaten und sogenannte DDoS-Attacken, die durch gezielte Überlastung ganze Server lahmlegen, verursachen jährlich Kosten in Milliardenhöhe.
Wir beobachten eine zunehmende Professionalisierung unter Cyberkriminellen. Das Darknet dient als Handelsplattform für Cyberangriffskomponenten aller Art. Noch kritischer: Auch staatlich betriebene Hackerangriffe sind auf dem Vormarsch.

Genaue Summen sind schwer zu ermitteln; Schätzungen gehen derzeit von wirtschaftlichen Schäden durch Cyberangriffe zwischen 400 Milliarden US-Dollar und einer Billion US-Dollar pro Jahr aus. Insgesamt nehmen Cyberattacken und damit auch die verursachten Schäden weiter zu.

Mit der ansteigenden Konzentration von digitalen Werten rücken auch staatliche und supranationale Regulation sowie Präventions- und Deckungskonzepte durch die Privatwirtschaft in den Fokus. Insbesondere für Versicherer stellen Cyberrisiken eine Herausforderung, gleichzeitig aber auch ein wachsendes Marktsegment dar. Derzeit ist nur ein geringer Teil der ökonomischen Schäden durch Cyberangriffe versichert. Vergleicht man die Schadensummen und Auswirkungen mit anderen Risiken, so ist das nur schwer zu verstehen. Reputationsschäden, gestohlene Geschäftsgeheimnisse, abgeflossene Kundendaten, betriebsstörende Eingriffe, komplette Betriebsunterbrechungen oder der Ausfall ganzer Lieferketten sind nur wenige der vielen verheerenden Konsequenzen, die aus einer erfolgreichen Cyberattacke entstehen können. Aus diesem Grund ist eine Versicherung gegen solche Schadenereignisse sinnvoll und wird auch zunehmend nachgefragt.

Anteil der deutschen Industrieunternehmen mit einer Cyberversicherung



Quelle: Bitkom Research | Studie „Spionage, Sabotage und Datendiebstahl – Wirtschaftsschutz in der Industrie“ 2018

Cyberrisiken schwer einzuschätzen

Cyberrisiken unterscheiden sich in wesentlichen Punkten von traditionellen Risiken. Die Daten aus vergangenen Cyberschäden werden uns zwar helfen, das Risiko noch besser einzuordnen, haben aber nur bedingte Aussagekraft für die zukünftige Einschätzung des möglichen Schadenpotenzials. Versicherer und Rückversicherer müssen im Zuge der rasanten technologischen Entwicklung stetig wachsender Angriffstechniken und neuer rechtlicher Anforderungen auch die sich permanent ändernden Risiken erkennen und modellieren können.

Hinzu kommt das Kumulrisiko: Ein einziges Cyberereignis kann gleichzeitig viele verschiedene Unternehmen treffen und darüber hinaus Betriebsunterbrechungsschäden in unterschiedlichen Policen triggern. Cyberrisiken unterliegen keinen geografischen Grenzen und bedrohen alle digital angebundenen Systeme im eigenen Unternehmen und bei angeschlossenen Geschäftspartnern. Hierbei können signifikante Kosten für die Wiederherstellung von Daten und technischen Infrastrukturen, Betriebsausfall und Forensik oder auch die Begleichung von Ansprüchen Dritter entstehen.

Der Cyberversicherungsmarkt ist in den vergangenen Jahren stark gewachsen und verfügt weiterhin über ein beachtliches Potenzial. Dies sorgt in mancher Hinsicht für einen käuferfreundlichen Markt, denn bestimmte Versicherer oder Makler wollen sich gegenüber ihren Kunden durch erweiterte Deckungsbedingungen differenzieren. Umgekehrt sind einige Versicherer angesichts der Tatsache, dass das Verständnis des Kumulpotenzials nach wie vor eine zentrale Herausforderung darstellt, eher vorsichtig, wenn es um eine Erhöhung ihrer Cyberexponierung geht. Die von den Versicherern eingesetzten Akkumulationsmodelle verbessern sich schnell, dennoch bleibt die Marktkapazität im Vergleich zu der von einigen Kunden gewünschten Breite und Größe der Deckung begrenzt.

Die Komplexität der Risiken kann dazu führen, dass es für einen Aktuar eine Herausforderung ist, die Risiken korrekt einzuschätzen, damit sich das eingegangene Kumulrisiko in risikoadäquaten Preisen abbildet. Folglich sollten schon bei der Modellierung der Risiken Teams aus Aktuaren, Versicherungsexperten und Cyberexperten eng und branchenübergreifend zusammenarbeiten.

Aktuare müssen die beabsichtigten Deckungen vollständig verstehen und dabei überlegen, welche Schadenereignisse zu berücksichtigen sind. Darüber hinaus haben sie auch zu beachten, wie sich die spezifischen Bedingungen der einzelnen Verträge auf die Schadenhöhe auswirken.

Cyber als neue Risikoart

Wie lassen sich also Marktchancen nutzen und dabei neue Risiken beherrschen? Sind Cyberrisiken am Ende gar nicht versicherbar, wie einige Branchenvertreter sagen? Sicher ist: Es gibt einige extreme Risiken, die die Versicherungswirtschaft nicht alleine tragen kann. Dazu zählen aktuell Netzwerkausfälle, die die Strom-, Internet- oder Telekommunikationsversorgung unterbrechen. Bei solchen Szenarien können staatliche und Poollösungen durchaus eine ganzheitliche Absicherung komplettieren.

Ein Ansatz, der allein auf Versicherungs-Know-how setzt, gerät schnell an seine Grenzen. Vielmehr sollte das Ziel aller Beteiligten sein, größtmögliche Transparenz zu schaffen. Auch IT-Spezialisten, Behörden sowie Wissenschaft und Forschung können dazu beitragen, Personen und Unternehmen hinsichtlich Cybergefahren zu sensibilisieren und wertvolles Know-how in die Entwicklung von Cyberdeckungen und umfassende Services einzubringen.

Im Schulterschluss zu mehr Sicherheit

Munich Re setzt bei ihren Lösungen für Cyberrisiken auf die Zusammenarbeit mit Technologieunternehmen und IT-Security-Providern. Denn die Anforderung an einen umfassenden Schutz ist komplex und die Absicherung gegen finanzielle Einbußen ist nur ein Teil des Gesamtkonzepts. Dafür entwickeln wir mit Technologiepartnern zusammen hochwirksame und automatisierte Präventionsservices für unsere Kunden. Sie sollen permanent deren Infrastruktur überwachen und so zeitnah Risiken erkennen und Schäden verhindern. Besonders wichtig: Im Schadenfall muss ein Unternehmen schnell reagieren, um den Schaden zu begrenzen und den Normalbetrieb rasch wieder aufnehmen zu können. Dabei stehen wir unseren Kunden mit einem Netzwerk von Experten zur Seite.

Cyberrisiken bleiben eine Herausforderung und die Versicherungswirtschaft ist aufgerufen, sich dieser ganzheitlich anzunehmen. Nur wenn es gelingt, die Angebote an neue oder veränderte Risiken und Bedarfe kontinuierlich anzupassen und zu verbessern, bleibt sie für die Kunden relevant. Und auch nur dann stellt die Herausforderung Cyber eine Möglichkeit für ein nachhaltiges Neugeschäft innerhalb der gesamten Industrie dar.

1) http://bwcio.businessworld.in/article/125-Billion-Connected-IoT-Devices-by-2030/26-10-2017-129552

Dr. Clemens Frey

Cyberrisiken: Neue Aufgaben für Aktuare

Die Absicherung von Cyberrisiken stellt Versicherungsunternehmen vor ganz neue Herausforderungen. Es gibt heutzutage vermutlich kein anderes Versicherungsprodukt, bei dem die Diskrepanz zwischen den aktuariellen Möglichkeiten zu seiner Entwicklung und Bewertung einerseits und dem offenkundigen Potenzial auf den Versicherungsmärkten andererseits größer sein könnte. Um den Herausforderungen zu begegnen und diese Diskrepanz zu verkleinern, müssen wir Aktuare uns neuen Aufgaben stellen. Dazu gehört ein enger interdisziplinärer Austausch ebenso wie die Entwicklung und die Anwendung neuer aktuarieller Methoden.

Um die Auswirkung von zukünftigen Cyberschadenereignissen abzuschätzen, sind angemessene Daten nötig, die passenden aktuariellen Methoden ebenso wie ein umfassendes Risiko-, Markt- und Produktverständnis. Dazu müssen Aktuare nicht nur die Mechanik der Produkte verstehen, sondern auch die (haftungs-)rechtlichen Rahmenbedingungen. Nur dann können sie Modelle zur Tarifierung sowie zur Reservierung und zum Risikomanagement adäquat entwickeln, anpassen und einsetzen.

Herausforderung Cyberrisiken

Dies fällt für den Bereich Cyberversicherung schwer. Denn Cyberrisiken sind anders als bekannte Risiken der Schadenversicherung. Sie weisen aufgrund des hohen Grades an Vernetzung der heutigen Computersysteme (Internet of Things, Cloud Services) starke Abhängigkeiten auf. Ihr Großschadenpotenzial ist aufgrund der heute hohen Verfügbarkeitsanforderungen für Computersysteme enorm.

Kurze Innovationszyklen in der Informationstechnik bedingen eine hohe Veränderungsgeschwindigkeit der zu bewertenden Risiken. Dies betrifft Schadenszenarien ebenso wie Schutz- und Abwehrmechanismen. Das macht es oft unmöglich, auf Grundlage von historischen Schadendaten zu arbeiten. Schließlich fehlen allgemein akzeptierte Messmethoden für bereits eingegangene (non-affirmative) Cyberrisiken ebenso wie für die Risiken aus neuen, dezidierten Cyberprodukten.

Neue Aufgaben

Diese Herausforderungen führen dazu, dass für Cyberrisiken einige grundsätzliche Fragen neu gestellt werden müssen:

- Wie können Cyberrisiken grundsätzlich charakterisiert werden, und wie können Risikoausprägungen – zum Beispiel systematisch im Rahmen von Schadenszenarien – beschrieben und gemessen werden?
- Wie kann die sehr dynamische Entwicklung von Cyberrisiken in die Produktgestaltung und die Tarifierung beziehungsweise Modellierung einbezogen werden?
- Wie kann die Herausforderung mangelnder historischer Schadendaten adressiert werden? Wie können öffentlich verfügbare externe Daten zur Bewertung von potenziellen Cyberschadenereignissen verwendet werden, zum Beispiel Informationen über Netzstrukturen oder über aktuelle Beinaheschäden (Near Losses)?
- Wie können die Risiken in spezifischen Situationen – seien es Einzelrisiken aufseiten von Versicherungsnehmern, seien es die Risiken eines Versicherungsbestandes – systematisch gemessen, bewertet und gesteuert werden?

Vor allem die Frage nach einer verlässlichen Datenbasis steht immer wieder im Mittelpunkt. Auch die Aufsichtsbehörden sehen diesen Punkt als eine der „intrinsischen Herausforderungen“ im Bereich Cyber.

Enge interdisziplinäre Zusammenarbeit notwendig

Eine umfassende Bearbeitung der aufgeworfenen Aufgaben bedarf der engen interdisziplinären Zusammenarbeit von Experten aus verschiedensten Fachgebieten. Dazu gehören IT-/Netzwerkspezialisten, Produkt- und Dienstleistungsexperten, Juristen und Schadenfachleute ebenso wie Aktuare und Risikomanager. Nur auf dieser Grundlage können wir Aktuare unserem Auftrag nachkommen, die mit der Cyberversicherung verbundenen finanziellen Risiken unter Berücksichtigung der spezifischen Risiko- und Produktbesonderheiten – insbesondere auch unter Einbeziehung von Maßnahmen zur Prävention und zum Schadenmanagement – verlässlich messbar zu machen.

Um den in diesem Bereich tätigen Aktuaren eine Orientierung zu geben, hat der Ausschuss Schadenversicherung der Deutschen Aktuarvereinigung die Gründung einer Arbeitsgruppe *Daten und Methoden zur Bewertung von Cyberrisiken* beschlossen. Sie soll einen Beitrag zu einem tieferen aktuariellen Verständnis von Cyberrisiken leisten und wird zeitnah ihre Arbeit aufnehmen.

Positionen von Parteien und Institutionen

Europäische KI-Strategie entwickeln

Deutschlands Unternehmen sind in vielen Bereichen Weltmarktführer, doch in Zeiten der Industrie 4.0 verlieren sie zunehmend den Anschluss. Die Politik ist gefordert, Rahmenbedingungen zu schaffen, damit sich auch hierzulande eine florierende Digitalwirtschaft entwickeln kann. Mit Blick auf die Konkurrenten aus den USA, Japan oder China erscheint ein nationaler Alleingang hier aber wenig Erfolg versprechend. Gefragt sind bilaterale oder multinationale Lösungen mit den europäischen Partnern.

Jens Zimmermann
Digitalpolitischer Sprecher der SPD-Bundestagsfraktion

„Künstliche Intelligenz ist die entscheidende Technologie für die künftige Wettbewerbsfähigkeit unseres Standorts. Wir wissen, Europa hat im globalen Wettbewerb aufzuholen. Doch Deutschland und Frankreich verfügen über Potenziale. Unsere Chance ist es, eine KI mit europäischen Werten zu etablieren. Damit können wir uns zwischen China einerseits und dem Silicon Valley andererseits positionieren. Aus meiner Sicht ist zwingend, dass sich unsere Gesellschaft bei dieser Technologie über die großen ethischen und rechtlichen Fragen verständigt. Mit der KI-Strategie, die wir in der Koalition auf den Weg gebracht haben, bündeln wir die Maßnahmen und stellen drei Milliarden Euro an Fördergeldern bereit."

„Künstliche Intelligenz wird künftig immer mehr Einfluss darauf haben, wie wir leben, arbeiten und wirtschaften. Sie hat das Potenzial, unser Leben innovativer und leichter zu machen. Unsere KI-Strategie zielt darauf ab, Wohlstand und unsere Wettbewerbsfähigkeit zu sichern, aber auch die Standards zu setzen für einen KI-Einsatz mit hohem ethischen Anspruch. Notwendig ist dafür eine nationale und gemeinsame europäische Kraftanstrengung in der Forschung, ein stärkerer Transfer hin zu erfolgreichen Produkten und Geschäftsmodellen und ein breiter gesellschaftlicher Diskurs über den wünschenswerten Einsatz der KI-Technologie. Dazu wird auch das Wissenschaftsjahr 2019 beitragen."

Tankred Schipanski
Sprecher für Digitale Agenda der CDU/CSU-Bundestagsfraktion

Mario Brandenburg
Technologiepolitischer Sprecher der FDP-Bundestagsfraktion

„Die Freien Demokraten sehen in Künstlicher Intelligenz nicht nur eine Schlüsseltechnologie, sondern vielmehr eine Zukunftstechnologie, die einen großen Einfluss auf das Leben aller Menschen haben wird. Trotz der guten, deutschen Grundlagenforschung im Bereich KI fehlt uns der Transfer der Forschung in die Anwendung. Andere vergleichbare Nationen wie Kanada oder Japan liegen dort eindeutig weiter vorne. Neben einer sogenannten Agentur für radikale Innovationen mit einem Frühwarnsystem für disruptive Technologien benötigen wir eine effektive steuerliche Forschungsförderung sowie ein mutiges Konzept für Investitionsanreize, um KI Erfolg versprechend für unsere Zukunft in Anwendung zu bringen."

„Künstliche Intelligenz muss im Sinne von Gemeinwohl und Nachhaltigkeit eingesetzt und weiterentwickelt werden. Um den Standort Europa zu stärken und unsere Werte in die Entwicklung von KI einfließen zu lassen, müssen wir gemeinsame europäische Forschungsprojekte vorantreiben. Wir wollen im Rahmen eines internationalen KI-Gipfels weltweite Standards etablieren. Es gilt, Persönlichkeitsrechte wie Privatheit zu schützen, aber gleichzeitig durch Open Data den Zugang zu qualitativ hochwertigen Daten zu erleichtern, damit eine Diskriminierung durch algorithmische Entscheidungssysteme ausgeschlossen werden kann. Daneben muss ein Hauptaugenmerk auch auf der Weiterentwicklung der Green-IT liegen, damit Klimaziele nicht gefährdet werden."

Tabea Rößner
Sprecherin für Netzpolitik der Bundestagsfraktion von Bündnis 90/Die Grünen

Im Gespräch mit Dr. Frank Grund

Bigtechs werden keine Versicherungen

INTERVIEW

Die Digitalisierung belebt zwar nach Ansicht von Dr. Frank Grund, Exekutivdirektor der Versicherungsaufsicht bei der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin), den Wettbewerb im Finanz- und Versicherungswesen. Echte disruptive Veränderungen sieht er am Horizont aber nicht aufziehen. So bezweifelt er auch, dass die Bigtechs als Risikoträger auftreten und damit den Versicherungen im Kerngeschäft Konkurrenz machen. Vielmehr erwartet er, dass sich Google, Amazon und Co. auf das Geschäft mit den Versicherern konzentrieren und beispielsweise als Versicherungsvermittler an der Kundenschnittstelle tätig werden. Mit Blick auf die künftig noch stärker an Bedeutung gewinnenden Algorithmen fordert die BaFin von allen Marktteilnehmern eine größere Transparenz über die (automatischen) Prozesse und betont: Auch im Digitalzeitalter tragen nicht etwa Computerprogramme, sondern die menschlichen Vorstände die Verantwortung für die Entscheidungen.

Dank Big Data und künstlicher Intelligenz (BDAI) sinken auch im Finanz- und Versicherungswesen vor allem für Vertriebsservices die Markteintrittsbarrieren für neue Wettbewerber. Welche Entwicklungen erwarten Sie diesbezüglich?

Lassen Sie mich mit einer Zahl einsteigen: Seit 2017 haben wir fünf sogenannten Insurtechs eine Lizenz zum Betrieb des Versicherungsgeschäfts erteilt. Solche Neugründungen tun dem Markt gut, denn Wettbewerb belebt das Geschäft – und das ist wiederum gut für die Kunden. Außerdem bringt der Wettbewerb die Vorteile der Digitalisierung erst richtig zur Geltung, beispielsweise in Form schnellerer Prozesse und vereinfachter Kommunikation. Disruptive Veränderungen, also jemand, der den Markt mit einer völlig neuen Idee auf den Kopf stellt, sehen wir bisher allerdings nicht. Ich persönlich glaube auch nicht daran.

In China ist Alibaba Ende vergangenen Jahres aktiv ins Versicherungsgeschäft eingestiegen, Amazon hat in den USA seine eigene Krankenversicherung gegründet. Mit welchen Aktivitäten der Bigtechs rechnen Sie in Europa bzw. hierzulande?

Ich gehe im Moment nicht davon aus, dass Bigtechs zu echten Risikoträgern, also zu Anbietern auf dem Versicherungsmarkt, werden. Zumindest Google Deutschland hat dies bereits verneint. Ich glaube vielmehr, dass sich die Bigtechs auf das Geschäft mit den Versicherern verlagern und beispielsweise als Versicherungsvermittler an der Kundenschnittstelle tätig werden, wie es etwa Amazon in Großbritannien macht. Die Kundenschnittstelle ist besonders attraktiv für neue Marktteilnehmer – zumal im Bereich der Versicherungsvermittlung andere regulatorische Anforderungen bestehen.

Viele Verbraucher haben Sorge, dass in der Zukunft primär Algorithmen ohne menschliche Moralvorstellungen Entscheidungen treffen und es dadurch zu diskriminierenden Differenzierungen kommt. Wie will die BaFin dieser Sorge entgegentreten?

Die Aufsicht ist grundsätzlich technologieneutral. Für uns spielt es also keine Rolle, welche innovativen Finanztechnologien ein Unternehmen einsetzt, solange es alle relevanten aufsichtsrechtlichen Anforderungen erfüllt. Dies schließt selbstverständlich eine geeignete Governance-Struktur mit ein. Darüber hinaus erwarten wir vom Vorstand, dass er uns die Verwendung von Algorithmen in seinem Unternehmen erklären und die maßgeblichen Faktoren für eine automatisierte Entscheidung darlegen kann. Der Vorstand bleibt also weiterhin für alle Vorgänge verantwortlich.

In Ihrer letztjährigen Studie „Big Data trifft auf künstliche Intelligenz“ warnen Sie davor, dass unregulierte BDAI-Anbieter für den Finanzmarkt systemrelevant werden könnten. Wie werden Sie auf diese Entwicklung reagieren?

Hier geht es beispielsweise um Anbieter von Scorings, Ratings oder auch von Cloud-Dienstleistungen. Die Thesen zu „Big Data trifft auf künstliche Intelligenz“ haben wir zur Konsultation gestellt. Nach den Rückmeldungen ist für uns klar: Künftig müssen wir noch stärker auf die gesamte Wertschöpfungskette schauen. Wir müssen solche Aktivitäten unter die Lupe nehmen, die Einfluss auf das Kundenvertrauen und die Integrität des Finanzmarktes haben, auch wenn die betreffenden Unternehmen vielleicht nicht zum regulierten Finanzmarkt gehören. Dabei helfen uns bereits heute die Anforderungen, die Versicherer bei einer Ausgliederung wichtiger Funktionen oder Tätigkeiten erfüllen müssen. Wie wir das konkret umsetzen, ist noch in der Entwicklung. Hier hilft sicher der weitere Dialog mit Wissenschaft und Praxis.

Lassen Sie uns über das Thema IT-Sicherheit sprechen. Ihr Haus hat den Versicherungen im vergangenen Jahr diesbezüg-

lich erheblichen Nachholbedarf attestiert. Wie fällt Ihr Urteil heute aus?

Bereits 2017 haben wir eine umfangreiche „Cyberabfrage" durchgeführt. Dadurch haben wir unter anderem eine gute Übersicht über den Stand der IT-Sicherheit in der Branche erlangt. Den daraus gewonnenen Erkenntnissen gehen wir nun im Rahmen von Aufsichtsgesprächen und örtlichen Prüfungen nach. Deshalb haben wir auch die Aspekte der IT-Sicherheit und die Umsetzung der Versicherungsaufsichtlichen Anforderungen an die IT (VAIT) zu einem Schwerpunkt in unserem Aufsichtsprogramm gemacht.

Für ein abschließendes Urteil ist es natürlich noch zu früh. Allerdings haben erste Ergebnisse gezeigt, dass die Unternehmen ihre IT-Governance nachschärfen sollten. Wir erwarten, dass wir im Rahmen zukünftiger Prüfungen bei den meisten Unternehmen verbesserte Strukturen vorfinden. Gerade die IT-Sicherheit ist ein fortwährender Prozess, sodass uns das Thema in den nächsten Jahren weiter begleiten wird.

BaFin-Präsident Felix Hufeld deklarierte IT-Risiken vor einiger Zeit sogar zur systemweiten Bedrohungslage, auf die auch das Risikomanagement der Versicherungen angepasst werden muss. Inwieweit spiegelt sich diese erhöhte Bedrohungslage bereits ausreichend im Solvency-II-Risikokatalog wider?

Jedes Unternehmen muss sich mit seinen Risiken angemessen beschäftigen – und IT-Risiken können für manche Unternehmen schon heute wesentlich sein. Die Unternehmen müssen sich also gerade im Risikomanagement Gedanken machen, welchen IT-Risiken sie ausgesetzt sind, ob diese wesentlich sind und wie diese in geeigneter Weise gesteuert werden können. Welche Mindestanforderungen an das Risikomanagement der IT zu erfüllen sind, haben wir im vergangenen Jahr in der VAIT konkretisiert. Darüber hinaus haben wir unsere Erwartungshaltung zu IT-Risiken, die speziell mit Cloud-Diensten verbunden sind, in dem kürzlich veröffentlichten Merkblatt Orientierungshilfe zu Auslagerungen an Cloud-Anbieter beschrieben.

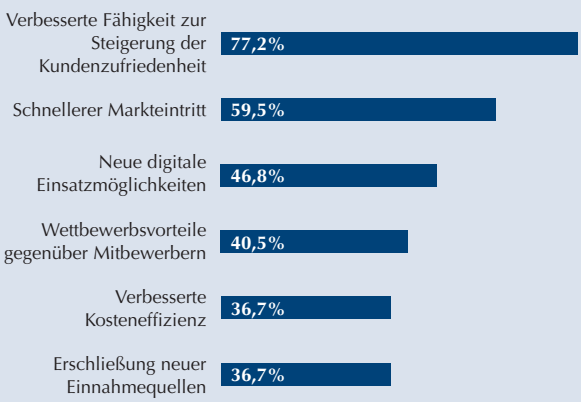
Untersuchungen prognostizieren, dass durch BDAI in den kommenden zehn Jahren zwischen 50 und 70 Prozent der Jobs im Versicherungswesen wegfallen, ein Großteil davon im Bereich Kundenbetreuung und Schadenmanagement. Aber auch immer mehr aktuarielle Routinearbeiten werden zunehmend von Computern übernommen. Welche Rolle werden Aktuare Ihrer Meinung nach künftig in den Versicherungen spielen?

Algorithmen werden in Zukunft sicherlich eine Reihe von Routinearbeiten übernehmen. Und natürlich wird sich dadurch auch die Rolle des Aktuars weiter wandeln. Wenn Sie mich fragen, wird der Aktuar in den kommenden Jahren aber eher an Bedeutung gewinnen. Nehmen Sie beispielsweise die Risikomodellierung, die Produktentwicklung oder die Tarifierung. Diese Bereiche erfordern tiefgreifende versicherungsmathematische Kenntnisse. Gleiches gilt für das aufsichtliche Berichtswesen und die damit verbundenen Anforderungen an Transparenz und Offenlegung. Trotz der unbestrittenen Vorteile der Digitalisierung wird der Aktuar also auch weiterhin eine bedeutsame Rolle im Versicherungsbereich spielen.

Herr Dr. Grund, abschließende Frage: Was war für Sie persönlich die größte digitale Disruption der vergangenen zehn Jahre?

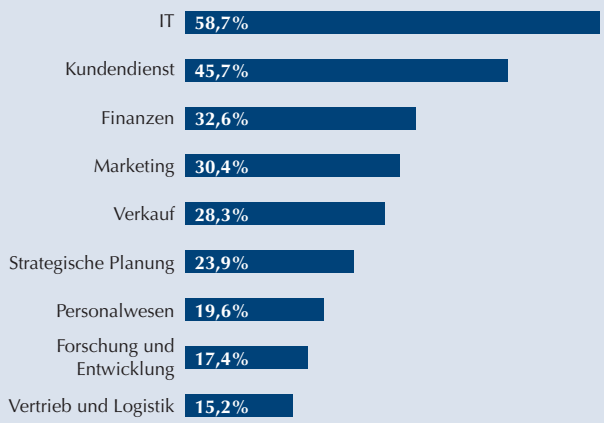
Das Smartphone mit ständig verfügbarem Internet hat sicher auch mein Leben in den letzten zehn Jahren deutlich verändert – bis in den Bereich der privaten Kommunikation. Man kann in den meisten Lebenssituationen unmittelbar Informationen beschaffen, Thesen verifizieren und besprechen. Das empfinde ich als durchaus bereichernd.

Vorteile der Zusammenarbeit zwischen Versicherungen und InsurTechs



Quelle: Capgemini / Efma | Studie „InsurTech"

Einsatz Künstlicher Intelligenz bei Versicherungen weltweit



Quelle: Tata Consultancy Services | Studie „Getting Smarter by the Sector: How 13 Global Industries Use Artficial Intelligence 2017"

Rainer Fürhaupter und Prof. Dr. Manfred Feilmeier

Neue Regeln für personenbezogene Daten, den Treibstoff der digitalen Welt

Daten stehen heute massenhaft in jeder Form – vollständig anonymisiert bis zu rein personenbezogen – zur Verfügung und die permanent steigenden Rechnerleistungen eröffnen neue technische Möglichkeiten, aus denen neue Erkenntnisse und Optionen auch für die sich wie andere Wirtschaftszweige (Industrie 4.0) transformierende Versicherungswirtschaft mit ihrem datenbasierten Geschäftsmodell entstehen.

Die breite Verfügbarkeit von Daten ist essenziell für die globale Wettbewerbsfähigkeit der deutschen und der europäischen Wirtschaft und in vielen Bereichen – gerade auch in der Versicherungswirtschaft – werden in großem Umfang neben anonymisierten auch personenbezogene Daten insbesondere für neue, innovative Produkte benötigt. Damit entstehen neben einem großen Nutzen für die Verbraucher auch einige Risiken, sodass der Schutz der persönlichen Daten wichtiger denn je ist. Diesen Schutz zu garantieren, ist in der globalisierten Welt aus einer rein nationalen Perspektive nicht mehr möglich. Insofern ist die EU-Kommission angetreten, für den europäischen Wirtschaftsraum ein einheitliches Datenschutzrecht durchzusetzen, das sowohl den Schutz der persönlichen Daten als auch den freien Verkehr der Daten für die heutigen und zukünftigen digitalen Prozesse adressiert.

In Deutschland war der Schutz von personenbezogenen Daten bisher schon gesetzlich verankert – für Personenversicherer sogar strafrechtlich. Die seit Mai 2018 gültige EU-Datenschutzgrundverordnung (DSGVO) stärkt nun EU-weit die Rechte der Betroffenen und stellt einige neue Spielregeln für den Umgang mit personenbezogenen Daten auf: neben dem Recht auf Vergessen(werden) auch die Forderung nach Datenminimalität und das Verbot rein algorithmenbasierter Entscheidungen ohne Möglichkeit einer manuellen Überprüfung. All diese Regelungen sind nachvollziehbar und werden selbstverständlich von den Unternehmen und den Aktuaren beachtet. Deren Hauptarbeitsgrundlage sind seit jeher große Mengen personenbezogene, aber vor allem auch die von der DSGVO nicht betroffenen, anonymisierten Daten.

Aus diesem Grund beschäftigt sich die Deutsche Aktuarvereinigung (DAV) eingehend mit der Frage, wie das neue Rahmenwerk im Interesse der Kunden und der Versicherungen mit Leben gefüllt werden kann, um dem berechtigten Anspruch auf Datenschutz und Datensouveränität auf der einen und innovativen, zum Teil immer stärker personalisierten Versicherungsprodukten auf der anderen Seite Rechnung zu tragen.

Die DSGVO präzisiert EU-weit das Verhältnis zwischen den Kunden und den Versicherungsgesellschaften, das nun einem schlichten Credo folgt: Die Kunden haben die Kontrolle über ihre eigenen personenbezogenen Daten. Entsprechend müssen die Unternehmen sicherstellen, dass ihnen Einwilligungen zur Datennutzung der rein personenbezogenen Daten vorliegen und sie müssen klar benennen, wofür diese Daten genutzt werden sollen. Die Kunden haben das Recht auf Auskunft über die gespeicherten personenbezogenen Daten sowie auf deren Löschung. Kurzum: Die personenbezogenen Daten sind das Eigentum der Kunden, das sie für ihre eigenen Zwecke nutzen können oder Unternehmen beziehungsweise Organisationen zur Verfügung stellen können, denen sie ihr Eigentum überlassen möchten. Den Versicherungsgesellschaften ist deshalb bewusst, dass ihnen der Zugriff auf diese personenbezogenen Kundendaten nur zeitlich begrenzt gewährt wird und dass sie in dem Moment, in dem der Kunde das Vertragsverhältnis beendet hat, alle Vorgänge abgeschlossen sind und die Löschung der Daten verlangt wurde, nicht mehr auf die individuellen Daten des Kunden zugreifen dürfen. Daten, die in übergreifende, anonymisierte Statistiken eingegangen sind, sind davon natürlich nicht betroffen.

Verhaltensbasierte Versicherungen sind weiterhin erlaubt

Allein diese kurze Aufzählung zeigt: Die DSGVO hat erhebliche Konsequenzen für das operative Geschäft der Versicherer und damit auch für die Aktuare. Sie sind gefordert, neben der hohen Datenqualität für Kalkulationszwecke jeder Art auch die Datensicherheit zu gewährleisten. Denn bei vielen Produkten und Policen sind die Versicherer darauf angewiesen, dass sie umfangreiche personenbezogene Daten erhalten, gerade wenn sie neben den bisherigen statischen Daten mittels neuer digitaler Möglichkeiten auch dynamische Daten wie Verhaltensdaten in die Produkte und deren Preise – wie in der Kfz-Versicherung (pay-as-you-drive) – einbeziehen wollen. Im Lichte des Grundgedankens der DSGVO stellt sich schnell die Frage, ob Versicherungsunternehmen diese perso-

nenbezogenen Daten überhaupt nutzen dürfen. Die Antwort für die Aktivitätsdaten lautet: Ja! Denn Verhaltensdaten sind für die Erfüllung eines mit dynamischen Preisen versehenen Versicherungsvertrages, zum Beispiel pay-as-you-drive, notwendig und damit ist deren Nutzung grundsätzlich erlaubt. Selbstverständlich müssen aber neben der DSGVO die nationalen Rechtsvorschriften beachtet werden. Siehe dazu auch den nachfolgenden Beitrag.

Menschen haben das letzte Wort

Die DSGVO regelt aber nicht nur, wer wann welche Daten zu welchem Zweck nutzen darf. Sie begegnet mit klaren Vorschriften auch der Sorge vieler Bürger, dass künftig ausschließlich Computer auf Grundlage von Algorithmen ohne menschlichen Eingriff Entscheidungen über das Wohl und Wehe der Versicherungsnehmer treffen: Versicherte haben laut DSGVO das Recht, nicht einer ausschließlich auf einer automatisierten Verarbeitung beruhenden Entscheidung unterworfen zu werden, die ihnen gegenüber rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt.

Für die Versicherungsbranche und insbesondere die Aktuare steht diese Regelung im Einklang mit der über Jahrzehnte praktizierten Vorgehensweise: Kalkulationen von Tarifen und Rückstellungen bedeuten immer, dass mit Daten der Vergangenheit mittels statistischer Verfahren in die Zukunft projiziert wird, wobei immer die Unsicherheit bezüglich der Gültigkeit der Vergangenheitsdaten für die zum Teil Jahrzehnte währende Zukunft entsteht. Daher müssen sich Aktuare sorgfältig um die Auswahl der adäquaten Modelle und Verfahren kümmern, dann die Resultate qualitätssichern und gegebenenfalls manuell korrigieren. Im Ergebnis führt das dazu, dass maschinelle Tools zwar verwendet werden, die Ergebnisse und Entscheidungen aber vom Aktuar persönlich abgenommen und verantwortet werden. Ein weiteres Beispiel ist eine im Zuge einer automatisierten Portfolio-Analyse für eine bestimmte Klasse von Policeninhabern ermittelte Prämienerhöhung, die nur dann nach DSGVO zulässig ist, wenn Aktuare die Abläufe überwachen beziehungsweise in sie eingreifen. Auch da handelt es sich um keine ausschließlich automatisierte Entscheidungsfindung. Die Standesordnung verbietet es den Aktuaren, maschinelle Verfahren „blind“ einzusetzen.

Die Versicherungsgesellschaften und die Aktuare müssen selbstverständlich auch die weiteren Regelungsgebiete der DSGVO wie die Nicht-Diskriminierung von Versicherungsnehmern und auch alle anderen behördlichen und gesetzlichen Vorgaben wie das Gendiagnostikgesetz beachten und einhalten. Normalerweise ist gemäß DGSVO die Verarbeitung personenbezogener Daten der sogenannten besonderen Kategorien verboten. Hierzu zählen zum einen personenbezogene Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Mitgliedschaft in einer Gewerkschaft hervorgehen. Zum anderen gehört dazu auch die Verarbeitung von genetischen beziehungsweise biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung. Diese Daten dürfen nur genutzt werden, wenn sie für die Risikoklassifizierung des Versicherungsnehmers im jeweiligen Produkt unbedingt notwendig sind, gesetzlichen Vorgaben nicht widersprechen und die betroffene Person dem ausdrücklich zugestimmt hat. Die Aktuare müssen sicherstellen, dass diese Anforderungen eingehalten werden und dass sie für Kalkulationen jeder Art geeignete mathematische oder statistische Verfahren einsetzen sowie technische und organisatorische Maßnahmen zur Datenqualität und -sicherheit umsetzen.

Ausblick: Aktuarvereinigung entwickelt Hilfestellungen

Die DSGVO stellt die Versicherungen und ihre Aktuare vor ganz neue Herausforderungen, unter vollständiger Wahrung des Datenschutzes für die Kunden in sinnvoller Weise mit dem „Rohstoff Daten“ weiterhin optimale Ergebnisse zu liefern. Dieser Aufgabe stellt sich auch die DAV mit ihrem neuen Ausschuss Actuarial Data Science, der derzeit Handreichungen für die DAV-Mitglieder entwickelt. Diese sollen die ohnehin schon vorhandenen Standesregeln ergänzen, die die Aktuare zum sorgfältigen Umgang mit (personenbezogenen) Daten und Anwendungen anhalten. Daneben will die DAV eine weitergehende Diskussion zum Umgang mit Daten und Anwendungen insbesondere aus dem Bereich der Künstlichen Intelligenz national wie international anstoßen. Die Versicherungswirtschaft hat ein großes Interesse, das Vertrauen ihrer Kunden gerade auch bezüglich des Datenschutzes zu erhalten. Andererseits sieht sie sich teilweise in Konkurrenz mit den großen Playern der digitalen Welt, die nicht in den Grenzen von Nationalstaaten denken und dem Datenschutz offensichtlich eine untergeordnete Rolle beimessen. Deshalb muss gefragt werden, ob eine Art europaweiter Kodex, der ethische Grenzen festlegt, welche Daten für die Kalkulation von Versicherungstarifen verwendet werden dürfen, der Versicherungswirtschaft und auch ihren Kunden mehr nützt als schadet.

Daniela Rode

Neue Chancen für Prävention und Gesundheitsmanagement

Big Data und Data Analytics halten auch in der Privaten Krankenversicherung Einzug – aber bisher eher im Hintergrund. Moderne Data-Analytics-Verfahren werden beispielsweise dazu genutzt, die Automatisierung in der Leistungsregulierung zu unterstützen oder Vorhersagen zur Entwicklung künftiger Erkrankungen zu machen. Die öffentlichen Diskussionen über die Nutzung von Big Data verengen sich hingegen viel zu oft auf die Frage, ob die Daten von Gesundheitstrackern künftig für die Prämienkalkulation genutzt werden. Aus aktuarieller Sicht lautet die Antwort darauf klar und deutlich: nein!

Denn die private Vollversicherung und viele Krankenzusatzversicherungen werden hierzulande nach Art der Lebensversicherung kalkuliert, sodass für diese Tarife der aufsichtsrechtliche Rahmen sehr eng gefasst ist. Preisdifferenzierungen, beispielsweise durch die Gewährung von Beitragsrabatten innerhalb eines Tarifs, führen zu getrennten Kollektiven und damit zu getrennten Tarifen. Zur Kalkulation der lebenslangen Tarife werden außerdem Längsschnittdaten benötigt, die den Risikoverlauf über sehr lange Zeiträume wiedergeben. Datenreihen von Wearables weisen solche Historien noch nicht auf und eignen sich daher auf absehbare Zeit nicht für das Pricing.

Diskriminierende Preisdifferenzierung ist verboten

Aber auch bei einer ausreichenden Datengrundlage, die eine preisliche Differenzierung erlauben würde, sind nachteilige Bewertungen des Versicherten im Verlauf der Versicherung zum Beispiel wegen einer Verschlechterung seiner Körper- oder Fitnesswerte rechtlich unzulässig. Aufgrund dieser regulatorischen Vorgaben werden in der nach Art der Lebensversicherung kalkulierten Krankenversicherung derzeit kaum Ansätze für eine preisliche Differenzierung durch die Nutzung zusätzlicher Daten gesehen. Deshalb ist die vielfach geäußerte Sorge unbegründet, dass im Zeitalter von Big Data nur noch die Kunden günstige Versicherungstarife erhalten, die sich besonders gesundheitsbewusst verhalten und ihre Daten den Versicherungen über Fitnesstracker oder Smartwatches zur Verfügung stellten.

Deutlich größere Potenziale bietet Data Analytics im Bestands- und Gesundheitsmanagement sowie in der Leistungsregulierung. So kann zum Beispiel die Betrugserkennung im Leistungsbereich verbessert werden. Auffällige, untypische Muster werden durch spezielle Verfahren erkannt und mit entsprechenden Hinweisen zur detaillierten Prüfung an den Sachbearbeiter weitergegeben. Davon profitiert am Ende das gesamte Versichertenkollektiv.

Darüber hinaus sind durch die personenbezogene Analyse von Krankheitshistorien auf Basis von Data Analytics genauere Prognosen über künftige Erkrankungen und Leistungsverläufe möglich, wodurch der einzelne Versicherte individueller betreut werden könnte. Im Fall einer erhöhten Wahrscheinlichkeit für den Eintritt einer ernsthaften Erkrankung kann der Versicherte seinem Bedarf entsprechend Hinweise und Angebote zur Unterstützung erhalten. Und im Krankheitsfall kann die individuelle Versorgung des Versicherten durch ein besseres Zusammenspiel der Fachärzte optimiert und somit das Auftreten von Folgeerkrankungen vermieden oder hinausgezögert werden.

Daneben kann Big Data auch Präventionsmaßnahmen unterstützen. Denkbar wäre zum Beispiel die Erfassung und Bewertung verschiedener Gesundheitsdaten, sportlicher Aktivitäten und der Ernährung. Der Versicherte könnte speziell auf seine Gesundheitssituation abgestimmte Hinweise und Vorschläge, aber auch Erinnerungen an Vorsorgetermine oder Medikamenteneinnahmen erhalten.

Fazit: Der aktuarielle Werkzeugkoffer wächst

All dies zeigt: Die neuen Data-Analytics-Methoden erweitern den aktuariellen Werkzeugkasten, sodass Krankenversicherungs-Aktuare noch besser in der Lage sind, die versicherungstechnischen Risiken einzuschätzen. Zugleich stellen die neuen Möglichkeiten die Versicherungen und ihre Aktuare aber auch vor neue Herausforderungen. So müssen bei allen Anwendungsfällen die strengen Datenschutzvorgaben beachtet werden. Denn das Erheben, Verarbeiten und Nutzen von personenbezogenen Daten und vor allem von Gesundheitsdaten ist nur dann zulässig, wenn der Betroffene einwilligt oder ein gesetzlich definierter Ausnahmefall vorliegt. Die Aktuare sind es aber seit jeher gewohnt, mit großen Mengen sensibler Daten der Versicherten zu arbeiten, sodass sie für diese auch gesellschaftspolitisch wichtige Aufgabe hervorragend qualifiziert sind.

Philipp Miehe

Automatisierung aktuarieller Tätigkeiten

Versicherungsmathematiker sind emotionslose Datenanalysten, humorlose Besserwisser und leben in ihren Formelwelten, möchte man meinen. Tatsächlich werden mit heutigem Stand der Digitalisierung bereits viele aktuarielle Aufgaben fast vollständig von Computern übernommen. Entwickelt, programmiert und gesteuert von Aktuaren, die die Möglichkeiten sowie Grenzen der Statistik kennen und die Veränderung als Lernprozess begreifen.

Digitalisierung und Automatisierung in der Versicherung erfordert ein Neudenken von Prozessen, Systemen und Datenspeicherung. Kann man Maschinen anhand von Realdaten antrainieren, Entscheidungsprozesse zu übernehmen, Trends zu erkennen, und Risiko sowie Betrug einzuschätzen?

Die Tarifierung

Wir alle hören Schlagworte wie individuelle oder dynamische Preisfindung, Mustererkennung, Prognosen von Verhaltensweisen, Schadenminimierung und dynamische Produktanpassung. Aus Pricing-Sicht sind all diese Themen spannend – nicht nur, aber auch wegen Big Data. Die extreme Veränderung in Gesellschaft und Technik – und damit auch des Versicherungsbedarfes – bewegt Trends langjähriger Zeitreihen: Es gibt mehr auswertbare Informationen, mehr Datenkategorien, und vor allem viel mehr Daten. Statistiken werden erneuert und angereichert, sowohl mit neuem Wissen als auch mit besseren Schätzwerten. Die heutige Produktvielfalt und Preisdynamik bei realen Produkten (beispielsweise die zeitliche Anpassung von Flugticketpreisen) treibt Anforderungen an die Flexibilität dazugehöriger Versicherungsprodukte und deren Preisfindung.

Die Reservierung

Open-Source-Bibliotheken oder Spezialsoftware von Beratungshäusern ermöglichen die automatisierte Anwendung verschiedenster Reservierungsmethoden auf Schadendreiecken. Einzig der aktuarielle sowie der Management-Entscheidungsprozess erfordern manuellen Aufwand. Sie bieten mithilfe von Digitalisierung und verbesserter Modellierung ebenfalls Optimierungspotenzial. In internen Modellen werden schon länger „Actuaries in the Box“ eingesetzt, um einfache Reservierungs- und Managemententscheidungen vollautomatisch in den Hunderttausenden von Einjahres-Simulationen zu modellieren.

Das Risikomanagement

Generelle Ansätze zur Automatisierung von aktuariellem Risikomanagement folgen der Philosophie von Tarifierung und Reservierung. Insbesondere Solvency II erfordert die Digitalisierung von Basiskennzahlen, die dann Effizienzen in Risikoberechnung, Buchung und Berichten von Bilanzzahlen ermöglichen. Eine strukturierte Basis erlaubt konsistente Berechnungen, füttert quantitative regulatorische Berichte und ermöglicht klare Einblicke in die Risikotreiber. Entstehende Erkenntnisse können damit für die Unternehmenssteuerung eingesetzt werden. Erläuterungen in quantitativen Reports benötigen noch manuellen Input und sind durch selbstlernende Algorithmen sowie Texterkennungen auf lange Sicht teilautomatisierbar.

Bei Coya – allgemein

Bei Coya, einem InsurTech mit BaFin-Lizenz, also einem durch Technologie getriebenen Sachversicherer, ist Digitalisierung die „Butter auf dem Brot”, die Basis allen Handelns und Denkens. Wir digitalisieren Struktur, Konzeption und Funktion der Abbildung von Realdaten und ermöglichen damit eine optimale Anpassung an die Kundenwünsche der Zeit. Transparenz, Einfachheit und Intuition sind hierbei wichtige Bausteine, die Flexibilität für spätere Erweiterungen erlauben. Die Auswertung und Visualisierung der verwendeten Realdaten sowie deren Anreicherung ermöglichen erst digitale Managementprozesse in Produkt- und Unternehmenssteuerung. Die automatisierte Unterstützung dieser Steuerung (Produktstrategie, -gestaltung und -positionierung) ist eins unserer Ziele. Denn wenn allen Beteiligten Geschäftsinformationen transparent und verständlich vorlegen, wird auch die Struktur einer gemeinsamen Entscheidungsfindung digitalisierbar.

In unserer sich ständig verändernden Welt ist die Digitalisierung – hier gemeint: die digitale Analyse und Visualisierung – von (noch) manuellen Geschäfts- und Entscheidungsprozessen der Schlüssel für eine Effizienzgewinnung von aktuariellen Tätigkeiten. Wir Aktuare bestimmen diesen Zeitenwandel, indem wir komplizierte Themen einfach darstellen, andere motivieren, gut kommunizieren und die Philosophie unserer Tools und Methoden erweitern.

Prof. Dr. Ralf Korn

Data Science und Machine Learning – Herausforderungen und Möglichkeiten für den Aktuar

Der Hype um Data Science lässt den Eindruck entstehen, dass Data Scientists die Allround-Wissenschaftler der Zukunft sind und auch Aktuaren ihre Positionen streitig machen werden. Ist dem wirklich so? Müssen sich Aktuare mit Machine Learning und Data Science auseinandersetzen, um weiter bestehen zu können? Oder ist alles nur halb so wild? Hier wird die Sichtweise der Mathematik, speziell der Statistik, eingenommen, um die Begriffe Data Science und Machine Learning sowie die Rolle des Aktuars entsprechend einzuordnen.

Das durch Google und Co. geförderte Credo von Data Science als universelle Disziplin ist, dass man nur Daten in großem Umfang benötigt, um die ihnen zugrunde liegenden Muster und Gesetzmäßigkeiten durch ein Machine-Learning-Verfahren zu erkennen. Das Verhalten eines Systems – zum Beispiel eines Würfels oder einer Zeitreihe von Aktienkursen – vollständig entschlüsseln zu können und exakte Vorhersagen seiner zukünftigen Werte in Abhängigkeit vom Input (beispielsweise der Handhaltung beim Würfeln oder der Zeitreihe vergangener Aktienkurse) treffen zu können, erscheint ambitioniert. Teils ist es auch unmöglich, wie beim Würfel. Eine mathematisch/stochastische Modellierung des Systems wird von den Datengläubigen als nicht mehr benötigt angesehen. Dieser Gedanke ist nicht neu und liegt auch der historischen Simulation zugrunde, bei der man die Daten der Vergangenheit als vollständige Beschreibung der Realität ansieht und so leugnet, dass die Zukunft Überraschungen birgt.

Data Science = Statistik?

Das Sammeln, Aufbereiten, Darstellen und Analysieren von Daten und das Ziehen von Schlüssen daraus sind Kerngebiete der Statistik und stellen in ihrer Gesamtheit die Definition der Statistik als Wissenschaft dar. Statistiker haben sich schon immer mit Big Data beschäftigt, nämlich den größtmöglichen Datensätzen, die sie mit den Methoden ihrer Zeit analysieren konnten. Man denke an Volkszählungen, Sterbetafeln oder Steuerberechnungen. Dabei wurde oft die maximal vorhandene Rechenkapazität ausgeschöpft, ob menschlicher oder maschineller Natur.

Nicht zuletzt aufgrund beschränkter Rechenkapazitäten in früheren Jahrhunderten ist die Statistik stark modellbasiert ausgerichtet. Durch die Annahme zugrunde liegender Verteilungen für Eigenschaften betrachteter Daten ermöglicht die Konzentration auf wenige Parameter der Verteilung oft eine vollständige Beschreibung der Situation. Gleichzeitig lassen sich Hypothesen über die Parameter mit geringem zusätzlichem Rechenaufwand testen. Schließlich rechtfertigen klassische Resultate der Wahrscheinlichkeitsrechnung wie der zentrale Grenzwertsatz (gerade bei Big Data!) die asymptotische Gütigkeit der getätigten Annahmen. So sind konzeptionell lediglich IT-Aspekte wie das Laden, Speichern und Verarbeiten sehr großer Datensätze nicht schon im Konzept der Statistik vorgesehen.

Machine Learning als rechenintensive Statistik

Dass die modellbasierte, parametrische Statistik auf Verteilungsannahmen basiert, hat ihr schon in der Vergangenheit Kritik eingebracht (sogar eher bei der Behandlung kleiner Datensätze!), der die Entwicklung nicht parametrischer oder verteilungsfreier Verfahren entgegengesetzt wurde. Diese sind häufig sehr rechenintensiv und nur mittels enumerativer Ansätze durchführbar. Unter enumerativen Ansätzen wird das Bestimmen aller auftretenden Möglichkeiten und das Ermitteln der optimalen Lösung eines Problems durch Vergleich über all diese Möglichkeiten verstanden.

Ein Beispiel hierfür ist die Methode der *K-nächsten-Nachbarn* zur Klassifikation, nach der man eine Beobachtung X in die Klasse einstuft, die der mittleren Klasse ihrer K-nächsten-Nachbarn am nächsten kommt. Vergleicht man den Rechenaufwand, der allein für die Ermittlung der Nachbarn und dann speziell der nächsten Nachbarn eines Punkts entsteht, mit dem einer linearen Diskriminanzanalyse, so stellt man einen klaren Unterschied fest.

Das Beispiel ist auch für den Aspekt typisch, dass viele unter dem Oberbegriff Machine Learning subsumierten Verfahren statistische Verfahren sind, die bereits im vorigen Jahrhundert entwickelt wurden und deren Anwendung erst mit der heute zur Verfügung stehenden Rechenpower möglich ist.

Verfahren wie neuronale Netze oder Entscheidungsbäume sind teils seit Mitte des zwanzigsten Jahrhunderts bekannt, werden aber erst mit der gegenwärtigen Welle des Machine Learning von den Anwendern wahrgenommen.

Data-Science-Hype durch Programmierkomfort

Neben der verfügbaren Rechenpower ist die Menge an vorinstallierten Machine-Learning-Verfahren ein Grund für ihre plötzliche Popularität. Ob in R oder in Python, getestete und vollständig implementierte Prozeduren nahezu aller verfügbaren statistischen Verfahren samt Möglichkeiten der grafischen Darstellung stehen komfortabel zur Verfügung und ermöglichen die Anwendbarkeit klassischer statistischer Verfahren als auch rechenintensiver Verfahren (wie zum Beispiel neuronale Netze), ohne diese explizit programmieren zu müssen. Die Spezifikation der Verfahren reicht dafür aus, wobei diese speziell bei neuronalen Netzen bei Weitem nicht immer einfach ist.

Leichte Anwendbarkeit, unkritische Anwendung?

Der Programmierkomfort und der Hype um Machine Learning verführen zu unkritischen Anwendungen von Vorzeigemethoden des Machine Learning, wie zum Beispiel der neuronalen Netze. Sie sind aber als nicht lineare Verfahren sehr anfällig dafür, suboptimale Lösungen als Vorhersagen zu produzieren, die teils weit von der zugehörigen optimalen Lösung entfernt sind. Der Ausweg sehr großer, fein detaillierter Netze kann zu einer Überanpassung an vorhandene Trainingsdaten und damit wiederum zu fehleranfälligen Vorhersagen führen.

Es ist deshalb mit rechenintensiven, nicht linearen Verfahren besonders sorgfältig umzugehen. Ein reines Kalibrieren der Parameter (im Data Science Jargon auch „Trainieren“ oder „Lernen“ genannt) und anschließendes Verwenden der Verfahren zur Vorhersage oder Klassifizierung sollte immer erst nach ausführlichem Test und Vergleich mit einer linearen Methode (zum Beispiel lineare Regression, Diskriminanzanalyse) erfolgen, bei der die optimalen Parameter explizit berechnet werden können.

Mehr noch, um die Zuverlässigkeit nicht linearer Methoden zu erreichen, ist ein sehr sorgfältiges Arbeiten nötig, bei dem Domänenwissen über mögliche Phänomene in den Daten, die Skalierung der verschiedenen Variablen und eventuell weiteren Datentransformationen sowie mit einfacheren Methoden oder Expertenwissen bestimmten Startwerten für die zu kalibrierenden Parameter eine ganz große Bedeutung zukommt. Reine Black-Box-Anwendungen führen eher selten zu guten Ergebnissen. Es ist somit der künstlichen Intelligenz fast immer viel menschliche Intelligenz vorzuschalten, wenn es um ernsthafte Anwendungen geht.

Black Box und Interpretierbarkeit

Die Verwendung hochdimensional parametrisierter, nicht linearer Algorithmen, bei denen keine einfache Input-Output-Beziehung zu erwarten ist, erschwert die Begründbarkeit für erhaltene Resultate wie den Preis einer Versicherung, die auf individuellen Daten basiert. Dies ermöglicht teils noch nicht einmal eine Empfehlung, was zu tun ist, um den Preis durch Verzicht auf eine Absicherungsart unter eine gewünschte Grenze zu drücken. Die leichte Interpretierbarkeit der erzielten Resultate samt Möglichkeiten für eine einfache Sensitivitätsanalyse ist eine Herausforderung, der sich nicht lineare Machine-Learning-Verfahren stellen müssen.

Machine Learning und Data Science als Chance für den Aktuar

Die oben behandelten Aspekte neuer Machine-Learning-Verfahren und die auch in letzter Zeit verstärkt in Fachzeitschriften auftauchenden Anwendungen von Machine-Learning-Verfahren in der Versicherungsmathematik sollen Aktuare ermutigen, sich neutral aber kritisch mit dem Data-Science-Hype auseinanderzusetzen. Aktuare sollten sich nicht scheuen, einfache Fragen an Berater aus dem Data-Science-Bereich zu stellen, und eine für sie verständliche Sprache einfordern. Dies ist vor allem vor dem Hintergrund zu sehen, dass es tatsächlich auch immer eine mathematisch-statistische Beschreibung der Sachverhalte und Verfahren aus dem Machine-Learning-Bereich gibt, die ohne esoterisch anmutende Wortwahl auskommt.

Das Erlernen der Programmiersprachen R oder Python sowie das Vertrautmachen mit neuen statistischen Verfahren, deren Anwendung Erfolg versprechend ist und dank vorimplementierter Software einen überschaubaren Aufwand benötigt, wird den Aktuar in die Lage versetzen, auch von Data-Science-Konzepten zu profitieren, die im Bereich der Statistik angesiedelt sind oder sie zumindest im Hinblick auf ihre Vorteilhaftigkeit zu beurteilen. Dabei sichern ihm sein aktuarielles Fachwissen und die Selbstverpflichtung zur Weiterbildung auch zukünftig seine Position.

Wir rechnen mit der Zukunft

DAV
DEUTSCHE AKTUARVEREINIGUNG e.V.

DGVFM
DEUTSCHE GESELLSCHAFT FÜR VERSICHERUNGS- UND FINANZMATHEMATIK e.V.