Wirtschaftskriminalität:

Auswirkungen der Pandemie auf die Versicherungsbranche

Autoren: Tatewik Kunzmann und Gunter Lescher | PwC Deutschland

Juli 2022

Einleitung

Einmal sind es abgesprochene oder provozierte Verkehrsunfälle, ein anderes Mal fingierte Wasserschäden, dann wieder ist teure Tiefkühlkost nach einem Stromausfall angeblich verdorben: Seit Beginn der Pandemie hat die Versicherungsbranche deutlich mehr Betrugsversuche registriert als zuvor. Allein bei der Allianz Versicherung stieg die Zahl der Betrugsversuche seit Beginn der Pandemie um zehn Prozent[1] – in der allgemeinen Haftpflichtversicherung sogar um gut 20 Prozent[2]. Hinzu kommt, dass Versicherer zunehmend ins Visier von Cyberkriminellen geraten. Diese legten im Sommer 2021 beispielsweise eine Versicherung aus Südhessen lahm und erbeuteten Versichertendaten[3]. Weil sich die Versicherungsbranche seit Beginn der Corona-Krise offen zeigt für mobiles Arbeiten, hat sich mit der zunehmenden Verlagerung der Tätigkeiten ins Homeoffice auch das Risiko eines Angriffs durch Cyberkriminelle deutlich erhöht[4].

Hat die Pandemie Kriminalität begünstigt?

Mit der Pandemie stellen sich der Versicherungswirtschaft beim Thema Wirtschaftskriminalität viele Fragen: Ist der Anstieg von Betrugsversuchen und Cyberangriffen noch als zufällig zu bewerten? Handelt es sich tatsächlich um Einzelfälle oder sind mit der Pandemie verschiedene Deliktarten signifikant angestiegen? Besteht die Gefahr, dass sich hier Muster verfestigen? Haben sich mit der Pandemie auch die Täterprofile und Motive verändert, etwa weil die Straftaten mit den finanziellen Einbußen von Gewerbetreibenden zusammenhängen? Vor allem aber: Brauchen Versicherer neue Instrumente und Strategien, um sich vor jeglicher Form der Wirtschaftskriminalität besser zu schützen?

Diese Fragen beantworten wir mit dem vorliegenden Whitepaper. Dafür haben wir insgesamt 51 Versicherungsunternehmen in Deutschland befragt[5]. **Die empirische Basis der Studie bilden Daten aus der Zusammenarbeit mit Prof. Andreas Klasen vom Institute for Trade and Innovation an der Hochschule Offenburg.** Das Whitepaper widmet sich der empirischen Analyse und behandelt die Instrumente, die die Unternehmen präventiv einsetzen sollten, um dem Risiko von Wirtschaftskriminalität entgegenzutreten. Denn Unternehmen müssen wissen, wie sie sich umfassend schützen und im Ernstfall richtig reagieren können, damit sie aus Krisenzeiten wie der Pandemie gestärkt hervorgehen.

---

1 https://www.allianz.de/presse/mitteilungen/betrueger-werden-digital-die-betrugsaufklaerung-auch/

2 https://www.wiwo.de/finanzen/vorsorge/deutschlands-groesster-versicherer-allianz-stellt-in-der-coronakrise-steigende-zahl-von-versicherungsbetrug-fest/27374218.html

3 https://www.hessenschau.de/wirtschaft/mehr-cyber-attacken-in-hessen-hacker-erbeuten-daten-von-versicherten,cyberangriff-haftpflichtkasse-100.html

4 https://www.versicherungsmagazin.de/rubriken/branche/versicherer-offener-fuer-homeoffice-als-andere-branchen-2938737.html

5 Betrachtungszeitraum: 2020/2021; Rücklaufquote 39 %. Fünf Interviewgespräche ergänzen die quantitative Analyse.

1. Wirtschaftskriminalität steigt um mehr als 20 Prozent

Zugegeben, Wirtschaftskriminalität ist kein neues Phänomen und sie trifft nicht nur Versicherungsunternehmen. Krisen sind nicht der alleinige Auslöser von Wirtschaftskriminalität, aber sie bieten ein Umfeld, das Delikte begünstigt. Erstmals seit 2017 verzeichnet das Bundeslagebild Wirtschaftskriminalität 2020 des Bundeskriminalamts mit einem Plus von 21,5 Prozent eine steigende Zahl von Wirtschaftsdelikten[6]. Exakt 49.174 Fälle verursachten einen Gesamtschaden von rund drei Mrd. Euro. Neu hinzugekommen sind neben Subventionsbetrug bei den Corona-Hilfen, Unregelmäßigkeiten bei den Abrechnungen in Corona-Testzentren und gezielte Spam- und Phishing-Kampagnen im Zusammenhang mit Covid-19.

Klar ist auch: Wirtschaftskriminalität setzt dem Versicherungssektor schon vor dem Ausbruch von Covid-19 überdurchschnittlich zu. 2017 etwa gaben fast drei von vier der befragten Versicherungsunternehmen in einer Studie von PwC an, bereits mindestens einmal von Wirtschaftskriminalität betroffen gewesen zu sein[7]. Die Versicherer lagen damit deutlich über dem Durchschnitt aller Branchen (51 Prozent)[8]. So attestiert eine weitere PwC-Studie beispielsweise den privaten wie gesetzlichen Krankenversicherungen eine besondere Verwundbarkeit in Sachen Abrechnungsbetrug[9]. Insbesondere die hohe Dunkelziffer, von der 84 Prozent der Unternehmen ausgehen, macht den Versicherern zu schaffen.

Laut Gesamtverband der Deutschen Versicherungswirtschaft (GDV) gehen seine Mitgliedsunternehmen davon aus, dass jede zehnte Schadensmeldung dubios ist[10]. Die Pandemie hat die Gefahrenlage verschärft: Der Verband bestätigte bereits im Jahr 2020, dass es Hinweise darauf gebe, dass „betrugsverdächtige Schäden im Zusammenhang mit der Corona-Krise“ stünden.

Die vorliegenden neuen Daten erhärten die Vermutung, dass die Pandemie das Risiko für Versicherungsbetrug noch deutlich erhöhen und sich die Krise zum Brandbeschleuniger der Wirtschaftskriminalität entwickeln könnte.

Sie zeigen, dass sich die Gefährdungslage mit der Pandemie weiter verschärft hat: 60 Prozent der befragten Versicherungsunternehmen registrierten in der Pandemie einen signifikanten Anstieg von Wirtschaftsstraftaten; bei 40 Prozent stagnierten die Zahlen auf hohem Niveau.

---

6 https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Wirtschaftskriminalitaet/wirtschaftskriminalitaetBundeslagebild2020.html

7 PRICEWATERHOUSECOOPERS AG. Wirtschaftskriminalität in der analogen und digitalen Wirtschaft. Martin-Luther-Universität Halle-Wittenberg, 2017.

8 PRICEWATERHOUSECOOPERS AG. Wirtschaftskriminalität in der analogen und digitalen Wirtschaft. Sonderauswertung Versicherungswirtschaft. Martin-Luther-Universität Halle-Wittenberg, 2017

9 https://www.pwc.de/de/managementberatung/forensic-services/krankenversicherungen-sind-anfallig-fur-abrechnungsbetrug.html

10 https://www.gdv.de/de/medien/aktuell/sorge-der-versicherer-corona-gibt-betruegern-auftrieb-61842

2. Die häufigsten Deliktarten: Versicherungsbetrug und Cyberattacken

Am häufigsten haben Versicherungsunternehmen in der Pandemie mit Betrug und Cyberkriminalität zu kämpfen. Nahezu jedes befragte Unternehmen (95 Prozent) sah sich im Berichtszeitraum mit Versicherungsbetrug konfrontiert – einerseits mit überhöhten Schadensmeldungen, andererseits mit frei erfundenen oder absichtlich herbeigeführten Schäden. 35 Prozent der Befragten bestätigten, dass bei ihnen die Verdachtsfälle zugenommen haben.

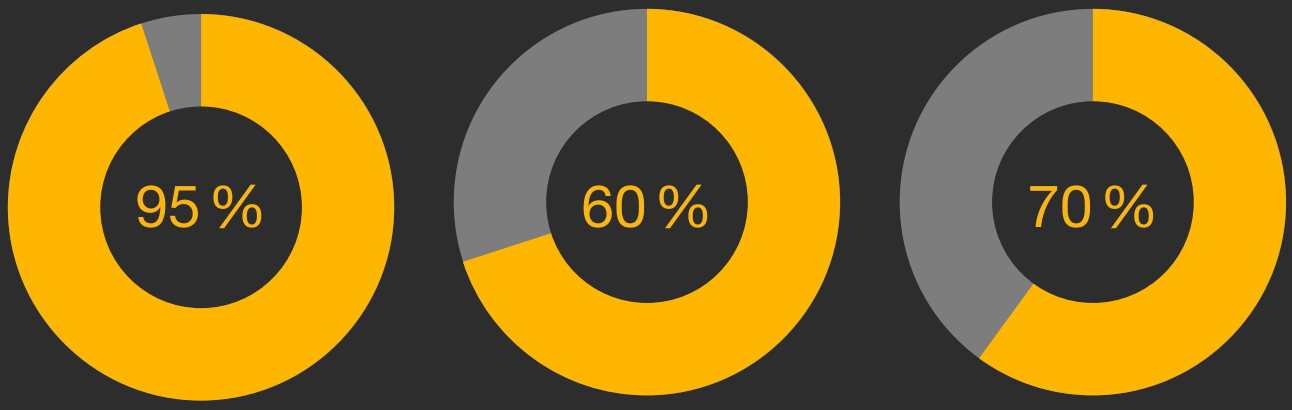
70 Prozent der Befragten mussten im Berichtszeitraum Cyberangriffe abwehren oder deren Folgen bewältigen. Selbstverständlich sahen sich Versicherungen auch schon vor der Pandemie durch Cyberattacken bedroht, mussten Hackerangriffe abwehren und sich vor dem illegalen Zugriff auf Daten und IT-Systeme, Ransomware oder DDoS-Attacken[11] schützen. Doch 55 Prozent der Befragten merkten an, dass sich die Gefährdungslage mit der Coronakrise weiter verschärft habe. Die Versicherer sehen im Wechsel ins Homeoffice einen wesentlichen Grund für den Anstieg dieser Straftaten.

Besonders der CEO-Fraud hat sich mit 15 Prozent zu einer relevanten Größe entwickelt[12]. Ebenfalls 15 Prozent der Versicherer wurden zudem Opfer von Korruption. Anders als beim Versicherungsbetrug oder der Cyberkriminalität erkennen die Versicherungen bei Wirtschaftsdelikten wie Korruption, Geldwäsche oder Insiderhandel keinen pandemiebedingten Anstieg.

11 DDoS steht für Distributed-Denial-of-Service.

12 CEO Fraud ist eine Betrugsmethode, bei der sich der Angreifer als Mitglied des Managements ausgibt und Beschäftigte beispielsweise dazu auffordert, Geld auf ein bestimmtes Konto zu überweisen.

Wirtschaftsdelikte in der Pandemie



95 % der Versicherungsunternehmen sind von Versicherungsbetrug betroffen

60 % der Versicherungsunternehmen registrieren einen deutlichen Anstieg von Wirtschaftsstraftaten

70 % der Versicherungsunternehmen berichten von Cyberangriffen

3. Täterprofile unverändert, aber Zahl der Delikte steigt

In der Versicherungsbranche begehen diverse Tätergruppen Wirtschaftsdelikte. Bei internen Tätergruppen (z. B. Management, Beschäftigte oder gebundene Vermittler:innen, die nur für die betreffende Versicherung arbeiten) erkannten die Unternehmen keine pandemiebedingten Abweichungen.

Anders sieht es bei den Delikten aus, die Externe (z. B. Versicherte sowie Makler und Lieferanten) verüben. Hier sahen sich die Versicherungsunternehmen während der Pandemie überwiegend von zwei Tätergruppen geschädigt: von ihren eigenen Versicherten und von Cyberkriminellen. Dabei stellten die Befragten deutliche Verschiebungen durch die Pandemie fest. Vor der Pandemie begingen Versicherte bei 75 Prozent der Befragten häufig Versicherungsbetrug. 10 Prozent meinten, dass die eigenen Versicherten sehr häufig zu Täter:innen würden.

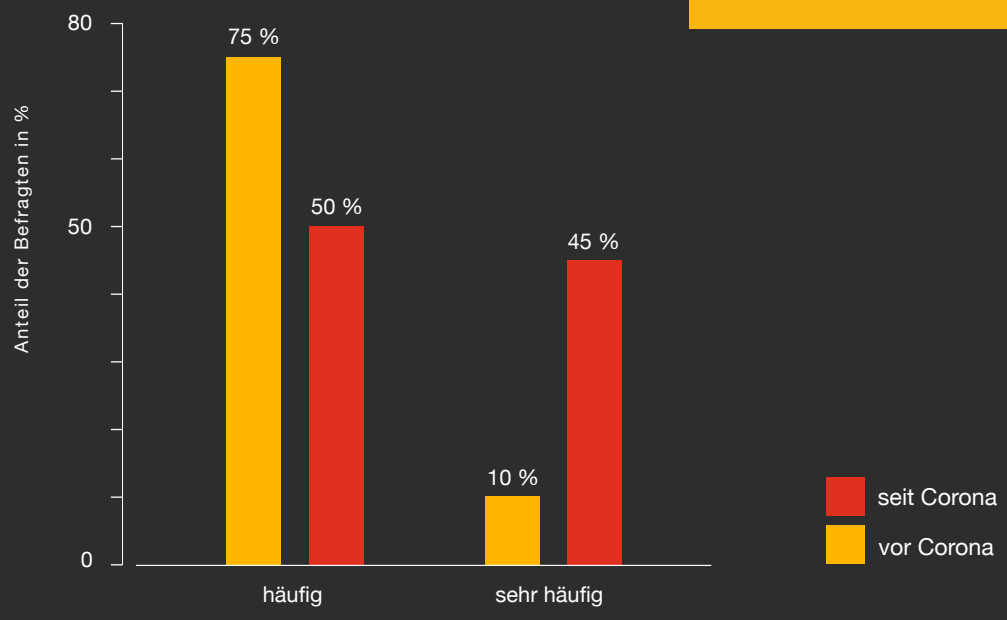
Während der Pandemie traten Versicherte bei 50 Prozent der befragten Unternehmen häufig als Wirtschaftskriminelle in Erscheinung, bei weiteren 45 Prozent sogar sehr häufig.

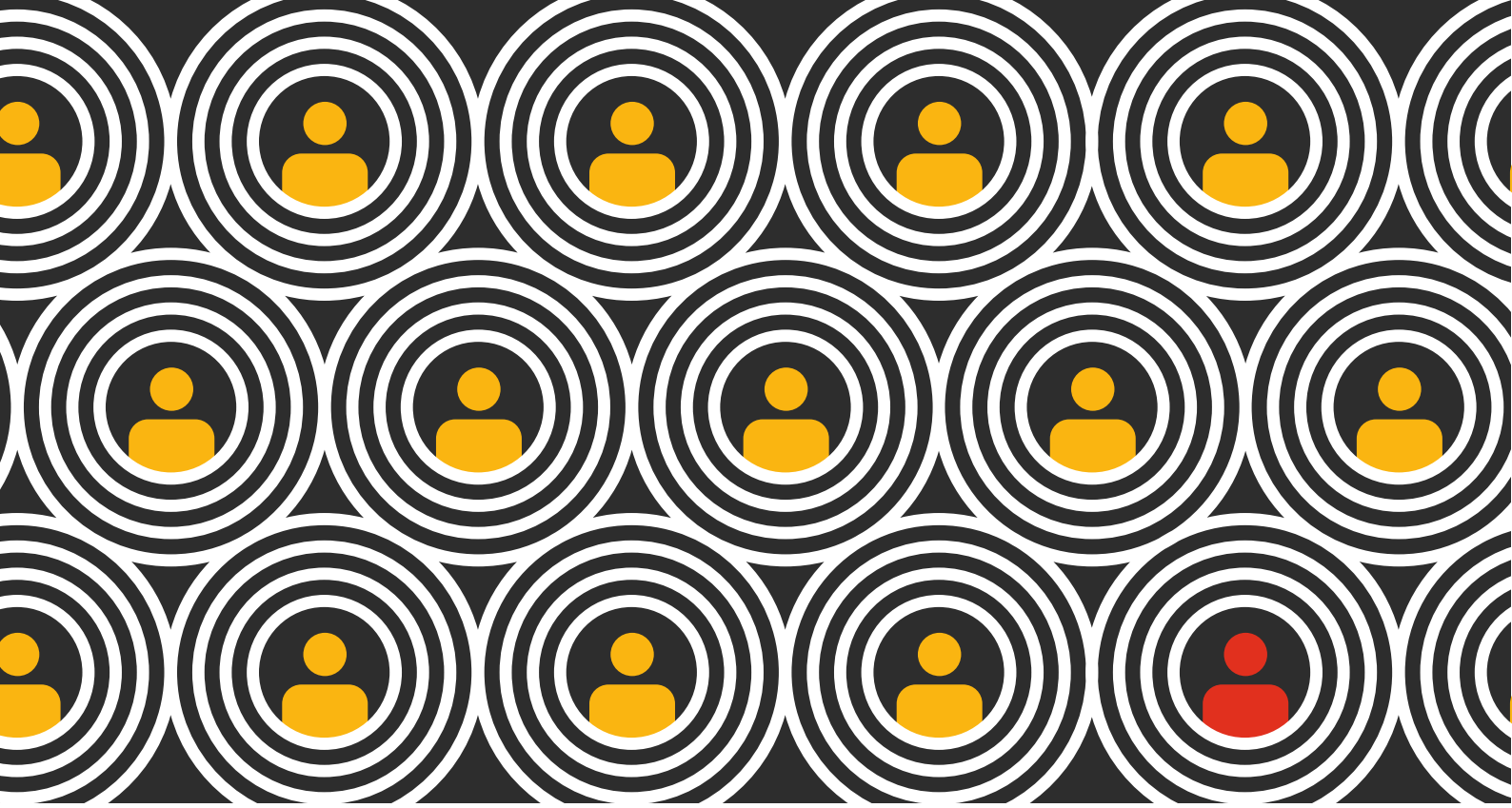
Ein ähnliches Bild zeichnen die Befragten von der Tätergruppe der Cyberkriminellen. Vor der Pandemie schlugen diese bei 30 Prozent der Befragten häufig und bei 5 Prozent sogar sehr häufig zu. Diese Zahlen haben sich mit der Pandemie fast verdreifacht. Nun gaben 60 Prozent der Befragten an, dass Cyberkriminelle häufig Wirtschaftsdelikte begehen – bei nunmehr 35 Prozent sogar sehr häufig.

Fazit

Die Corona-Pandemie hat die Typologie der Wirtschaftskriminellen nicht beeinflusst, wohl aber die Häufigkeit der Delikte erhöht.

Tätergruppe Versicherte –
Relative Häufigkeit verübter Wirtschaftsdelikte





4. Motiv finanzielle Notlage

In finanziell schwierigen Zeiten nehmen Betrugsversuche häufig zu: So hoffen einige Menschen, Umsatz- und Gehaltseinbußen durch unrechtmäßige Schadenszahlungen auffangen zu können. Manches Unternehmen, das durch die Pandemie in Schieflage geriet, kommt in Versuchung, sich von seinem Versicherer indirekt subventionieren zu lassen[13]. Für Versicherungsunternehmen ist dies ein bekanntes Muster. Auch nach der Finanzkrise 2008 häuften sich die Schadensmeldungen.

Mehrheit der Täter:innen sind Unternehmen

Wirtschaftliche Nöte sieht die Versicherungsbranche nun auch in der Pandemie als Hauptursache für die Zunahme von Betrugsversuchen. Legt man das Betrugs-Dreieck des Kriminologen Dr. Donald Cressey[14] zugrunde, gaben alle Versicherungsunternehmen (100 Prozent) finanzielle Notlagen bis hin zur Existenzangst als Motivation für die Betrugsversuche ihrer Versicherten an. So seien viele Menschen und Unternehmen durch die Pandemie unverschuldet in finanzielle Zwänge geraten. Durch Versicherungsbetrug hätten sie ihre Einbußen kompensieren wollen. Um Leasinggebühren zu sparen, meldeten Versicherte beispielsweise Geräte als defekt oder Fahrzeuge als gestohlen. Anfällig für solche Delikte zeigten sich laut der Befragung aber weniger Privatleute als vielmehr von der Krise besonders getroffene Unternehmen. In der Folge nahmen im gewerblichen Bereich auffällige Schadensmeldungen zu: So teilten beispielsweise Fitnessstudios vermehrt Wasserschäden mit, Restaurants zeigten den Ausfall ihrer Kühltheken mit hochpreisigen Produkten an und Einzelhändler schickten fingierte Meldungen von gestohlener Saisonware. Die unverschuldete Notlage diente dabei der inneren Rechtfertigung der Versicherten.

Kriminelle haben die Homeoffice-Situation mit den schlechteren IT-Sicherheitsvorkehrungen als „günstige Gelegenheit“ gezielt ausgenutzt. Der fehlende persönliche Kontakt zwischen Vorgesetzten und Beschäftigten hat nicht nur CEO-Fraud, sondern auch gezielte Phishing- und Spam-Kampagnen erleichtert. Cyberkriminellen fiel es in dieser Ausnahmesituation leichter, vertrauliche Daten von Kund:innen und Unternehmen auszuspähen oder abzufangen.

13 https://www.versicherungsbetriebe.de/business/2020/erst-die-infektionswelle-dann-die-betrugswelle--.html

14 Das vom amerikanischen Kriminologen Dr. Donald Cressey entwickelte Betrugs-Dreieck (Fraud Triangle) nennt drei wesentliche Voraussetzungen, unter denen Menschen (wirtschafts-)kriminelle Handlungen begehen: Anreiz, Gelegenheit und innere Rechtfertigung. In globalen Krisenzeiten verstärke sich die Wahrscheinlichkeit, dass alle drei Faktoren zusammentreffen.

5. Schutzmaßnahmen: Fast ein Drittel der Versicherungen sieht Lücken

Versicherungsunternehmen sind sich der Gefahren bewusst und besitzen längst eigene Abteilungen, um interne Betrugsfälle zu bekämpfen. Um Tätergruppen aus dem eigenen Unternehmen keine Angriffsflächen zu bieten, haben 90 Prozent der Versicherer solche Teams der Compliance-Abteilung zugeordnet. Bei den übrigen 10 Prozent fallen sie dem Zuständigkeitsbereich der Internen Revision zu.

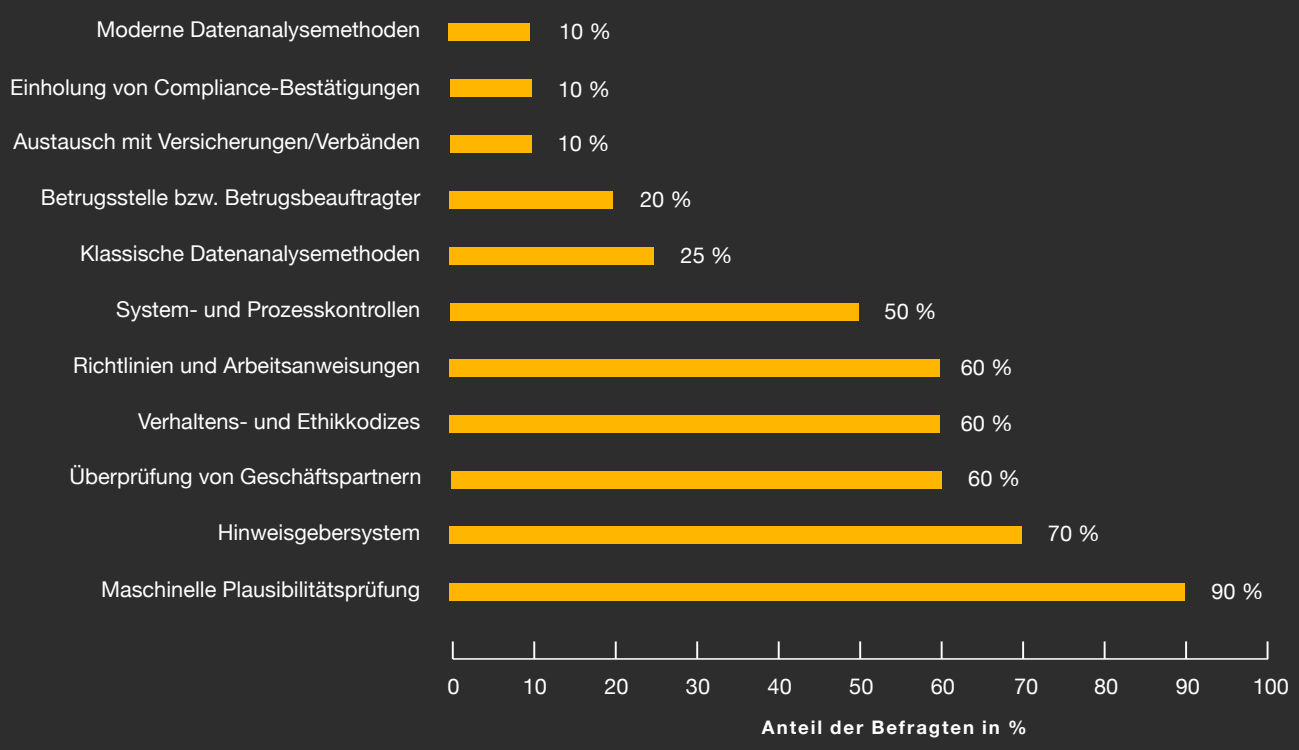
Neben dem internen Betrug wird in der Branche auch der Versicherungsbetrug aktiv bekämpft. Dies erfolgt vorwiegend in den Schaden- und Leistungsbereichen.

Fasst man internen und externen Betrug zusammen, so beschäftigen sich laut der Umfrage bei 60 Prozent der Versicherungsunternehmen zwischen einer und fünf Mitarbeitenden mit der Prävention von Wirtschaftskriminalität. 25 Prozent haben zwischen sechs und zehn Beschäftigte und bei den verbleibenden 15 Prozent der Versicherungsunternehmen sind mehr als 20 Vollzeitkräfte für die Bekämpfung von Wirtschaftskriminalität verantwortlich.

Generell gilt: Alle befragten Versicherungsunternehmen dokumentieren Verdachtsfälle von Wirtschaftskriminalität und werten sie systematisch aus. 90 Prozent haben dazu maschinelle Plausibilitätsprüfungen und etwa 70 Prozent ein zusätzliches Hinweisgebersystem installiert. 60 Prozent haben Verhaltens- und Ethikkodizes, Richtlinien und Arbeitsanweisungen entwickelt und überprüfen regelmäßig ihre Geschäftspartner.

70 Prozent der Befragten schätzen die vorhandenen Maßnahmen als angemessen ein, um die Wirtschaftskriminalität in der Corona-Pandemie einzugrenzen. 30 Prozent räumten ein, dass ihre bisherigen Instrumente nicht ausgereicht haben.

Eingerichtete Schutzmaßnahmen zur Bekämpfung von Wirtschaftskriminalität



6. Nachholbedarf bei digitaler Unterstützung

Zur Kriminalitätsbekämpfung stehen Versicherern bereits digitale Tools zur Verfügung. Moderne Betrugserkennungssoftware erkennt zum Beispiel auf der Grundlage forensischer Software, ob Betrüger:innen Schadensmeldungen mehrfach einreichen. Smarte Algorithmen können Bild- und Textdateien analysieren und Widersprüche aufdecken.

Doch bei der digitalen Unterstützung gibt es großen Nachholbedarf: Nur 25 Prozent der Befragten setzen systematisch auf Datenanalysemethoden wie Red-Flag-Analysen[15]. Lediglich 10 Prozent nutzen künstliche Intelligenz (KI), um Betrugsversuche aufzudecken. Versicherungen, die bereits digitale Analysetechniken einsetzen, bewerten sie als hilfreiche Instrumente, die die menschliche Expertise unterstützen, aber nicht ersetzen können.

15 Bei Red-Flag-Analysen werden alle Transaktionen auf bekannte Betrugsmuster und statistische Auffälligkeiten hin analysiert.

7. Anti-Fraud Management: So bereiten sich Versicherer auf Krisen vor

Jede Krise ist anders. Dennoch gibt es Strategien, die Unternehmen dabei unterstützen, Krisen jedweder Art besser zu bewältigen. Mehr noch: aus solchen unsicheren Zeiten resilienter hervorzugehen. Mit der Pandemie, so zeigt die empirische Analyse, stellen sich für Versicherungsunternehmen keine grundsätzlich neuen Probleme. Mit Betrugsdelikten und Cyberattacken mussten Versicherungsunternehmen auch vor Corona jederzeit rechnen. Lange schon haben sie Fraud als strategisch wichtiges Thema behandeln müssen. Schon weil die finanziellen Kosten bei Versicherungsbetrug und Cyberattacken erheblich sind. Und Reputation wie Vertrauen leiden, wenn Cyberkriminelle persönliche Daten der Versicherten erbeuten. Mit der jüngsten Krise hat sich der Handlungsdruck und die Notwendigkeit eines nachhaltigen Anti-Fraud Managements allerdings nochmals erhöht.

Was aber können Versicherungen tun, um sich grundlegend besser vor Betrug zu schützen – auch und gerade, wenn exogene Krisen die Wahrscheinlichkeit noch einmal deutlich erhöhen, davon getroffen zu werden? Professionelles Anti-Fraud Management gliedert sich in drei Stufen:

1.

Erste Stufe: Prepare – immer vorbereitet sein

Wer sich auf unvorhersehbare Krisen wie eine Pandemie vorbereiten möchte, muss mögliche Schwachstellen beseitigen. Dabei unterstützen das interne Kontrollsystem (IKS) und effektive Hinweisgebersysteme, ein wirksames Compliance- sowie Anti-Fraud-Management-System. Zusätzlich sind solide IT-Systeme, wirksame IT-Security-Maßnahmen und regelmäßige Penetrationtests Pflicht, um sich vor Cyberkriminellen zu schützen. Nur wer seine Schwächen kennt, kann sie beseitigen. Daher ermitteln unsere Teams im ersten Schritt mit einem modular aufgebauten Fraud-Risk Assessment, wie stark die Abwehrkräfte der Kunden sind, ob sie sich ausreichend gegen Betrug, Korruption, Bestechung oder andere Formen der Wirtschaftskriminalität wappnen[16]. Ist dies nicht der Fall, unterstützen wir beispielsweise bei der Einrichtung wirksamer Anti-Fraud-Maßnahmen wie beispielsweise dem Aufbau eines professionellen Hinweisgebersystems, mit dessen Hilfe Unternehmen früh auf Verdachtsfälle stoßen und diese dann eigenständig aufklären können. Wir identifizieren mit der kennzahlengestützten Analyse auch Fraud-Muster der Unternehmen. Für Red-Flag-Analysen setzen wir mathematische und statistische Analysen sowie Data-Mining-Verfahren ein. Zudem unterstützen wir Unternehmen dabei, sichere IT-Strukturen aufzubauen, mit denen sie interne und externe Cybercrime-Angriffe abwehren können. Digitale Technologien wie künstliche Intelligenz oder Prozessautomatisierung verstärken die Prävention.

16 https://www.pwc.de/de/managementberatung/forensic-services/anti-fraud-management-assessment.html

2.

Zweite Stufe: Respond – auf Fraud richtig reagieren

Auch in Zukunft wird sich nicht jeder Angriff, nicht jede Krise verhindern lassen. Daher müssen Versicherer in der Lage sein, angemessen zu reagieren, wenn ihr Unternehmen und somit Marke und Gewinne bedroht sein sollten. An der Digitalisierung ihrer Bearbeitungs- und Aufklärungsprozesse kommen Versicherungsunternehmen damit nicht mehr vorbei. KI-Systeme können beispielsweise die Abwehrkräfte der Versicherer stärken, weil sie Betrugsvorgänge zuverlässig und selbstlernend erkennen. Bei wirtschaftskriminellen Handlungen und Compliance-Verstößen unterstützt unser Investigationsteam[17] bei der Aufklärung, damit Unternehmen rasch belastbare Erkenntnisse gewinnen. Wir stellen sicher, dass betroffene Unternehmen auch in Krisenzeiten die gesetzlichen Vorgaben und internen Regelungen befolgen. Unsere PwC-Forensikteams[18] suchen in den IT-Systemen der Unternehmen nach digitalen Spuren von Cyberkriminellen und erstellen bei Verdachtsfällen, internen Verstößen oder dolosen (vorsätzlichen) Handlungen gerichtsverwertbare Dokumentationen. Wir erarbeiten und implementieren Cybercrime-Notfallpläne, die unseren Kunden eine rasche und adäquate Reaktion ermöglichen (Cyber Incident Response), um größere Schäden zu vermeiden.

3.

Dritte Stufe: Emerge stronger - an Krisen wachsen

Was nach Küchenpsychologie klingt, kann die Immunität eines Unternehmens tatsächlich stärken. Vorausgesetzt, Management und Beschäftigte lernen aus den Erfahrungen einer bewältigten Krise. Wir unterstützen Unternehmen dabei, ihre Compliance-Organisation zu stabilisieren und sich auf so unvorhersehbare Ereignisse wie eine Pandemie und andere vergleichbare Krisen effektiver vorzubereiten.

---

17 https://www.pwc.de/de/managementberatung/forensic-services/investigations.html

18 https://www.pwc.de/de/managementberatung/forensic-services/forensic-technology-solutions.html

Ihre Ansprechpersonen

Sie wollen Ihr Unternehmen krisenfest machen? Wirtschaftskriminellen weniger Angriffsflächen bieten und im Ernstfall angemessen reagieren? Wir unterstützen Sie gern.

Tatewik Kunzmann
Tel.: +49 40 6378-1755
tatewik.kunzmann@pwc.com

Gunter Lescher
Tel.: +49 211 981-2968
gunter.lescher@pwc.com

Mehr Informationen:
www.pwc.de/de/managementberatung/forensic-services.html

Die PricewaterhouseCoopers GmbH Wirtschaftsprüfungsgesellschaft bekennt sich zu den PwC-Ethikgrundsätzen (zugänglich in deutscher Sprache über www.pwc.de/de/ethikcode) und zu den Zehn Prinzipien des UN Global Compact (zugänglich in deutscher und englischer Sprache über www.globalcompact.de).

© 2022 PricewaterhouseCoopers GmbH Wirtschaftsprüfungsgesellschaft. Alle Rechte vorbehalten. „PwC“ bezeichnet in diesem Dokument die PricewaterhouseCoopers GmbH Wirtschaftsprüfungsgesellschaft, die eine Mitgliedsgesellschaft der PricewaterhouseCoopers International Limited (PwCIL) ist. Jede der Mitgliedsgesellschaften der PwCIL ist eine rechtlich selbstständige Gesellschaft.