# Aktives Betrugsmanagement als Teil der Unternehmensstrategie

Patrick Mäder

Lisa Maria Stöfelz

Juliane Welz

**Die Autoren**

Patrick Mäder ist Partner und Verantwortlicher für das firmenweite Versicherungssegment bei BearingPoint.

Lisa Maria Stöfelz ist Business Analyst im Financial Services Bereich mit dem Schwerpunkt Versicherung bei BearingPoint.

Juliane Welz ist Business Consultant im Financial Services Bereich mit dem Schwerpunkt Versicherung bei BearingPoint.

*Hohe Wettbewerbsintensität, sinkende Margen und wechselwillige Kunden prägen den aktuellen Versicherungsmarkt. Vor diesem Hintergrund ist die nachhaltige Steigerung der Profitabilität des Versicherungsgeschäftes von höchster Bedeutung. Ein aktives Betrugsmanagement kann dabei ein wichtiges Instrument zur nachhaltigen Senkung der Schadenaufwände sein und damit zur Steigerung der Wettbewerbsfähigkeit beitragen. Die strategische Relevanz des Themas wurde von der Assekuranz bereits erkannt: Ein Grossteil der Versicherer wird in den kommenden Jahren in eine Optimierung des Betrugsmanagements investieren. Dieser Artikel beschreibt einen konkreten Ansatz zum Aufbau eines effektiven Betrugsmanagements. Dabei werden mehrere Steuerungsfelder betrachtet, um angestrebte Einsparungsziele in vollem Umfang realisieren zu können.*

## Grosses Betrugspotenzial in allen Versicherungssparten

Versicherungsbetrug ist definiert als «jede vorsätzliche Handlung oder Unterlassung, um ungerechtfertigte oder unrechtmässige Leistungen oder Vorteile zu beanspruchen, welche dem Versicherungsunternehmen oder dessen Geschäftspartner materiellen oder immateriellen Schaden zufügt und den Ruf des Unternehmens gefährdet.»[1] Gemäss einer aktuellen Studie von BearingPoint ist das Betrugspotenzial hoch und beträgt auf dem europäischen Versicherungsmarkt zwischen fünf und 25 Prozent (Abbildung 1).[2]

Gemäss Schätzungen der Versicherungsbranche haben rund zehn Prozent aller Schadenmeldungen einen betrügerischen Charakter. Je nach Versicherungssparte kann der Anteil noch höher ausfallen: Beispielsweise wird in der Sparte Haftpflicht ein Betrugspotenzial von bis zu 25 Prozent aller gemeldeten Schadenfälle angenommen.[3] Die Sparten der Motorfahrzeugversicherung sowie die Kranken- und Unfallversicherung weisen ebenfalls ein besonders starkes Betrugspotenzial auf. Aggregiert entsprächen solche zu Unrecht geltend gemachten Versicherungsansprüche jährlich einer Summe von mehr als 93 Milliarden Schweizer Franken weltweit.[4] Eine Entdeckungsquote von lediglich ein bis drei Prozent der betrugsverdächtigen Zahlungen ist heute im Markt üblich. Das zu hebende Potenzial an Kosteneinsparungen ist demnach enorm.

Die aktuelle Situation in den Versicherungsunternehmen lässt sich wie folgt zusammenfassen:

- Durchschnittlich werden vier Prozent der Schadenbearbeiter zur Betrugsbekämpfung eingesetzt.
- Ein effektiver Betrugsexperte deckt jährlich einen Versicherungsbetrug zwischen 700 000 und einer Million Schweizer Franken auf (Benchmark).
- Ein Schweizer-Franken-Ersparnis aus Versicherungsbetrug «kostet» zwischen 0.15 und 0.25 Schweizer Franken (Benchmark).
- 25 Prozent der Versicherungsunternehmen haben Prozesse der Betrugs-

| Versicherungsmarkt / Betrugspotenzial | |
|---|---|
| Deutschland | 5 - 25 |
| Spanien | 5 - 22 |
| Türkei | ca. 15 |
| Frankreich | 6 - 15 |
| Schweiz | ca. 10 |
| UK | 7 - 10 |
| Niederlande | 5 - 10 |
| Österreich | 5 - 10 |
| Italien | 5 - 10 |
| Irland | 5 - 10 |
| Belgien | 5 - 10 |

**Angaben in Prozent**
(n = 11)

**Abb. 1: Betrugspotenzial auf dem europäischen Versicherungsmarkt 2011**

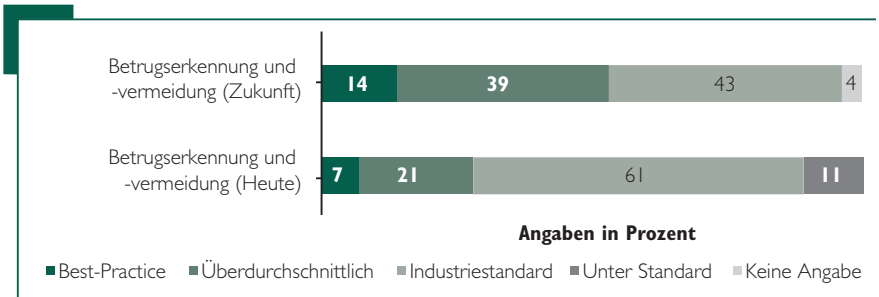


**Abb. 2: Heutiger und zukünftiger Stand von Betrugserkennung und -vermeidung in Unternehmen**

bekämpfung an externe Anbieter ausgelagert.
- 90 Prozent der Versicherungsgesellschaften nehmen aktiv an Brancheninitiativen zur Betrugsbekämpfung teil.

## Betrugsbekämpfung versus Kundenservice und Wettbewerbsfähigkeit

Versicherungsbetrug ist für die Assekuranz ein ambivalentes Thema. Sie bewegt sich hier im Spannungsfeld zwischen den mehrheitlich ehrlichen Versicherungsnehmern, die eine rasche Schadenabwicklung erwarten und der zeitintensiven, detaillierten Prüfung auffälliger Schadenfälle. Während einerseits die Kundenzufriedenheit durch eine möglichst schnelle Leistungserbringung im Schadenfall gestärkt werden soll, muss andererseits die Schädigung der Versichertengemeinschaft durch betrügerische Ansprüche verhindert werden.

Dies bestätigt eine aktuelle Studie: Über 95 Prozent der Befragten befürworten, dass Versicherungsunternehmen bei Verdacht auf Betrug genauere Abklärungen vornehmen. 75 Prozent erkennen an, dass betrügerische Forderungen der Versichertengemeinschaft schaden.[5] Dabei ist das Einsparungspotenzial für die Versicherungsbranche enorm. Die Branchenregel besagt, dass auf sechs Schweizer Franken Kosten für Betrugsbekämpfung eine Schadenersparnis von 14 Schweizer Franken erzielt wird.[6] Dies führt letztlich zu einer verbesserten Combined Ratio, die sowohl den Unternehmen als auch den Versicherungskunden zugutekommt.

Eine effektive Betrugsbekämpfung hat folglich einen Einfluss auf die Schadenquote und auf die Kundenzufriedenheit, was Versicherungsunternehmen motivieren sollte, ein aktives Betrugsmanagement in ihrem Unternehmen zu etablieren. Laut einer aktuellen Studie von BearingPoint unter Versicherungsgesellschaften im deutschsprachigen Raum wurde die strategische Relevanz des Themas erkannt. Bereits mehr als die Hälfte der befragten Unternehmen wollen in den kommenden Jahren in die Optimierung des Betrugsmanagements investieren.

Abbildung 2 zeigt, dass der Best-Practice-Einsatz in den Bereichen Betrugserkennung und -vermeidung stark steigen wird. Immer mehr Versicherungsunternehmen haben den Anspruch, in diesen Bereichen besser als der Industriestandard zu sein.

Um jedoch ein erfolgreiches Betrugsmanagement zu implementieren, muss dem skizzierten Spannungsfeld zwischen Serviceleistung und Betrugsabwehr mit einem integrativen, ganzheitlichen Lösungsansatz begegnet werden.

## Ganzheitliches Framework des Betrugsmanagements

Auf Basis jahrelanger Projekterfahrung und aktuellen Studien hat BearingPoint ein ganzheitliches Framework entwickelt, um Einsparpotenziale im Betrugs-

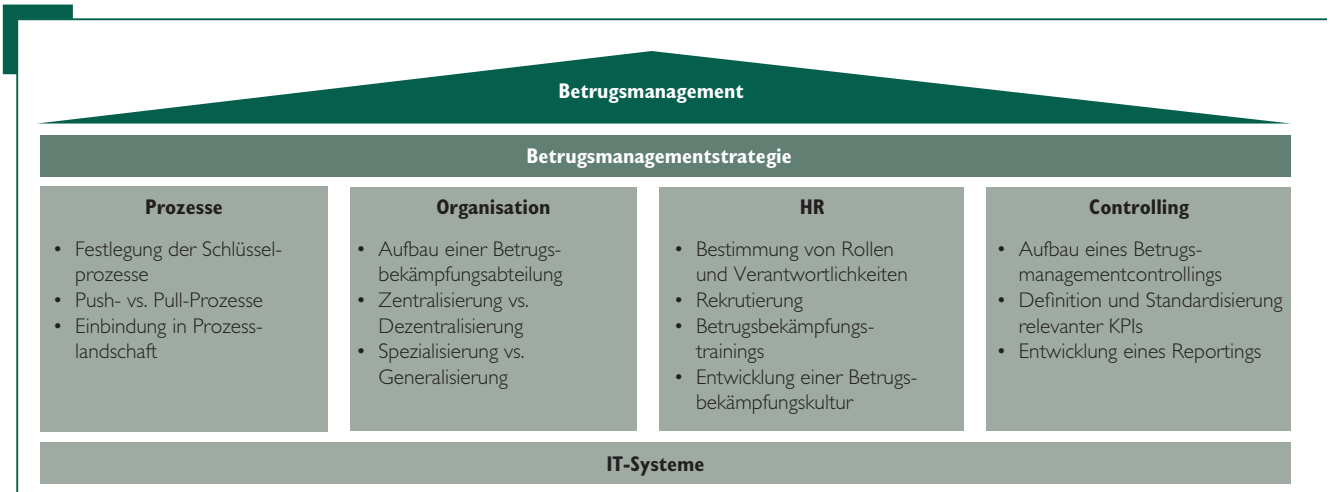


**Abb. 3: Das ganzheitliche Framework Betrugsmanagement**

management zu identifizieren. Dieses Framework umfasst die Steuerungsfelder Strategie, Prozesse, Organisation, IT-Systeme, Human Resources (HR) und Controlling. Dabei wird eine ganzheitliche Betrachtung der einzelnen Steuerungsfelder empfohlen, da bestehende Abhängigkeiten untereinander sonst unberücksichtigt bleiben und angestrebte Einsparungsziele nicht im vollen Umfang realisiert werden können (Abbildung 3).

Die Massnahmen innerhalb der Steuerungsfelder müssen AKTIV im Unternehmen vollzogen werden, um ein nachhaltiges Betrugsmanagement zu gewährleisten und die geplanten Einsparungsziele zu erreichen. Das heisst, die Massnahmen sollten wie folgt umgesetzt werden:

- A – Anwendbar
- K – Kosteneffizient
- T – Transparent
- I – Integrativ
- V – Vorausschauend.

Für den Aufbau eines effizienten und effektiven Betrugsmanagements ist es wichtig eine Strategie zu entwickeln, die im Businessplan integriert ist. Um die erfolgreiche Implementierung sicherzustellen, werden folgende Schritte empfohlen: Analyse, Evaluierung, Design und Operationalisierung sowie eine übergreifende Entwicklung einer Betrugsprävention (Abbildung 4).

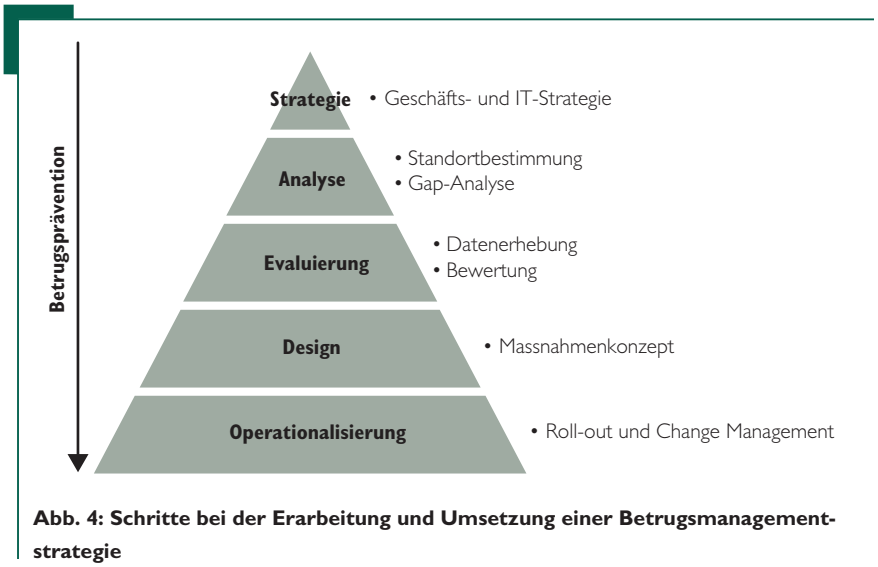


**Abb. 4: Schritte bei der Erarbeitung und Umsetzung einer Betrugsmanagementstrategie**

## HyperCube® unterstützt die Betrugsmanagementstrategie

Das Steuerungsfeld «Strategie» bildet die Grundlage für das Framework, das entsprechende Massnahmen innerhalb der einzelnen Steuerungsfelder festlegt und lenkt. Die Betrugsmanagementstrategie ist dabei in einem Unternehmen kein einmaliger Akt, sondern ein aktiv, immer wieder zu leistender Prozess, der ebenfalls eine Betrugspräventionsstrategie enthält. Sie umfasst ausgehend vom Benchmark eine Standort- und Zielbestimmung, eine Ermittlung des Potenzials, die Festlegung des Gesamtziels sowie eine einheitliche Betrugsdefinition. Nach Festlegung der Betrugsstrategie werden alle nachfolgenden Steuerungsfelder anhand dieser analysiert und ausgerichtet.

Eine zusätzliche Untersuchung komplexer betriebswirtschaftlicher Zusammenhänge bei Schadenfällen und bei Betrug erfolgt mit Hilfe der Datenanalysesoftware HyperCube® von BearingPoint. Anhand dieser Auswertungen werden Optimierungspotenziale identifiziert und Handlungsempfehlungen zur Betrugsbekämpfung und -prävention abgeleitet. Die allgemeine Handlungsorientierung soll dem Ideal nach aus den grundsätzlichen Unternehmenszielen und auf Basis der Ist-Situation im Unternehmen erfolgen. Mit dem Einsatz von HyperCube® kann eine Verbesserung der Combined Ratio von bis zu vier Prozent erreicht werden.

Für die Gesamtbeurteilung der Ist-Situation und die Erstellung der Gap-Analyse im Unternehmen kommt das BearingPoint Reifegradmodell zur Anwendung. Basierend auf diesen Reifegraden wird die aktuelle Situation der einzelnen Steuerungsfelder im Unternehmen bestimmt und mit der angestrebten Zielposition verglichen. Das Modell umfasst die fünf Entwicklungsstufen: unbewusst, reaktiv, proaktiv, gemanagt und optimiert. Anhand dieser Entwicklungsstufen werden Gestaltungsoptionen innerhalb der einzelnen Steuerungsfelder identifiziert (Abbildung 5).

### Prozesse

Effiziente und klar strukturierte Prozesse sind die wichtigste Voraussetzung für ein funktionierendes Betrugsmanagement im Unternehmen, um bei Betrugsverdacht standardisiert und systematisch vorzugehen. Eine klare Definition der Prozesse schafft zudem Sicherheit bei den Mitarbeitern und erhöht die Erfolgsaussichten einer neuen Betrugsmanagementstrategie.

In einem ersten Schritt müssen Schlüsselprozesse zur Bearbeitung von Betrugsfällen definiert werden. Hierzu gehören Prozesse zur Sammlung und Sicherung von Beweisen in Verdachtsfällen sowie Prozesse zur eventuellen Ablehnung des Falles, zur Prozessvorbereitung und für die Beweisführung. Prozesse müssen die Aktivitäten, den Inhalt sowie die beteiligten Personen / Abteilungen beschreiben und anhand geeigneter Kennzahlen messbar gemacht werden.

Die meisten Prozesse im Betrugsmanagement sind Push-Prozesse, das heisst, der Betrugsverdacht wird beispielsweise bei der Schadenaufnahme festgestellt, validiert und an einen Betrugsexperten übergeben. Eine andere Prozessmöglichkeit, um einen grossen Erfolg in der Betrugsbekämpfung zu erzielen, sind sogenannte Pull-Prozesse. Bei diesen können sich die Betrugsermittler, die die aktuellen Betrugsmethoden vor Ort kennen, Schadenfälle mit entsprechenden Indikatoren selbständig herausfiltern.

| | Unbewusst | Reaktiv | Proaktiv | Gemanagt | Optimiert |
|---|---|---|---|---|---|
| **Strategie** | • Keine (zufall-gesteuert) | • Keine (es wird nur reagiert) | • Rudimentär (nicht messbar) | • Messbare Strategie<br>• Zielsetzungen | • Sparten- und bereichsübergreifend (UW, Produkt, Risk-mgmt., Vertrieb etc.) |
| **Organisation** | • Keine Betrugs-organisation | • Betrugsfunktion (z. B. Existenz von Ansprech-partnern) | • Betrugsorganisation / -funktion | • Betrugsbereich (Verantwortungs-bereich)<br>• Betrugscontroller | • Übergeordneter Verantwortungs-bereich |
| **Prozesse** | • Keine definierten Prozesse | • Checklisten<br>• Prozess- und Ansprechpartner dokumentiert | • Optimierte, verein-heitlichte Prozesse<br>• Gelebte Prozesse | • Prozesse sind messbar<br>• Prozesse werden gesteuert | • Prozesse werden kontinuierlich optimiert und berücksichtigen Schnittstellen |
| **IT-Systeme** | • Keine IT-Unter-stützung | • Existenz rudimentärer Regeln / Risikoindikato-ren (keine direkte Anbindung) | • Betrugserkennungs-system ist vorhanden<br>• Keine Workflow-unterstützung | • Intelligentes Betrugs-erkennungssystem (hohe Datenqualität)<br>• Worfklowsteuerung | • Sparten- und bereichs-übergreifende Integration und Nutzung der Betrugs-daten (UW etc.) |
| **Controlling** | • Keine Controlling-Instrumente | • Manuelle Listen<br>• Ad-hoc-Aus-wertungen | • Basiskennzahlen<br>• Auswertung von Listen<br>• Festlegung von Massnahmen | • Controllingkreislauf<br>• Erfolgscontrolling | • Frühwarnsystem<br>• Forecast |
| **HR** | • Keine Stellen-beschreibungen / Schulungen | • Stellenbeschreibung (integriert) | • Regelmässige Schulungen<br>• Sensibilisierung der Mitarbeiter (Awareness) | • Rollengruppen-gerechte Trainings<br>• Recruitingprozesse<br>• Anreizsystem | • Sparten- und bereichs-übergreifender Wissens-transfer |

**Abb. 5: Das BearingPoint Reifegradmodell – Gestaltungsoptionen**

In einem zweiten Schritt werden die Prozesse zur Betrugserkennung und -bearbeitung in die bestehende Prozesslandschaft eingebunden. Der Ausbau des Automatisierungsgrades der Prozesse ist in Zukunft erstrebenswert, da dadurch kürzere Bearbeitungszeiten und geringere Kosten erzielt werden können.

## Organisation

Dieses Steuerungsfeld beschreibt den Aufbau und die organisatorische Einbindung des Betrugsmanagements in das Unternehmen. Rollen und Verantwortlichkeiten innerhalb des Betrugsmanagements müssen klar definiert und dokumentiert sein, damit Prozesse im Rahmen der Betrugsüberprüfung greifen können. Möglichkeiten dafür sind unter anderem der Aufbau einer zentralen Betrugsbekämpfungsabteilung, die sich generalistisch um alle Verdachtsfälle kümmert oder mehrere dezentrale Einheiten, die spezialisiert – nach Sparten, Regionen oder Ähnlichem – agieren.

Das Versicherungsunternehmen muss an dieser Stelle evaluieren, ob es alle Prozessschritte des Betrugsmanagements selbst durchführen will oder Teile der Wertschöpfungskette an externe Kooperationspartner, wie beispielsweise Betrugsermittler, Gutachter und Ähnliche, auslagert. Aktuell gibt es einen Trend zum Outsourcing von Prozessen der Schadenregulierung und -steuerung. Dadurch entstehen Netzwerke von Regulierungsberechtigten, in denen interne und externe Dienstleister zusammenarbeiten. Es ist zu erwarten, dass diese Organisationsformen im Bereich Betrugsmanagement künftig ebenfalls eine immer wichtigere Rolle spielen werden.

## IT-Systeme

Im Rahmen der IT sind grundsätzlich die Integration von Betrugsfunktionen im Schadensystem oder in einer Software zur Betrugserkennung und -bearbeitung sowie spezifische Workflowfunktionen zu definieren. Hierbei ist im Rahmen der Planung und Implementierung das Beziehungsgeflecht zwischen den Prozessen, der Organisation und der IT-Unterstützung zu berücksichtigen.

Für die Betrugserkennung und -ermittlung werden zwei Kategorien von Software eingesetzt: einerseits die neu entwickelten, sogenannten «Predictive Analytics Packages», die durch statistische Methoden und Datenbankauswertungen allgemeine Prognosen und Einschätzungen entwerfen, sowie andererseits die seit längerer Zeit auf dem Markt etablierten spezialisierten Softwarelösungen mit standardisierten, spartenspezifischen Vorkonfigurationen. Das Ziel der IT-Systeme muss es sein, die automatisierte Erkennung von Schadenfällen mit Betrugspotenzial vorzunehmen. Darüber hinaus soll das IT-System die anschliessende Betrugsermittlung unterstützen, den Workflow der notwendigen Prüfungen sowie die Involvierung zuständiger Personen regeln und damit eine optimale Grundlage zur Abwehr betrügerischer Ansprüche schaffen.

Derzeit unterstützt nur etwas mehr als ein Drittel aller Schadensysteme die Betrugserkennung und -bearbeitung. Der Grossteil der Versicherer plant jedoch einen Ausbau dieser Funktionalitäten in den kommenden drei Jahren.

### Human Resources

Die Mitarbeiter haben einen massgeblichen Einfluss auf den Erfolg des Betrugsmanagements und stehen dabei zahlreichen Herausforderungen gegenüber. Für Schadensachbearbeiter gilt es, Betrug zu erkennen, bei Betrugsverdacht zu ermitteln sowie die Ergebnisse in geeigneter Form aufzubereiten, um im Falle der Ablehnung oder bei einem Gerichtsprozess jederzeit auskunfts- und handlungsfähig zu sein. Eine weitere hohe Relevanz hat die Betrugsprävention, für deren Ansätze die Beobachtungen und Erfahrungen der Mitarbeiter eine wesentliche Rolle spielen.

Eine aktive Einbindung der Mitarbeiter im Innen- und Aussendienst ist deshalb eine wichtige Voraussetzung für die erfolgreiche Realisierung von Erfolgspotenzialen. Das Management hat demnach «top-down» die festgelegten Rahmenbedingungen an die Mitarbeiter zu kommunizieren und mit konsequentem Change Management eine Kultur zur Betrugsbekämpfung in der gesamten Organisation zu schaffen. Zudem zählen der Aufbau einer spezifischen Betrugsbekämpfungsabteilung, die Rekrutierung von Betrugsexperten sowie spezielle Trainings zu den entsprechenden Massnahmen.

### Controlling

Als letztes Steuerungsfeld ist das Controlling für die laufende Überwachung und Steuerung des Betrugsmanagements essenziell. In diesem werden relevante Key Performance Indicators (KPIs) zu Effektivität, Kosten, Einsparungen sowie Prozessen definiert und im zentralen Führungstool integriert. Diese werden nach operativen und strategischen Kennzahlen unterteilt. Die Berichterstattung sollte in regelmässigen Abständen erfolgen, um zeitnah entsprechende Massnahmen einleiten zu können. Ein standardisiertes Reporting und der Aufbau eines Management-Cockpits bilden dafür die Grundlage.

## Erfolgsfaktoren für ein aktives Betrugsmanagement

Bisher wurde das Potenzial zur Betrugsbekämpfung unterschätzt oder nur bedingt ausgeschöpft. Ein aktives Betrugsmanagement ist jedoch ein strategisch wichtiger Ansatz zur nachhaltigen Optimierung der Combined Ratios der Versicherungsunternehmen. Die sich daraus ergebenden Einsparungen an Schadenaufwendungen ermöglichen es, das Prämienniveau spürbar zu senken und das Absatzpotenzial zu steigern. Versicherungsunternehmen, die sich also frühzeitig für einen solchen Weg entscheiden, generieren zusätzliche Markteffekte.

Im Rahmen der Betrugsprävention können Medienkampagnen explizit auf die negativen Folgen von Versicherungsbetrug für die Versicherungsgemeinschaft hinweisen. Durch Verbände vorangetriebene Initiativen, die zentrale Betrugserkennungssysteme mit zentraler Datenspeicherung zur Betrugsabwehr unterhalten und diese Informationen den Versicherungsunternehmen zur Verfügung stellen, bieten ebenfalls eine entscheidende Möglichkeit der Kundensensibilisierung. Als weitere Erfolgsfaktoren sind die Berücksichtigung von Betrugsabwehrexpertisen in der Produktentwicklung und -gestaltung zu nennen. Diese sollten das Ziel verfolgen, dem Aussen- und Innendienst als Unterstützung in der Betrugserkennung und -vermeidung zu dienen, was im Rahmen von Bonussystemen, Incentivierung, Schadenfreiheitsklassen und Ähnlichem erfolgen kann.

Aufgrund der wachsenden Anzahl an Schadenfällen spielt die Entlastung und Unterstützung der Betrugsermittler durch spezielle Software eine tragende Rolle. Insbesondere in den Sparten des Massengeschäfts, wie der Motorfahrzeugversicherung sowie der Sach- und Haftpflichtversicherung, scheint der Bedarf an Entwicklung und Unterstützung mittels einer automatisierten Betrugserkennung und Workflowimplementierung auch weiterhin ungebrochen zu sein.

### Anmerkungen

1 BearingPoint Definition.
2 Vgl. BearingPoint / Institut für Versicherungswirtschaft der Universität St. Gallen (2011): Internationale Studie zum Betrugsmanagement.
3 Vgl. Rösler, Reinald (2004): Versicherungsbetrug – eine dauerhafte Herausforderung. In: Versicherungsbetrug. Neue Methoden – effizientere Abwehrtechniken.
4 Vgl. Finanz und Wirtschaft (2011): Versicherungsbetrug eingrenzen, 26.10.2011.
5 Studie des Schweizerischen Versicherungsverbands SVV (2009): Die Schweizer Privatassekuranz. http://www.svv.ch/sites/default/files/document/file/bericht_meinungsumfrage_privatassekuranz_2009.pdf (Abrufdatum: 09. Oktober 2012).
6 Siehe Anmerkung 4.