

**Automatisierte Betrugserkennung –  
Ein innovativer Beitrag zum aktiven Schadenmanagement**

von

Dr. Eberhard Fähnrich, Gen Re

Oliver Lindsiepe, Gen Re

1. Einführung
  - 1.1. Ausgangssituation in der Schadenbearbeitung
  - 1.2. Betrugsbearbeitung als Teil des Schadenmanagements
2. Grundkonzept von RiskShield/ISP
3. Von der Idee zur Lösung
  - 3.1. Zielsetzung
  - 3.2. Realisierung
  - 3.3. Funktionsweise
4. Vorteile von RiskShield/ISP
  - 4.1. Geringe Folgekosten
  - 4.2. Flexible Anpassung an vorhandene EDV-Systeme
5. Aktueller Entwicklungsstand
  - 5.1. Module für die Kraftfahrt-Versicherung
  - 5.2. Module für andere Sparten
  - 5.3. Entwicklung einer kompletten Schadensoftware
  - 5.4. Erfahrungen im Ausland
6. Erfahrungen und Konsequenzen
7. Weitere Erkenntnisse
  - 7.1. Eingeschränkte Wahrnehmung von Versicherungsbetrug
  - 7.2. Unterschätzter Wert von Daten

## 1. Einführung

Versicherungsbetrug ist - nicht nur in Deutschland - zu einer beliebten Einnahmequelle geworden. Brillen werden mutwillig zerstört, sogenannte „Autobumser“ manipulieren oder provozieren Verkehrsunfälle und es gibt sogar Menschen, die vor Selbstverletzung nicht zurück schrecken. Bei Umfragen gaben 27% aller Befragten an, ihre Versicherung schon einmal betrogen zu haben (psychonomics Versicherungs-Betrugsstudie, 1996; Kundenmonitor Assekuranz, 2001). Die finanziellen Auswirkungen für die gesamte Versicherungsbranche beträgt mehrere Milliarden Euro jährlich.

Vor diesem Hintergrund hat die Schadenabteilung der GeneralCologne Re zusammen mit führenden deutschen Erstversicherern und dem Aachener Softwarehaus INFORM GmbH eine Software zur automatischen Erkennung betrügerischer Schadenmeldungen (RiskShield/ISP, wobei ISP für Intelligente Schadenprüfung steht) entwickelt. In Deutschland wird die Software bereits von vielen Versicherungen erfolgreich eingesetzt. Auch im Ausland sind die ersten RiskShield/ISP-Systeme im Einsatz.

### 1.1. Ausgangssituation in der Schadenbearbeitung

Die Kraftfahrt-Versicherung in Deutschland steckt ebenso wie in den meisten anderen Ländern in einer schwierigen Situation. Aufgrund des starken Wettbewerbs gelingt es kaum, auskömmliche Prämien zu erzielen. Auch wenn sich die Rahmenbedingungen in den letzten Jahren leicht verbessert haben, machen nach wie vor viele Versicherungsunternehmen Verluste. Konnte ein Teil der Verluste in der Vergangenheit durch Erträge aus den Kapitalanlagen ausgeglichen werden, macht die dramatisch geänderte Lage an den nationalen und internationalen Geld- und Kapitalmärkten einen solchen Verlustausgleich derzeit nahezu unmöglich. Generell müssen sich die Versicherungsunternehmen in allen Sparten der Aufgabe stellen, den Schadenaufwand zu begrenzen.

Die Schadenabteilungen stehen in dieser Situation vor einer Vielzahl von Herausforderungen:

- Eine steigende Anzahl von Schäden muss mit der gleichen bzw. einer gesunkenen Anzahl von Mitarbeitern in den Schadenabteilungen bearbeitet werden.
- Servicequalität und die Kundenorientierung sind zu verbessern, denn der Schadenfall ist derjenige Kontakt, bei dem die Kundenbindung am meisten beeinflusst wird. Dies führt zu neuen Aufgaben in den Schadenabteilungen: Weg vom „Rechnungsprüfer“ hin zum „Problemlöser“.
- Gleichzeitig arbeiten die Unternehmen daran die Schadenbearbeitung zu beschleunigen und - zumindest bei den zahlreichen Kleinschäden – auf eine aktenarme oder aktenlose Bearbeitung umzustellen. Das konsequente

Ergebnis dieser Entwicklung ist die Schadenaufnahme und die teilweise Schadenbearbeitung im Callcenter, bei der schon am Telefon über die weitere Bearbeitung entschieden werden sollte.

- Daneben müssen die Versicherungsunternehmen die wachsende Anzahl von betrügerischen Schadenmeldungen in den Griff bekommen. Schätzungen gehen davon aus, dass ca. 10% aller Verkehrsunfälle in der Kraftfahrt-Haftpflichtversicherung einen betrügerischen Hintergrund haben. Die Schadenbelastung der Unternehmen wird dadurch allein in Deutschland um 1 Milliarde Euro pro Jahr erhöht. Für den Schweizer Versicherungsmarkt beläuft sich der Schaden allein in der Motorfahrzeugversicherung auf ca. 275 Millionen Schweizer Franken.

## 1.2. Betrugsbearbeitung als Teil des Schadenmanagements

Neben einer kundenorientierten, sachlich richtigen und schnellen Schadenregulierung ist es auch Aufgabe einer qualifizierten Schadenbearbeitung, unrechtmäßige Ansprüche abzuwehren. Viele Versicherungsunternehmen verfügen dementsprechend über spezialisierte Abteilungen, die sich der Betrugsbekämpfung widmen. Eine wirklich wirksame Betrugsabwehr ist aber nur möglich, wenn auffällige Schadenmeldungen möglichst unverzüglich, in jedem Fall aber so frühzeitig erkannt werden, dass die Entschädigungsleistung erst gar nicht zur Auszahlung gelangt. Hierzu bedarf es aber entsprechend ausgebildeter und sensibilisierter Schadensachbearbeiter. Doch selbst dann ist es nahezu unmöglich alle Schadenmeldungen auf ihren Betrugsverdacht zu überprüfen, ohne geeignete technische Unterstützung,

Das bislang in vielen Ländern angewendete Verfahren besteht im Einsatz von Datenbanken, um festzustellen, ob ein Versicherungsnehmer bzw. Anspruchsteller oder ein beteiligtes Fahrzeug bereits in einem anderen Schaden verwickelt war. Diese auf den ersten Blick nahe liegende Lösung führt im praktischen Einsatz allerdings zu mehreren Problemen, die Ihre Effektivität einschränken:

- In einigen Ländern, wie zum Beispiel in Deutschland, lassen die Bestimmungen des Datenschutzes das Speichern, Auswerten und vor allem den Austausch von personenbezogenen Daten nur unter sehr restriktiven Bedingungen zu. Eine automatisierte Betrugserkennung wird dadurch weitgehend unmöglich.
- Auch in Ländern, in denen die Bestimmungen des Datenschutzes weniger restriktiv sind, stellen sich vielfältige Probleme. Diese lassen sich nach unserer Erfahrung im Wesentlichen drei Bereichen zuordnen: Zunächst sind Datenbanken häufig nicht aktuell und nicht vollständig. Darüber hinaus sind automatisierte flächendeckende Prüfungen im Rahmen der Schadenbearbeitung kaum nicht möglich, da die Abfragen vergleichsweise zeitintensiv sind – Antwortzeiten von einigen Minuten sind eher die Norm – und führen häufig nicht zu einem eindeutigen Ergebnis. Dies erfordert somit

wiederum eine Interpretation durch einen qualifizierten Experten. Und letztlich treffen Datenbanken keine Entscheidung über die nächsten Bearbeitungsschritte.

Den größten Nutzen haben Datenbanken also nicht in der Erkennung verdächtiger Schadenfälle, sondern in der Ermittlungsphase. Hier geht es darum, den Verdacht durch Nachweis der Beteiligung an vorangegangenen Schadenfällen zu erhärten oder zu entkräften.

Eine andere Lösung zur Erkennung betrügerischer Schadenfälle wird zur Zeit in den Vereinigten Staaten unter dem Schlagwort „Data Mining“ propagiert. Abgeleitet aus den Erfahrungen in der Erkennung von betrügerischen Fällen in der Kreditkarten- und Telekommunikationsbranche, soll die auf der Basis statistischer Analysemodelle entwickelte Software auch in der Versicherungsbranche verdächtige Schadenfälle aufspüren. Die bislang erzielten Ergebnisse zeigen aber einen nur begrenzten Erfolg. Ein wesentlicher Grund für die geringe Performance dieser Modelle liegt in der komplexen Struktur der Betrugsmuster. Wird eine aussagekräftige Anzahl von Betrugsindikatoren berücksichtigt, müssen zuverlässige Analysen auf einer extrem großen Anzahl von Daten basieren. Dies soll an einem kleinen Beispiel verdeutlicht werden. Auf der Grundlage von zwanzig Betrugsindikatoren – dies ist nach unserer Erfahrung die Mindestanzahl für eine gute Entscheidungsqualität – mit jeweils fünf Ausprägungen, ergeben sich fünf hoch zwanzig verschiedene Fallkombinationen. Werden darüber hinaus jeweils 100 Schadenfälle für jede Kombination berücksichtigt, um statistisch relevante Aussagen treffen zu können, müsste ein Versicherungsunternehmen zunächst 9.536.743.146.062.500 Schadenfälle sammeln und bewerten. Selbst für große Versicherungsunternehmen mit einigen hunderttausend Schadenfällen pro Jahr würde dies Jahrmillionen dauern und ist damit schlichtweg unmöglich.

## 2. Grundkonzept von RiskShield/ISP

Die Experten in den „Betrugsabteilungen“ sind aufgrund ihrer Erfahrung in der Lage recht zuverlässig einzuschätzen, wie betrugsverdächtig eine Schadenmeldung ist und ob es lohnt, diesen Fall vertieft zu untersuchen. Angesichts dieser Situation und vor dem Hintergrund der Probleme, die sich beim Einsatz von Datenbanken ergeben, sahen wir den größten Nutzen darin, diese Entscheidung der Experten hinsichtlich des „Anfangsverdachts“ zu automatisieren.

Die Automatisierung der Expertenentscheidung wird erst dadurch ermöglicht, dass der überwiegende Teil der Betrugsfälle bestimmten Mustern folgt, allerdings mit einer großen Vielfalt in den Details. So ergeben sich aus der Kombination von Schadenort und Schadenzeit, der Beteiligung bestimmter Fahrzeugtypen am Unfall und Daten zum Versicherungsnehmer und zur Versicherungspolice wichtige Hinweise auf die Betrugswahrscheinlichkeit. Beispielsweise macht es einen großen Unterschied, ob sich ein Unfall nachts in einem Gewerbebetrieb oder am Freitagnachmittag auf einer Hauptstrasse ereignet. Ist der Versicherungsnehmer schon seit Jahren bei der Gesellschaft versichert oder erst seit ein paar Wochen. Wurde ein normales Mittelklassefahrzeug beschädigt oder ein schon etwas in die Jahre gekommenes Luxusfahrzeug, für das Ersatzteile und Reparaturen sehr kostenintensiv sind?

Mit Hilfe einer auf Fuzzy Logik basierenden Software der Firma INFORM ist es möglich, komplexe Entscheidungen auf der Basis menschlicher Erfahrungen und Einschätzungen in EDV-Systemen abzubilden. Ursprünglich ist die Software für die Realisierung flexibler Steuerungen in der Regelungstechnik entwickelt worden und wird von verschiedenen Kreditkartenprozessoren erfolgreich zur Betrugsabwehr eingesetzt. Damit schien die Software grundsätzlich auch gut geeignet für die automatische Betrugserkennung in der Versicherungsbranche zu sein.

### **3. Von der Idee zur Lösung**

#### **3.1. Zielsetzung**

Das primäre Ziel bei der Entwicklung einer Software für die Kraftfahrt-Haftpflichtversicherung war es eine konsistente Qualität der Anspruchsprüfung sicherzustellen, indem alle eingehenden Schadenmeldungen nach einem einheitlichen System einer Prüfung unterzogen werden.

Daneben sollte die Mehrbelastung für die Schadensachbearbeiter durch den Einsatz von RiskShield/ISP-KH möglichst gering sein. Unverdächtige Ansprüche sollten automatisch und möglichst frühzeitig im Bearbeitungsprozess als solche erkannt werden und ohne eine aufwendige weitere Prüfung einer Schnellregulierung zugeführt werden können.

RiskShield/ISP-KH sollte darüber hinaus die unterschiedliche Datenlage in jedem Schadenfall berücksichtigen und selbst bei fehlenden oder unbekanntem Informationen eine Entscheidung treffen können.

Schließlich sollte RiskShield/ISP-KH relativ einfach in die unterschiedlichen DV-Umfelder der Erstversicherer integriert werden können.

#### **3.2. Realisierung**

Zunächst war aber noch das Problem zu lösen, an das Expertenwissen hinsichtlich der Betrugserkennung – über das wir als Rückversicherer nicht verfügten – zu gelangen. Wir lösten diese Aufgabe dadurch, dass wir fünf namhafte deutsche Erstversicherer von den Vorteilen einer gemeinsamen Entwicklung der ersten Komponenten für die Kraftfahrt-Haftpflichtversicherung überzeugten. Diese Komponente, die wir RiskShield/ISP-KH nannten, wurde in etwas mehr als einem Jahr in enger Zusammenarbeit mit der Firma INFORM, den Betrugsexperten der Entwicklungspartner und GeneralCologne Re entwickelt.

Die Aufgabe der Experten bestand im wesentlichen in der Definition der grundsätzlichen Struktur der Entscheidungsregeln, der Bereitstellung und Bewertung der Testfälle, mit denen wir die Feineinstellung der Bewertungsregeln vornahmen und dem abschließenden Test der Regeln. Dank der hohen Flexibilität und Anpassungsfähigkeit der Software waren dafür insgesamt nur sechs - überwiegend eintägige - Treffen mit den Betrugsexperten notwendig.

#### **3.3. Funktionsweise**

RiskShield/ISP-KH ist eine Erweiterung der Schadensysteme der Erstversicherer, die im Hintergrund läuft und damit für die Anwender praktisch nicht sichtbar ist. Bei der Erfassung werden alle Schadenmeldungen durch RiskShield/ISP-KH automatisch auf der Basis der Informationen zu Versicherungsnehmer und versichertem Fahrzeug, zum Unfallhergang und zum Unfallgegner auf ihre Betrugsrelevanz überprüft. Je nach Schwere des Betrugsverdachts wird anhand der von den Unternehmen individuell

vorgegebenen Grenzen entschieden, ob ein Schadenfall normal reguliert oder den Betrugsexperten zur Entscheidung über das weitere Vorgehen vorgelegt wird. Das Ziel der automatisierten Betrugserkennung ist in erster Linie, unverdächtige „weiße Schafe“ zuverlässig als solche zu erkennen und auch bei nicht eindeutiger Sachlage durch ein Abwägen von belastenden und entlastenden Faktoren möglichst viele Fälle in der Schnellbearbeitung zu halten. Den spezialisierten Betrugsexperten sollen dann nur noch diejenigen Fälle vorgelegt werden, bei denen das System eine hohe Betrugswahrscheinlichkeit feststellt.

Die Regeln für die Bewertung des Betrugsverdachts werden mit einem speziellen Werkzeug in umgangssprachlich definierter „Wenn-Dann“-Form hinterlegt. Eine solche Regel könnte beispielsweise lauten: Wenn Verträge schon sehr lange bestehen und keine Vorschäden haben, dann sind sie eher unverdächtig. Umgekehrt sind solche Schadenmeldungen verdächtig, bei denen der Vertrag erst seit kurzem besteht oder bei denen schon zahlreiche Vorschäden auftraten. Der Vorteil dieser umgangssprachlichen Definition von Regeln besteht darin, dass sie von den Experten leicht formuliert werden können und ihre Plausibilität einfach zu überprüfen ist.

Die Verwendung solcher Regeln im Rahmen eines EDV-Systems setzt allerdings voraus, dass qualitative Begriffe wie „alter Vertrag“ aus den vorliegenden Daten - zum Beispiel der bisherigen Laufzeit des Vertrages - automatisch und konsistent ermittelt werden können. Hierfür wird die sogenannte Fuzzy Logik („fuzzy“ ist die englische Übersetzung von „unscharf“) verwendet, die es erlaubt, auch qualitative und unscharfe Begriffe wie zum Beispiel „etwas“ oder „sehr“ logisch konsistent zu verarbeiten. In RiskShield/ISP wird dies unter anderem genutzt, um den verschiedenen Vertragsdauern die qualitativen Begriffe „sehr alt“, „alt“, „jung“ oder „sehr jung“ mit fließenden Übergängen zwischen den einzelnen Begriffen zuzuordnen. In dem Entwicklungswerkzeug stehen hierfür graphische Hilfsmittel zur Verfügung. Diese zeichnen sich zum einen durch eine hohe intuitive Verständlichkeit aus. Zum anderen erlauben sie es, die Zuordnungen schnell und einfach zu verändern. Insgesamt werden im deutschen Marktmodell von RiskShield/ISP-KH 65 Eingangsgrößen mit weit über 250 Entscheidungsregeln verknüpft. Das System ist für Außenstehende kaum zu durchschauen; dadurch besteht nur ein geringes Risiko, dass Betrüger die Regelsystematik erkennen und überlisten.

## **4. Vorteile von RiskShield/ISP**

### **4.1. Geringe Folgekosten**

Sobald RiskShield/ISP in den EDV-Systemen der Erstversicherer eingebaut ist, können Änderungen und Anpassungen der Regeln leicht von der Fachabteilung vorgenommen werden, ohne hierfür die Unterstützung der IT-Abteilung zu benötigen (dies gilt natürlich nur, sofern keine neuen Entscheidungsgrößen berücksichtigt werden). Die Betrugserkennung zeichnet sich dadurch aus, dass häufig solche kleinen Änderungen und Anpassungen vorgenommen werden müssen, da es eine Strategie der Betrüger ist, die Details der Betrugsmuster zu verändern, um einer Erkennung durch starre EDV-Systeme zu entgehen.

### **4.2. Flexible Anpassung an vorhandene EDV-Systeme**

RiskShield/ISP hat darüber hinaus den Vorteil, gut auf unterschiedliche Datenverfügbarkeit und Datenqualität einstellbar zu sein. So stellen fehlende oder unbekannte Eingangsdaten kein Problem dar. Grundsätzlich kann das System – im Gegensatz zu herkömmlichen Expertensystemen – mit nur einer Eingangsinformation eine Entscheidung treffen; diese dürfte dann natürlich nur eine sehr begrenzte Aussagekraft haben. Von den oben genannten 65 Eingangsdaten benötigt RiskShield/ISP-KH nur etwa 25 Daten, um eine sinnvolle Entscheidung zu treffen. Zusätzliche Informationen verbessern lediglich die Entscheidungsqualität.

## **5. Aktueller Entwicklungsstand**

### **5.1. Module für die Kraftfahrt-Versicherung**

Die Entwicklung der Regeln für die Betrugserkennung in der Kraftfahrt-Haftpflicht-Versicherung waren im Mai 1999 abgeschlossen. Die Tests zeigten, dass die Bewertung von RiskShield/ISP-KH bei einer mittleren Datenlage (rund 30 Angaben zum Schadenfall, von denen aber zwei Drittel bereits in den Schadensystemen vorhanden sind) in über 90% der Fälle mit der Beurteilung der Experten übereinstimmt.

Dem sofortigen Einsatz von RiskShield/ISP-KH stand das Problem entgegen, dass die Schadensysteme der Entwicklungspartner keine bzw. fast keine Informationen zum Schadenhergang und zum Fahrzeug des Anspruchstellers enthielten. Diese Angaben sind aber für die Bewertung des Betrugsverdachts bei Kraftfahrt-Haftpflicht-Schäden unverzichtbar. Es dauerte daher bis Ende des Jahres 2000, bis die Systeme bei unseren Kunden um die erforderlichen 5 - 10 Datenfelder erweitert waren. Anschließend waren noch die Regeln von RiskShield/ISP-KH auf die unternehmensindividuelle Datenlage und Arbeitsabläufe hin zu optimieren.

Die Anwender, die die Optimierung inzwischen abgeschlossen haben, berichten über eine sehr gute Erkennungsqualität. Durch RiskShield/ISP-KH werden 8 - 10% aller Kraftfahrt-Haftpflicht-Schäden oberhalb eines vom Kunden festgelegten Punktwertes als betrugsverdächtig angesteuert. Einige Unternehmen lehnen etwa zwei Drittel dieser Ansprüche nach einer weiteren Prüfung des Sachverhalts durch spezialisierte Sachbearbeiter erfolgreich ab.

RiskShield/ISP-KH wird ständig weiterentwickelt und auf die individuellen Bedürfnisse und Datenlage der Kunden angepasst. Inzwischen ist unsere Lösung bei nahezu allen großen Erstversicherungsgesellschaften in Deutschland im Einsatz bzw. befindet sich in der Integrationsphase.

Parallel zum Einbau der Kraftfahrt-Haftpflicht-Komponente entwickelten wir in einer weiteren Entwicklungsgemeinschaft ein Modul für die Bewertung von Schäden in der Kraftfahrt-Kasko-Versicherung. Diese Sparte erwies sich als deutlich komplexer. Inzwischen ist es uns gelungen, die außerordentliche Vielfalt der Sachverhalte und Betrugsmotive in einem praxisgerechten System zu bewältigen. Die ersten Auslieferungen sind bereits Anfang 2001 erfolgt. Da die Entwicklungspartner durch den Einbau von RiskShield/ISP-KH und der damit einhergehenden Anpassung ihrer Arbeitsabläufe zeitlich sehr eingebunden waren, werden die Kasko-Module bei den Unternehmen erst jetzt integriert bzw. befinden sich in der letzten Phase der Feinabstimmung des Regelwerks.

### **5.2. Module für weitere Sparten**

Dem Wunsch unserer Kunden folgend, wollen wir für alle Nicht-Lebenssparten entsprechende Betrugsmodule anbieten. Die vorbereitenden Arbeiten für die

Komponenten in der Sachversicherung und der Allgemeinen Haftpflichtversicherung zeigten aber, dass der potentielle Nutzen von RiskShield/ISP in diesen Sparten insbesondere dann realisiert werden kann, wenn das System in größerem Maße zur Unterstützung der gesamten Sachverhaltsermittlung und -bewertung eingesetzt wird. Hierzu ist es notwendig, dass RiskShield/ISP nicht nur zu einem sehr frühen Zeitpunkt im Schadenprozess eine Entscheidung trifft sondern vielmehr den gesamten Schadenbearbeitung begleiten muss. Dies setzt aber eine engere Abstimmung der Software auf die individuellen Bedingungen und Arbeitsabläufe der einzelnen Unternehmen voraus.

Die Entwicklung unserer Module für die Betrugserkennung in der Sachversicherung werden wir voraussichtlich im Laufe des Jahres 2003 abschließen können. In einem ersten Schritt bieten wir für die Bereiche Leitungswasser, Brand, Überspannung, Einbruch-Diebstahl sowie Fahrraddiebstahl geeignete Lösungen an.

Darüber hinaus sieht unsere derzeitige Planung vor, mit der Entwicklung einer Komponente für den Privathaftpflicht Bereich zusammen mit interessierten Unternehmen im ersten Quartal 2004 zu beginnen.

### **5.3. Entwicklung einer kompletten Schadensoftware**

Die bisherige Erfahrung zeigt, dass häufig das entscheidende Problem, das vor dem Einsatz von RiskShield/ISP zu lösen war, die begrenzte Datenbasis der bestehenden Schadensysteme ist. Einige unserer Kunden entschieden sich dafür, die von RiskShield/ISP-KH benötigten Daten in ihre bestehenden Schadensysteme aufzunehmen. Für andere Unternehmen war dies keine sinnvolle Vorgehensweise, da deren Schadensysteme grundlegend überarbeitet werden müssen und weitere Investitionen in die Altsysteme nicht zu rechtfertigen waren.

Wir entwickelten daher zusammen mit unserem Softwarepartner INFORM ein Konzept für eine modulare Schadensoftware auf Basis moderner EDV-Technologie, die eine zeitlich gestufte Ablösung der alten Schadensysteme erlaubt. Ziel ist es, die Unternehmen in die Lage zu versetzen, schrittweise unter vorübergehender Verwendung der alten Teilsysteme und Datenbanken ein modernes Schadenbearbeitungssystem für alle Nicht-Lebenssparten aufzubauen, das unter anderem auch die entsprechenden Module für die Betrugserkennung nutzen wird. Das Konzept basiert auf dem Einsatz moderner Softwarearchitektur, die es erlaubt, unternehmensübergreifende Branchenlogik in mehrfach verwendbaren Fach-Modulen und unternehmensindividuelle Bildschirmoberflächen und Abläufe in leicht veränderbarer Standardsoftware zu realisieren. Das Ergebnis sind weitgehend individuelle Systeme, die zum Preis einer Branchensoftware schrittweise und mit begrenztem Risiko eingeführt werden können.

Der erste Kunde hat sich für die Realisierung eines Systems für die Schadenbearbeitung in der Kraftfahrt-Versicherung (Haftpflicht und Kasko) entschieden. Im Anschluss ist dann die Erweiterung auf ein spartenübergreifendes

System durch die Einbeziehung der Allgemeinen Haftpflicht- und der Sachversicherung geplant.

#### **5.4. Erfahrungen im Ausland**

Da die Regeln von RiskShield/ISP leicht zu verändern sind, planten wir von Anfang an, das System auch im Ausland anzubieten. Unsere Zielsetzung ist dabei, mit dem Werkzeug und unter Nutzung der in Deutschland gemachten Erfahrungen für die einzelnen Märkte jeweils individuelle Module zu erstellen, die speziell auf die Betrugsmuster in den einzelnen Ländern abgestimmt sind. Als ersten Erfolg dieser Strategie konnten wir Ende 2000 ein Modul für die Betrugserkennung in der Kraftfahrt-Haftpflicht-Versicherung in Italien fertig stellen und an die ersten beiden Kunden ausliefern. Dieses Modul vermarkten wir derzeit aktiv in Italien.

In der Schweiz haben wir ebenfalls ein Versicherungsunternehmen gewinnen können, mit dem wir zur Zeit die letzten Anpassungen an den Schweizer Motorfahrzeugversicherungsmarkt vornehmen. Wir gehen davon aus, dass die RiskShield/ISP-Module sowohl für die Kraftfahrthaftpflicht- als auch für die Kaskoversicherung noch in diesem Jahr in Produktion gehen.

Darüber hinaus besteht großes Interesse in England, Irland und Spanien. Versicherungsgesellschaften aus nahezu dem gesamten europäischen Ausland testen oder haben bereits im Internet (nach Freischaltung durch GeneralCologne Re) die deutschen Regeln von RiskShield/ISP getestet. Wir hoffen im laufenden Jahr auch in Spanien, Irland und Frankreich in Zusammenarbeit mit interessierten Unternehmen mit der Entwicklung der jeweiligen nationalen Module beginnen zu können.

Erste Präsentationen in den USA zeigen, dass RiskShield/ISP auch für den nordamerikanischen Markt grundsätzlich geeignet ist und auf großes Interesse stößt. Wir werden daher noch in diesem Jahr verstärkt versuchen, erste Unternehmen von einer gemeinsamen Entwicklung einer Version für die Betrugserkennung in den USA zu überzeugen.

## 6. Erfahrungen und Konsequenzen

Bei der Entwicklung von RiskShield/ISP-KH und Kasko haben wir angenommen ein Entscheidungssystem zu entwickeln, das in nahezu unveränderter Form bei allen Versicherungsgesellschaften eines Marktes zum Einsatz kommen kann. Die Individualisierung der Software sollte von den Entwicklungspartnern bzw. Neu-Kunden selbst vorgenommen werden.

Wir mussten jedoch feststellen, dass nahezu alle Entwicklungspartner sowohl bei der Integration als auch bei der anschließenden Regeloptimierung unsere Unterstützung benötigten. Die Gründe waren im wesentlichen zwei Bereichen zuzuordnen:

- Die Datenlage in den Versicherungsunternehmen wich zum Teil deutlich voneinander ab. Einige Eingangsgrößen des Marktmodells waren überhaupt nicht vorhanden dafür aber andere Größen, deren Überprüfung aus Betrugssicht durchaus sinnvoll ist. Darüber hinaus unterschieden sich die Ausprägungen vorhandener Eingangsgrößen von den im Schadensystem verwendeter Ausprägungen. In jedem Fall bedurfte es einer Anpassung des Regelsystems.
- Die mit der Regeländerung bzw. Regelanpassung betreuten Schadenspezialisten waren nach wie vor mit ihrer täglichen Arbeit voll ausgelastet. Damit war es ihnen kaum möglich, sich regelmäßig mit dem Entscheidungssystem auseinander zusetzen. Im Ergebnis führte dies bei den Schadenspezialisten trotz Schulung und einfacher Handhabung zu einer Verunsicherung im Umgang mit der Software. Diese Unsicherheit gipfelte letztlich in der Sorge durch eine Regeländerung das Entscheidungssystem so zu verändern, dass eine zu große Anzahl von Schadenfällen angesteuert oder das Entscheidungssystem unbrauchbar wird.

Aufgrund dieser Erfahrungen haben wir den gesamten Prozess der Individualisierung des Marktmodells bei allen weiteren Kunden von Beginn an intensiv betreut. Ausgehend vom deutschen Marktmodell werden in einem ersten Schritt mit den Schadenspezialisten/Betrugsexperten und IT-Fachleuten des Kunden sowohl die Eingangsgrößen als auch die Ausprägungen auf die individuelle Datenlage hin definiert. Gleichzeitig werden die noch im Schadensystem nachzupflegenden Eingangsgrößen festgelegt. In einen weiteren Schritt werden die Betrugsregeln und deren Gewichtung mit den Schadenspezialisten/Betrugsexperten des Kunden diskutiert und durch uns in ein Regelwerk eingebracht. Anschließend wird dieses Regelsystem noch unter zu Hilfenahme von Schadenfällen und zusätzlicher Analysen durch uns optimiert. Im Ergebnis erhält jeder Kunde ein auf seine individuellen Bedürfnisse und auf seine Datenlage hin optimiertes Entscheidungssystem.

Abgeschlossen wird die Einführung von RiskShield/ISP durch eine mehrtägige intensive Schulung der mit der Regelentwicklung/-wartung betrauten Schadenspezialisten/Betrugsexperten.

Während der Diskussionen mit unseren Kunden hinsichtlich der rein technischen Integration von RiskShield/ISP wurden wir zunehmend auch mit Fragen bezüglich der ablaforientierten Integration von RiskShield/ISP konfrontiert. Unsere Kunden benötigten unsere Unterstützung bei der Lösung von Fragen wie zum Beispiel :

- Wie soll die Bearbeitung der durch RiskShield/ISP als auffällig gekennzeichneten Schadenfällen aussehen?
- Welche der möglichen Integrationsvarianten von RiskShield/ISP in den bestehenden Schadenworkflow stiftet den höchsten Nutzen?
- Wie gehen andere Versicherungsunternehmen mit RiskShield/ISP um?
- Wann ist der beste Bewertungszeitpunkt für RiskShield/ISP?

Die Beantwortung dieser Fragen ist sehr stark von den unternehmensindividuellen Gegebenheiten und der strategischen Ausrichtung abhängig und fällt daher sehr unterschiedlich aus. Neben diesen allgemeinen Fragen zur ablaforientierten Integration von RiskShield/ISP, analysieren wir zunächst den Schadenbereich unseres Kunden und entwickeln dann gemeinsam mit ihm eine effiziente Lösung. Bei unserer Analyse stehen im wesentlichen die nachstehenden Fragen im Mittelpunkt:

- Handelt es sich um einen Direktversicherer, der ein Callcenter zur Schadenaufnahme einsetzt oder eher um ein Versicherungsunternehmen, das auf „traditionelle“ Weise Schäden bearbeitet?
- Welche Informationen zu einem Schadenfall stehen wann zur Verfügung?
- Wie ist die Betrugsbearbeitung derzeit organisiert und wie soll diese zukünftig aussehen? Gibt es eine zentrale Betrugsabteilung oder sind die Betrugsspezialisten über alle Niederlassung verteilt?
- Wie viele Betrugsexperten gibt es bzw. welche Bearbeitungskapazitäten stehen zur Verfügung?

Wir können heute unser umfassendes Knowhow hinsichtlich Betrugsbearbeitung im Allgemeinen und RiskShield/ISP im Besonderen, welches wir in den letzten Jahren bei unseren Kunden gesammelt haben, allen unseren Kunden zugänglich machen. Darüber hinaus fließen diese Erfahrung auch in die laufende Weiterentwicklung und Optimierung unserer RiskShield/ISP-Module ein.

## 7. Weitere Erkenntnisse

Der für uns erstaunlich schnelle Erfolg von Riskshield/ISP zeigt, dass die Versicherungswirtschaft in der Lage und Willens ist, neue Lösungen aufzunehmen und umzusetzen. Andererseits stießen wir an Grenzen, die für uns unerwarteten und auf den ersten Blick kaum verständlich waren:

- Bei mehreren Unternehmen eine eher geringe Bereitschaft, das Thema Versicherungsbetrug offensiv und konsequent anzugehen und
- bei zahlreichen Unternehmen eine unzureichende Datenbasis und eine sehr einseitige Behandlung der Frage, welche und wie viele Daten in den Schadensystemen erfasst und vorgehalten werden sollen.

### 7.1. Eingeschränkte Wahrnehmung von Versicherungsbetrug

Die Mehrzahl der Versicherungsunternehmen in Deutschland (wie auch in Europa) hat spezialisierte Abteilungen oder Referate, die betrügerischen Versicherungsfällen nachgehen. Aber nur bei wenigen Unternehmen verfügen diese Stellen auch über eine angemessene Ausstattung mit Mitarbeitern, häufig werden die Abteilungen von der Unternehmensleitung eher geduldet als konsequent unterstützt.

Die Ursachen für diesen zurückhaltenden Umgang mit dem Phänomen „Betrug“ liegen aus unserer Sicht in der Einschätzung von Versicherungsbetrug als „Kavaliersdelikt“, in der breiten Öffentlichkeit ebenso wie in den Versicherungsunternehmen. Hauptgrund dürfte aber die falsche Einschätzung des „Kosten-Nutzen-Verhältnisses“ einer konsequenten Betrugsbekämpfung durch die Unternehmensleitungen sein. Diese Fehleinschätzung bezieht sich sowohl auf die Kosten als auch den Nutzen:

- Die potentiellen Probleme mit Kunden und Außendienst werden nach unserer Erfahrung überschätzt. Mit Hilfe von RiskShield/ISP erfolgt die Bewertung der Betrugswahrscheinlichkeit sehr präzise, da neben belastenden auch entlastende Faktoren berücksichtigt werden. Bei ausreichender Datenbasis ist die Gefahr einer falschen Einschätzung der Betrugswahrscheinlichkeit folglich sehr gering. Die endgültige Entscheidung über die Ablehnung einer Entschädigung fällt zudem ein menschlicher Experte, und zwar nur dann, wenn er von dem betrügerischen Charakter und den Erfolgsaussichten einer Ablehnung überzeugt ist.
- Weiterhin werden die Kosten des Betrugsnachweises überschätzt. Die hohe Treffsicherheit von RiskShield/ISP führt bislang dazu, dass bei einem überraschend hohen Anteil der als unberechtigt abgelehnten Schäden die Anspruchsteller die Ablehnung ohne weitere Rückmeldung hinnehmen, so dass keine zusätzlichen Kosten für einen Betrugsnachweis entstanden.
- Schließlich wird häufig auch verkannt, wie häufig und vor allem auch wie teuer betrügerische Schadenmeldungen sind. Nach unseren bisherigen Erfahrungen

dürften die veröffentlichten Schätzungen über die finanziellen Auswirkungen von Versicherungsbetrug von der Realität weit überschritten werden.

Insgesamt führt dies zu einer deutlichen Unterschätzung des Einsparungspotentials einer konsequenten Betrugsbekämpfung, die dieses Thema aus Sicht des Topmanagements eher zu einer Nebensächlichkeit werden lässt. Diejenigen unserer Kunden, die Betrug konsequent und engagiert bekämpfen, berichten von beeindruckenden Ergebnissen wie „Einsparungen in Millionenbereich“ (ein großer Versicherer). Ein kleiner Direktversicherer überprüft intensiv 2% aller KH-Schäden und hat eine Nettoersparnis von Euro 2.700 pro intensiv bearbeitetem Schaden. Verzichtet ein Unternehmen auf die Realisierung dieser Einsparpotentiale, dürften sich auf Dauer negative Auswirkungen auf die Marktstellung des Unternehmens ergeben.

Wir gehen davon aus, dass in Zukunft bei einem vermutlich anhaltenden Wettbewerbs- und Kostendruck mehr und mehr Versicherungsunternehmen zu einer konsequenten Betrugsbekämpfung übergehen werden.

## **7.2. Unterschätzter Wert von Daten**

Das Haupthindernis der Einführung und konsequenten Nutzung von RiskShield/ISP war bzw. ist die unzureichende Datenlage der Schadensysteme. Diese „sehr dünne Datenlage“, die wir bei allen unseren Kunden vorfanden, ist unserer Einschätzung nach Konsequenz einer fehlgesteuerten Reduzierung der Schadenbearbeitungskosten.

Über den Datenumfang der Schadensysteme wurde und wird primär unter Kostengesichtspunkten entschieden: Ziel ist es, nur die unbedingt notwendigen Daten zu erfassen, um den damit verbundenen Aufwand zu minimieren. Die „Übertreibung“ dieses grundsätzlich richtigen Vorgehens führte aber zu Schadensystemen, die praktisch nur bessere Buchhaltungssysteme sind, d.h. sie enthalten über die zahlungsrelevanten Angaben hinaus kaum schadenbezogenen Daten. Außerdem sind diese wenigen Daten – vermutlich als Folge der hohen Arbeitsbelastung in den Schadenabteilungen - häufig von einer erschreckend geringen Qualität, also unvollständig, widersprüchlich oder einfach falsch.

Der systematische Fehler, den unserer Einschätzung nach sehr viele Versicherungen machten und zum Teil auch noch machen, besteht darin, den „Wert“ von Schadendaten nicht oder nicht vollständig zu erkennen. Folglich wird dieser Aspekt bei der Gestaltung von Schadensystemen nicht angemessen berücksichtigt. Dies führt in der Konsequenz zu einer quantitativ und qualitativ ungenügenden Datenbasis für

- Kostencontrolling und Schadenmanagement,
- Betrugserkennung sowie
- Produktgestaltung und Underwriting.

Die Bedeutung einer guten Datenbasis kommt allerdings mehr und mehr ins Bewusstsein der Unternehmen. Wegen des nach wie vor anhaltenden Kostendrucks ist die naheliegende Lösung, mehr Personal einzustellen um zusätzliche Daten zu erfassen, nicht oder nur teilweise möglich. Der einzig gangbare Ausweg besteht unserer Einschätzung nach darin, die inzwischen verfügbaren neuen IT-Technologien gezielt und konsequent dazu zu nutzen, Daten effizient und kostengünstig zu erfassen. Ansatzpunkte hierfür sehen wir vor allem in den Bereichen

- Durchgängige Nutzung einer Oberfläche für alle Bearbeitungsschritte
- Anwendergerechte Steuerung der Bildschirmdialoge
- Aufgaben- bzw. systemübergreifende Verwendung von Daten
- Flexible und fallabhängige Festlegung der Mussfelder
- Fallabhängige Vorbelegung der Eingabefelder
- Flexible und fallabhängige Plausibilitätsprüfung
- Flexible Bewertung der Datenqualität

Die besondere Herausforderung ist dabei, die Systeme so zu gestalten, dass sie sich flexibel und automatisch möglichst weitgehend an die sehr unterschiedliche Komplexität der Schäden anpassen können. Die Aufgabe besteht darin, bei einfachen Schäden nur wenige Daten und bei komplizierten Schäden gezielt die zusätzlich erforderlichen Informationen zu erfassen.

Es ist klar, dass diese zusätzliche Funktionalität nicht mehr im Rahmen einer Erweiterung der bestehenden Schadensysteme zu realisieren ist. Damit stehen die Unternehmen vor der großen Herausforderung, eine Ablösung der Altsysteme möglichst kostengünstig, schnell und mit minimalen Risiken zu bewältigen. Die dafür bislang verfügbaren Optionen, entweder eigenständige Neuentwicklung oder Kauf und Anpassung einer bestehenden Standardanwendung, entsprachen einer „Wahl zwischen Pest und Cholera“: Auf der einen Seite Aufwand und Komplexität jahrelanger Entwicklungsarbeiten an einem eigenen System, auf der anderen Seite Risiken und Kosten einer kurzfristige Ablösung im Rahmen eines „Big-Bang“.

Dank der inzwischen verfügbaren neuen Möglichkeiten der IT-Technologie gibt es einen Mittelweg, den wir für erfolgversprechend halten: Eine schrittweise Ablösung unter Verwendung von „vorgefertigten Standardmodulen“, die kostengünstig an die individuellen Anforderungen der Unternehmen angepasst werden können. Diese Vorgehensweise erlaubt, die vorhandenen Schadensysteme und insbesondere deren Schnittstellen zu den anderen Anwendungen (z.B. Bestandssystem, Partnersystem, Exkasso einschließlich Buchhaltung) in einem beliebig langen Parallelbetrieb mit zu

nutzen. Im Rahmen weiterführender Projekte mit Kunden von Riskshield/ISP machen wir derzeit erste Schritte auf diesem Weg.