Datenaustausch zur Betrugsprävention – Anforderungen und Lösungen

Entwicklung des Deutschen Schutz-Portals

Dirk Mayer

Deutschland geriet in den letzten Jahren immer mehr in den Fokus unternehmerischer Betrüger. Dabei traten enorme Schäden auf. Die Spitze des Eisbergs bilden Namen wie Flowtex und Parmalat, gefolgt von jüngeren Skandalen wie die der Erfurter Eliog-Gruppe, der Delitzscher Schokoladenfabrik, der Eisenberger Wurstwaren und des Finanzdienstleisters Infinus. Mit einem von der Wirtschaftsauskunftei Bürgel entwickelten neuen Portal zur Betrugsprävention dürfte sich das bald ändern.

Intensivbetreuung oder Revision finden immer wieder viele „Fehler“ in der Antragsprüfung. Oft scheint es schwer verständlich, wenn Mitarbeiter Unstimmigkeiten oder Verbindungen zu anderen Fällen nicht sehen. Der Verlust wirkt in der Rückschau vorhersehbar. Das Wissen um einen Rückstand oder Ausfall macht es leichter, Irrtümer und fehlerhafte Annahmen zu erkennen. Die Spezialisten arbeiten auch unter anderen Voraussetzungen als der Kreditprüfer, der einen Antrag unter Zeitdruck möglichst positiv entscheiden soll. Die notleidenden Kredite betreffen regelmäßig mehrere Institute. Die Verbindung zeigt sich dabei nicht zwingend über den Antragsteller: Schadensfälle decken sich in Kontaktdaten oder Bankverbindungen. Dubiose Ausfälle finden sich an der gleichen Adresse. Mehrere Banken finanzieren die gleichen Kraftfahrzeuge oder Maschinen.

Diese Kreditentscheidungen basieren auf Irrtümern über die Zahlungswilligkeit oder Zahlungsfähigkeit des Kunden. Nur für die Beitreibung ist es noch relevant, ob die Ausfälle durch Nichtbeachtung bestehender Regelungen bei der Herauslage, einen „Firmenbeerdiger“ oder einen professionellen Betrüger verursacht wurden. Handelt es sich um eine vorsätzliche Irrtumserzeugung, spricht man von Betrug.

Paragraf 25 h Kreditwesengesetz (KWG) schreibt vor, dass Institute angemessene Systeme betreiben sollen, mit denen sie Geldwäsche, Terrorismusfinanzierung und sonstige strafbare Handlungen erkennen. Unter die sonstigen strafbaren Handlungen fällt an erster Stelle der Betrug. Finanzdienstleister sollen also über Systeme zur Betrugsvermeidung verfügen. Zur Identifizierung dieser Straftaten dürfen sie sich untereinander austauschen.

Die Wirklichkeit entspricht kaum den Ansprüchen des Gesetzgebers. Nur wenige Banken, Leasing-Unternehmen und andere Finanzdienstleister setzen effiziente Systeme zur Betrugsprävention ein. Große Schadensfälle gelten häufig als unvermeidbare Ausnahme. Als Betrug erkannte Ausfälle im Mengengeschäft untersuchen Banken zwar systematischer, doch auch dort fehlt oft eine Unterstützung durch die IT. Betrugsprävention funktioniert anders als die Bewertung der Bonität. Die lange bekannte Tatsache findet beim Aufbau neuer Systeme jedoch nur selten Berücksichtigung.

Dabei treten enorme Schäden auf. Die Spitze des Eisbergs bilden medienwirksame Katastrophen wie in den 1990er-Jahren bei der Flowtex Technologie GmbH & Co. KG im badischen Ettlingen oder 2003 bei dem italienischen Lebensmittelkonzern Parmalat (Molkereiunternehmen). Im mittleren Segment tauchen jedes Jahr einige Fälle in den Medien auf – in Deutschland zum Beispiel die Erfurter Eliog-Gruppe mit einem offiziellen Schaden von mindestens 25 Millionen Euro; die Delitzscher Schokoladenfabrik mit 4,5 Millionen. Der Finanzdienstleister Infinus verursachte einen Schaden in dreistelliger Millionenhöhe; die Eisenberger Wurstwaren 4,5 Millionen. Die Reihe lässt sich fortsetzen.

Unter der medienpräsenten Oberfläche bewegt sich eine nahezu unbekannte Gefahr. Die Berichte beziehen sich auf existente Firmen. Diese versuchen, sich durch eine aktive Kommunikation reinzuwaschen. Über den

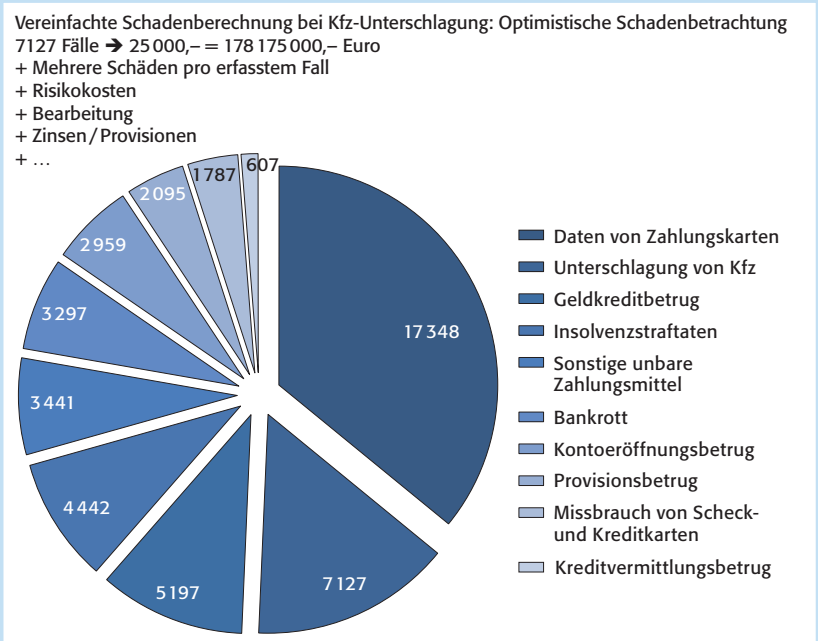
DER AUTOR:

Dirk Mayer, Hamburg,

ist Bankkaufmann und startete im klassischen Filialgeschäft. Bei der ersten reinen Internetbank Europas war er für den Aufbau der Kreditabteilung zuständig. Ab 2005 beriet er Finanzdienstleister und E-Commerce-Unternehmen. 2013 wechselte er zur Auskunftei Bürgel.

E-Mail: dirk.mayer@buergel.de

Abbildung 1: Delikte



Quelle: Polizeiliche Kriminalstatistik 2014

professionellen Missbrauch von Firmenmantelgesellschaften oder betrügerisch eröffnete GmbHs findet sich kaum eine Nachricht. Die Opfer fürchten einen möglichen Reputationsschaden; die Polizei Nachahmer. Den Medien fehlt nicht nur das Wissen, sondern auch ein Ansprechpartner.

Die Polizeiliche Kriminalstatistik (PKS) bietet nur wenige Anhaltspunkte für die wahren Ausmaße. Die Statistik der Kriminalisten unterscheidet nicht zwischen natürlichen Personen und Firmen. Die aus polizeilicher Sicht sinnvolle Bündelung von Anzeigen in einem Fall verdeckt die korrekten Zahlen. Verluste entsprechen aufgrund der Systematik in der Fallerfassung nicht den realen Kosten. Und bei weitem nicht alle Straftaten werden angezeigt.

Die Rubrik „Unterschlagung von Kfz“ in der Abbildung 1 lässt zumindest eine grobe Abschätzung eines Delikts zu, da die Fälle großteils auf Finanzierer zurückgehen. Dies lässt die Macht der Bedrohung erahnen: Mit sehr optimistischen Annahmen ergibt sich aus den 7127 Fällen mindestens ein Schaden von 178 Millionen Euro für das Jahr 2014. Das Dunkelfeld bewegt sich zwischen 250 Millionen Euro und einem Vielfachen davon.

Die Problematik

Mit standardisierten und teilweise automatisierten Abläufen verbessern Finanzdienstleister seit den 1980er-Jahren laufend ihre Prozesse. Dazu kommt die Umstellung auf statistische Verfahren zur Risikobewertung, um Entscheidungen zu optimieren und Risiken nach Vorgaben der Regulierungsbehörden zu bewerten.

Diese Verfahren bilden eine ideale Ausgangslage für Betrüger. Sie überlisten die automatisierten Systeme und Verfahren, indem sie Lücken ausnutzen oder die Daten gestalten. Statistische Prognosen setzen voraus, dass Entwicklungen in der Zukunft denen der Vergangenheit entsprechen. Ein Täter ändert bei einer Ablehnung jedoch sein Vorgehen. Es gibt für professionelle Betrüger keinen Grund, einen neuen Versuch mit den gleichen Daten zu starten; sie agieren dynamisch. Im besten Fall erläutert ein kundenfreundlicher Berater die Gründe für die Entscheidung. Der Täter passt dann die vorgelegten Informationen dem Wunsch des Instituts an. Dies entzieht den analytischen Modellen die Grundlage, eine falsche Risikokategorie wird prognostiziert. Andere Lücken finden sich vor allem bei der Überprüfung von Informationen. Professionelle Betrüger nutzen die vorhandene Bonität von Firmenmänteln, fälschen Webseiten, Bilanzen und Rechnungen.

Betrugsprävention basiert auf heuristischen Regeln. Heuristik ist die Kunst, mit wenigen Informationen gute Entscheidungen zu treffen. Im Alltag der Kreditprüfung zeigt sich das in der Erfahrung der Mitarbeiter, die richtigen Daten zu prüfen. Die Kreditprüfer entwickeln ein Bauchgefühl für Auffälligkeiten. Dieses Fachwissen geht der Branche nach und nach verloren. Erfahrene – und damit häufig ältere und teurere – Kreditexperten gehen, ohne ihr Wissen weiterzugeben. Die standardisierten Prozesse und Funktionstrennungen reduzieren den Wissensaufbau bei neuen Mitarbeitern in der Sachbearbeitung.

Liegen die Schäden im Dunkelfeld, erhalten IT-unterstütze Präventionssysteme keine ausreichende Priorität (Abbildung 2, Seite 225). Viele Institute verharren daher in den bewährten Entscheidungsprozessen. Das Bewusstsein, dass die Gegenspieler sich angepasst haben und Lücken ausnutzen, wächst nur langsam.

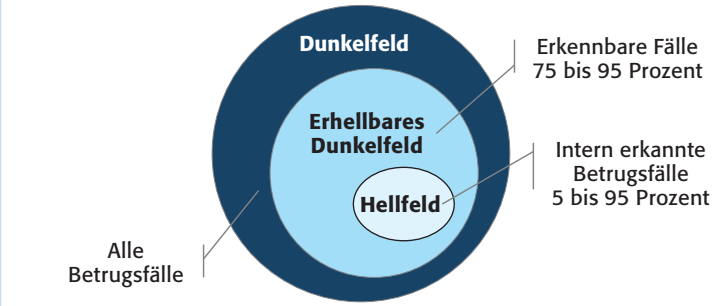
Diese Priorität ändert sich voraussichtlich mit den kommenden Prüfungen der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin). Bei Beanstandungen an den Risikopräventionssystemen greift der 2014 in Kraft getretene § 54 a. Die Prüfungsergebnisse bekommen mit den neuen Strafvorschriften, die direkt auf die Führungsebene zielen, eine andere

Qualität. Das Gesetz bedroht fahrlässige Geschäftsführer und Vorstände mit Freiheitsstrafen bis zu zwei Jahren.

Der bisher praktizierte Austausch unter den Instituten hat bekannte Schwächen. Die Kommunikation beschränkt sich meist auf Schadensfälle. Professionelle Betrüger sehen die genutzten Daten zu diesem Zeitpunkt bereits als „verbrannt" an und verwenden diese nicht mehr. Entsprechend reduzieren viele Meldungen bestenfalls Schäden bei den Engagements existenter Firmen. Ob dabei alle nach den gleichen Spielregeln einmelden, bleibt bei den bestehenden Systemen unklar. Einige Institute erkennen die Vorteile der gegenseitigen Information und bieten ihr Wissen aktiv an. Andere ziehen nur, ohne selbst zur Reduzierung der Gefahr beizutragen. Besteht die Verbindung bei Betrugsfällen nur in Teildaten, wie Konto- oder Telefonnummer, reichen die übermittelten Informationen für eine Identifizierung eigener Kunden dazu meist nicht aus. Teilweise fehlt den Instituten auch die Infrastruktur, um nach anderen Daten als Name oder Adresse zu suchen.

Erschwerend kommt besonders im B2B-Geschäft dazu, dass die Schadensbegrenzung im eigenen Haus Vorrang hat. Die Reaktion, dem Kunden einen Wechsel nahezulegen und damit das eigene Engagement schnell zu reduzieren, treibt den Gesamtschaden durch Folgetaten in die Höhe. Ein Spiel mit wechselnden Verlierern.

Abbildung 2: Betrugsfälle



Hellfeld: Anzahl der intern als Betrug klassifizierten Anträge/Verträge.
Dunkelfeld: Anzahl aller Betrugsfälle im Bestand.
Erhellbares Dunkelfeld: Anzahl der Betrugsfälle, die mit einer Dunkelfeldanalyse als betrügerisch identifiziert werden können.

Quelle: Bürgel Wirtschaftsinformationen

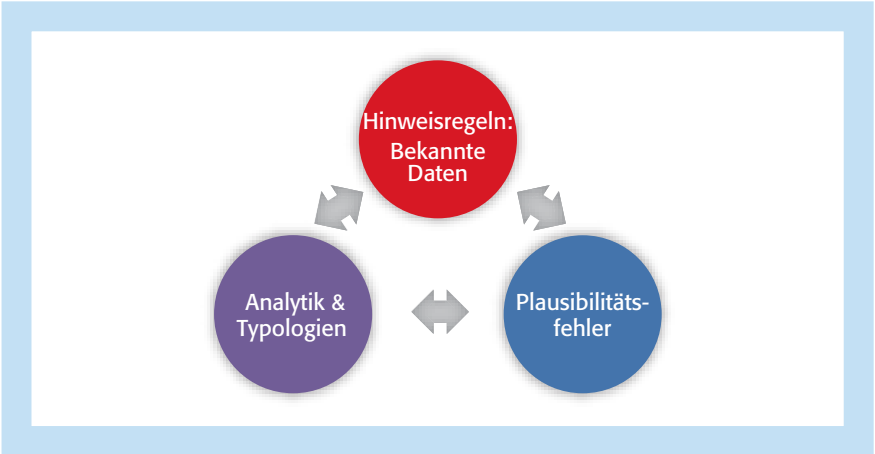
Lösungsentwicklung

Die Lösung kommt von den Konsumentenkreditbanken. Die Ausweitung der quasi-anonymen Kreditvergabe und Kontoeröffnung über das Internet konfrontierte die Online-Banken Anfang der 2000er-Jahre mit massiven Betrugsversuchen. Die neue Kommunikationskultur in den Aus- und Neugründungen erlaubte aber auch einen neuen, lösungsorientierten Austausch. Und es gab offensichtliche Überschneidungen: Professionelle Betrüger schädigen im Durchschnitt fünf bis sechs Institute. Je nach Produkt und Prozess werden 50 bis mehr als 95 Prozent aller Betrugsversuche im Antragsprozess identifiziert, allerdings nur bei wenigen Banken konsequent angezeigt. Die Warnmeldungen an andere Banken umfassen nur Bruchteile der Gesamtmenge. Ablehnungen basieren nicht selten auf Verdachtsmomenten, die dafür nicht ausreichend erscheinen.

Die beteiligten Banken bauten Regelwerke zur Wiedererkennung von Daten aus Betrugsversuchen in ihren Entscheidungssystemen auf. Mangels gemeinsamer Datenbestände blieb die Wirksamkeit natürlich beschränkt. Teilweise bestehen auch technische Schwierigkeiten, erkannte Regeln in den auf Bonitätsbeurteilung ausgelegten Systemen einzusetzen.

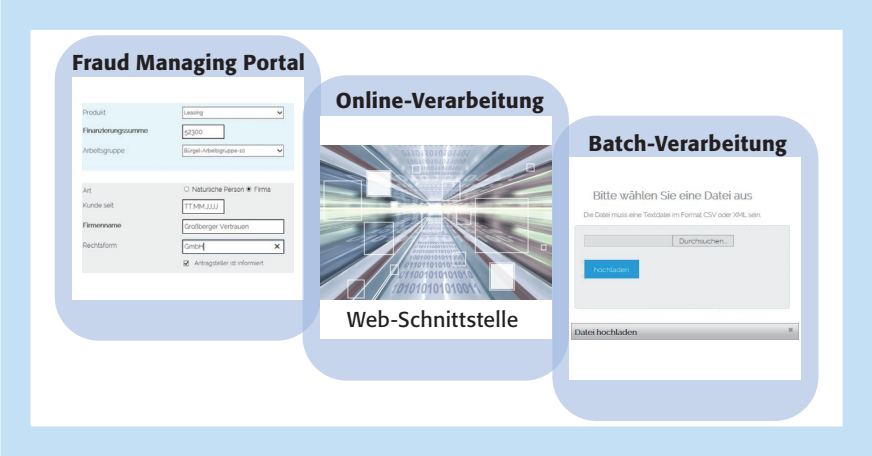
Neben den gewachsenen Systemen verhinderten vor allem datenschutzrechtliche Bedenken die auf der Hand liegende Lösung: der konsequente Austausch zu Verdachtsfällen und die Trennung der Betrugserkennung von der statistischen Prognose der Zahlungsfähigkeit. Das änderte sich mit der Aufnahme des § 25h (damals § 25c) in das KWG. 2012 schrieb der

Abbildung 3: Regelarten



Quelle: Bürgel Wirtschaftsinformationen

Abbildung 4: Zugangswege



Quelle: Bürgel Wirtschaftsinformationen

Bankenfachverband e. V. auf Anregung seiner Mitglieder eine technische Lösung für einen Fraud-Prevention-Pool aus. 2013 entschieden sich die meisten Teilnehmer für das Angebot von Bürgel Wirtschaftsinformationen.

Das neue Schutz-Portal

Im Juni 2015 ging das Deutsche Schutz Portal („DSPortal“[1]) live. Eine Entwicklungsgemeinschaft aus 18 Banken arbeitete zwei Jahre lang an der fachlichen, technischen und datenschutzrechtlichen Lösung.

Banken melden Verdachtsmomente ein und fragen Anträge gegen das System ab. Die Anfragen werden gegen den Hinweisbestand, auf Unplausibilitäten und betrugstypische Muster untersucht. Das System verarbeitet Anträge natürlicher Personen und von Firmen.

Das Portal prüft dabei drei Regeltypen:

- Hinweisregeln,
- Plausibilitäten und
- Typologien (vgl. Abbildung 3, Seite 225).

Hinweisregeln prüfen die einzelnen Datensegmente eines Antrags auf Übereinstimmungen zu eingemeldeten Verdachtsfällen. Im Gegensatz zu den typischen Blacklists verarbeitet das System alle identifizierungsrelevanten Daten. Dazu gehören Kontaktdaten, Sicherheiten und die Legitimation. Dies zielt auf die Wiederverwendung von Unterlagen, Geräten und Personendaten. Betrüger agieren dynamisch, bleiben aber Menschen: Niemand läuft gern mit verschiedenen Handys herum. Aufwendig aufgebaute Webseiten oder teuer eingekaufte Fälschungen nutzt ein Betrüger möglichst mehrfach.

Plausibilitätsregeln prüfen Unstimmigkeiten innerhalb eines Antrags oder mehrerer Anträge eines Antragstellers: die fehlerhafte Kontonummer, Doppelfinanzierungen, drastische Veränderungen in den finanziellen Verhältnissen in kurzer Zeit.

Typologien beschreiben ein Tatvorgehen. Sie basieren auf Erkenntnissen der Experten zum Verhalten. Ein professioneller Betrüger behält sein Vorgehen regelmäßig bei, so lange dieses Erfolg verspricht. Hier lagen die Probleme in der Vergangenheit zum einen in der fehlenden Kommunikation zwischen den Experten von Banken und der Polizei, zum anderen in einer zu langsamen Implementierung in die hauseigenen Regelwerke.

Die Gefährdungslage unterscheidet sich bei den Teilnehmern. Vertriebswege, Produkte, vorhandene Prüfprozesse, Marketing und verschiedene weitere Faktoren beeinflussen das Risiko, in den Fokus der Betrüger zu geraten. Generische Regeln erzielen daher immer nur mittelmäßige Ergebnisse. Im Portal optimieren die Institute Regeln, indem sie individuelle Gewichte hinterlegen. Erst bei Überschreitung eines Grenzwerts erfolgt die Aussteuerung. Die Folge ist eine sinkende False-Positiv-Rate.

Datenlage und Zugang

Sowohl die Menge als auch die Qualität der Daten zum Zeitpunkt einer Entscheidung hängen vom Vertriebsweg, dem Produkt und den internen Prozessen ab. Jedes Institut verfügt allerdings über Mindestdaten wie Name, Anschrift oder Produkt – bei natürlichen Personen kommt noch das Geburtsdatum dazu.

Zwar werden immer mehr Daten erfasst, doch teilweise erst nach einer ersten Entscheidung. Dies optimiert die Bearbeitungsprozesse, stellt für ein gemeinsames Vorgehen aber ein Problem dar. Die Teilnehmer des Portals nutzen einen einfachen Lösungsansatz: Die Institute entscheiden selbst, mit wie vielen Daten die Anfrage stattfindet. Die vorhandenen Daten bestimmen die nutzbaren Regeln. Dies eröffnet dazu den hausinternen Datenschützern einen erheblichen Spielraum.

Neben den datenschutzrechtlichen Voraussetzungen bildet die technische Integration externer Quellen oder Dienstleister für viele Banken eine Hürde. Das Portal bietet drei mögliche Ansätze:

- die Implementierung von Web-Services für eine vollständige Integration in die automatisierten Prozesse;
- manuelle Anfragen über eine browserbasierte Oberfläche;

1) Im Folgenden kurz Portal genannt.

- den Upload von CSV-Dateien mit Anfrage- oder Einmeldedaten.

Gerade die einfache Lösung eines Dateiuploads erweist sich als gute Option für einen Einstieg. Die meisten Banken können Antragsdaten leicht täglich extrahieren. Nur wenige Geschäftsbereiche, vor allem im B2C-Bereich, benötigen eine sofortige Entscheidung. Für alle anderen reicht eine zeitversetzte Prüfung zur Abwendung von Betrugsschäden.

Einige Teilnehmer kombinieren die Ansätze: Die Anfrage und Verarbeitung der Aussteuerungshinweise findet per Web-Service statt, um automatisierte Prozesse zu stoppen. Die Mitarbeiter bearbeiten die ausgesteuerten Anträge anschließend in den browsergestützten Oberflächen des Web-Portals (Abbildung 4, Seite 226).

Eine Erleichterung bei der Implementierung bieten auch Partnerschaften mit technischen Lösungsanbietern. Die Exec Software Team GmbH und die SHS-Viveon AG implementieren die Portal-Schnittstelle in ihre Bankmodule, sodass ihre Kunden die neue Lösung mit geringem Aufwand nutzen können. Die Zeb Rolfes Schierenbeck Associates GmbH bietet Analysen der vorhandenen Portfolien an.

Meldemerkmale und Prozess

Die Diskussion um die fachlich „richtige" Betrugsdefinitionen hält schon lange an. Betrug darf nur von einem Richter festgestellt werden. Auch Zuweisungen als „Täter" bergen kritische Reputationsrisiken. Der Fokus liegt daher auf den nachweisbaren Tatsachen. Dazu einigten sich die Teilnehmer auf 25 Meldemerkmale. Dazu gehören selbsterklärende Hinweise wie „Ausweis unplausibel, gefälscht oder verfälscht" oder „Anschrift nicht existent" und Auffangmerkmale wie „Auffällige Transaktionen mit Kontokündigung". Alle Teilnehmer dokumentieren entsprechende Verdachtsmerkmale schon heute. Eine Schuldfeststellung gibt es nicht, die Interpretation des Einzelfalls bleibt den Teilnehmern überlassen.

Die getroffenen Regeln steuern Anträge aus dem automatisierten Prozess in eine manuelle Prüfung. Die heuristischen Regelwerke bieten dafür konkrete Anhaltspunkte. Das ist Best-Practice. Bei Bedarf tauschen Mitarbeiter über das System Daten zu den getroffenen Fällen aus.

Betrugsprävention bleibt weiterhin teilweise Handarbeit. Betrugspräventionssysteme zielen darauf, die Menge der zu prüfenden Fälle einzuschränken und Hinweise für die Prüfung zu geben. Im Gegensatz zu statistischen Verfahren handelt es sich bei der Betrugsprävention nicht um die Prognose eines zukünftigen Verhaltens. Betrug findet in der Gegenwart statt. Dies erlaubt bei einer zielgerichteten Prüfung praktisch alle Daten zu verifizieren. Die Untersuchung zweifelhafter Anträge (Investigation) gehört in den Tätigkeitsbereich der zentralen Stelle. Die Spezialisten arbeiten nicht unter dem normalen Zeitdruck der Sachbearbeitung und bauen durch die laufende Konfrontation mit verdächtigen Anträgen schnell Wissen auf.

Monitoring und Datenschutz

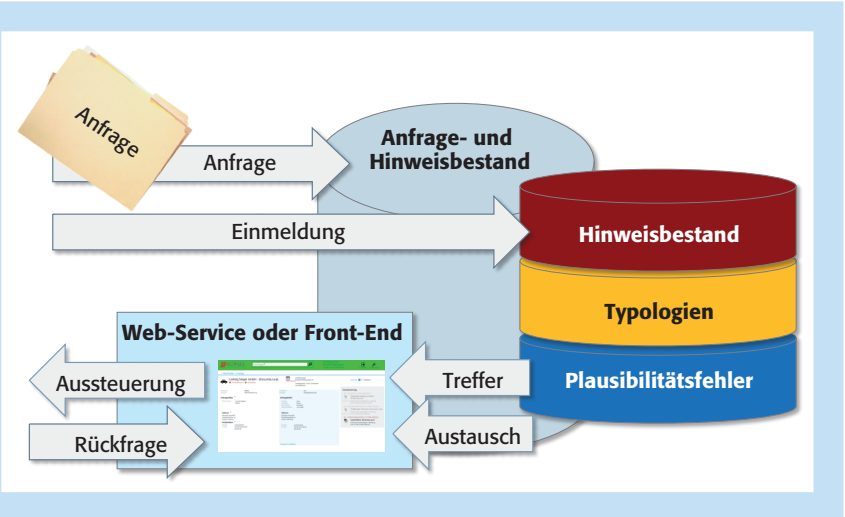
Gerade im B2B-Geschäft tritt Betrug oft erst bei Bestandskunden auf. Zur Reduzierung von Schäden verfügt das Portal über ein Bestandsmonitoring.[2)]

Professionelle Täter beuten eingesetzte Daten jedoch häufig auch schnell aus. Beim Identitätsbetrug steigt das Risiko für den Betrüger nach Kenntnis durch das Opfer stark an. Für den Zeitraum zwischen Anfrage und Vertragseinbuchung hilft das Antragsmonitoring.[3)] Gehen neue Hinweise ein, erhält der Teilnehmer bei einem Treffer innerhalb einer definierten Prozessdauer automatisch eine Meldung. Damit wird die gern genutzte Lücke geschlossen, welche bisher zwischen der ersten Anfrage und der Vertragseinbuchung bestand (Abbildung 5).

Die Abstimmung mit dem Datenschutz dauerte länger als zwei Jahre. Bürgel stellte das Konzept dem Ham-

2) Bestandsmonitoring: Einmeldungen werden mit bestehenden Verträgen abgeglichen.
3) Antragsmonitoring: Einmeldungen werden innerhalb einer definierten Prozesszeit mit Anfragen abgeglichen. Bei Treffern erfolgt eine Meldung.

Abbildung 5: Funktionsweise



Quelle: Bürgel Wirtschaftsinformationen

burger Datenschutz bereits vor Teilnahme an der Ausschreibung vor. Nach diversen Abstimmungsgesprächen folgte im Dezember 2014 die Präsentation vor dem Düsseldorfer Kreis. Eine Lösung liegt seit Ende März 2015 vor. Leider konnten sich nicht alle Landesdatenschutzbehörden einigen. Die gemeinsame Lösung scheiterte an einer Gegenstimme. Damit bleibt der Kriterienkatalog des Düsseldorfer Kreises prüfungsrelevant, jedoch inoffiziell.

Die Kritik richtet sich dabei nicht speziell gegen eine Lösung, sondern grundsätzlich gegen von Auskunfteien betriebene Betrugspräventionspools. Zu diesem Thema stellte die Fraktion „Die Linke“ eine kleine Anfrage. Die Antwort der Bundesregierung aus Juni 2015 stützt den Standpunkt der Wirtschaft und lässt an Eindeutigkeit nichts zu wünschen übrig (Bundestag Drucksache 18/5142, Frage 15). Selbst wenn die Stellungnahme den Standpunkt der unabhängigen Aufsichtsbehörde nicht beeinflusst, stellt sie doch ein erhebliches Gewicht bei den internen Datenschutzdiskussionen der Banken dar.

Trotz sehr ähnlicher Systeme im europäischen Ausland steht der Datenschutz der Plausibilitätsprüfung von Anträgen natürlicher Personen unter Nutzung der Daten verschiedener Institute weiterhin ablehnend gegenüber. Plausibilitätsregeln bleiben daher bei Privatpersonen auf den eigenen Bestand beschränkt. Bei Firmen gilt die Einschränkung nicht. Das Portal ist in Hamburg und Hessen als Auskunftei angemeldet. Damit stehen Teilnehmern und Betroffenen zwei Anlaufstellen im Bundesgebiet zur Verfügung.

Auskunfteidaten und Opferschutz

Eine Verknüpfung der Einmeldungen mit Auskunfteidaten zur Bonität ist nicht zulässig. Ob diese Bonitätsdaten umgekehrt im Portal verwendet werden dürfen, ist noch zu klären. Bis dahin schaltet Bürgel zeitgleich mit dem Portal in den Firmenvollauskünften einen Auffälligkeitsindex live, der Veränderungen in Firmen ausweist. Die Regeln benennen analog zum Portal konkrete Ereignisse. Die neue Kennzahl beeinflusst die statistische Bonitätsprognose nicht.

Das Phänomen des Identitätsdiebstahls nimmt zu. Die Verbreitung sozialer Netze und der illegale Handel mit personenbezogenen Daten macht es den Tätern leicht. Mit dem Going-Live des Portals fordert in Deutschland eine Auskunftei zum ersten Mal Opfer von Betrugsfällen auf, sich zu melden. Die Einmeldung bietet Opfern Schutz vor weiteren Straftaten. In Großbritannien beruhen circa 50 Prozent aller Fälle von Antragsbetrug auf Identitätsstraftaten. In einem Großteil davon nutzen die Betrüger übernommene Identitäten von Privatpersonen.

Hilfsmittel und Anreize

Aus den Anforderungen der Institute wurde eine Reihe von Zusatzfunktionen entwickelt, die bei der aktiven Arbeit in der Betrugsprävention helfen. Die browsergestützte Oberfläche bietet ein fallabschließendes Case-Management. Das Portal unterstützt Arbeitsgruppen, Wiedervorlagen, die zeitgesteuerte Bereinigung von Arbeitslisten und die Anzeige interner Service-Level zur Fallbearbeitung. Der eigene Anfrage- und Meldebestand kann gezielt nach allen verdachtsrelevanten Daten durchsucht werden; eine Funktion, die in den gewachsenen IT-Systemen von Finanzdienstleistern oft fehlt. Das monatliche Reporting hilft bei der Einstellung der Regeln.

Die False-Positive-Quoten der einzelnen Regeln erlaubt eine Einschätzung der Meldefreudigkeit eines Teilnehmers: kein Institut setzt gern dauerhaft Regeln ein, die schlecht funktionieren.[4] Bürgel fragt hier aktiv nach. Außerdem funktioniert der Austausch bei Verdachtsfällen nur im Umfang der angefragten Daten.

Die Beteiligung am Pool beeinflusst die Risiken der Teilnehmer auf verschiedenen Ebenen; in erster Linie vermeiden sie direkte Betrugsschäden. Darüber hinaus reduziert die Vereinfachung der Bearbeitung auch die Prozesskosten. Die eindeutige Fallkennzeichnung ermöglicht die Optimierung der Ankaufscorekarten und eröffnet damit den Weg zu mehr Geschäft. Die Banken diskutieren auch die Auswirkungen der klaren Trennung von Adress- zu operationellen Risiken, da Betrug heute meist in beide Sparten einfließt und damit doppelt bewertet wird.

Auswirkungen auf die Risikosituation

Die statistische Bonitätsbewertung behält natürlich ihren Platz. Sie ist weiterhin der beste Weg zur Optimierung der Ankaufstrategie, wenn es um redliche Kunden geht. Sie muss aber klar von den Anforderungen der Betrugsprävention getrennt werden. Dort steht die Prüfung konkreter Hinweise in Einzelfällen im Vordergrund. Dies schützt die Betroffenen und die Teilnehmer. Der Datenschutz gewinnt durch den regulierten und vor allem nachvollziehbaren Datenaustausch.

Die Entwicklung dieser neuen Auskunft basiert auf den konkreten Anforderungen der Kreditwirtschaft. Damit zeigt sich, dass trotz der hohen datenschutzrechtlichen Hürden auch in Deutschland neue Informationsdienste aufgebaut werden können.

Nur die Täter verlieren. Dies sollte der erste Schritt zu einem neuen Trend sein: Deutschland geriet in den letzten Jahren immer mehr in den Fokus der Betrüger, doch das dürfte sich mit dem neuen Portal bald ändern. ◄

4) False-Positive-Rate: Zeigt die Qualität eingesetzter Regeln. Verhältnis der erkannten Betrugsfälle zu den fehlerhaft ausgesteuerten Fällen. Je nach Produkt sind Quoten zwischen eins zu fünf (1:5) und eins zu dreißig (1:30) üblich.