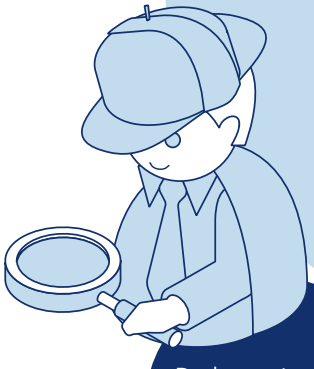
RISK IDENT

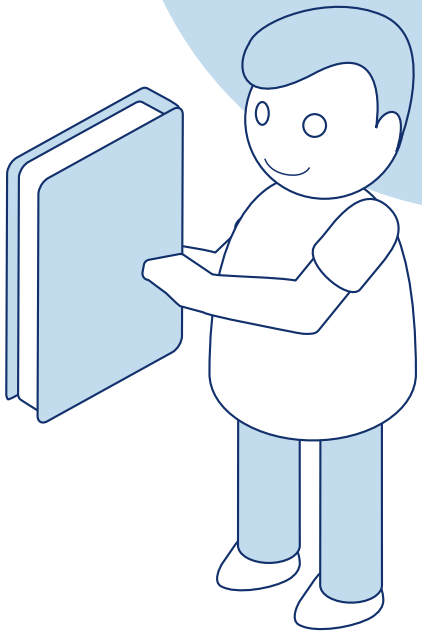
BETRUGSPRÄVENTION LOHNT SICH

Business-Cases berechnen, intern überzeugen
und Systeme nachhaltig aufbauen



Du kannst mich anklicken und direkt zum Kapitel gelangen!

INHALT



1 EINLEITUNG

Ob beim Aufbau neuer Systeme, der Implementierung von Datenquellen oder Kalkulation von benötigtem Personal: Gerade bei den Business-Cases der Betrugsprävention gibt es viele Stolpersteine. Mit diesem Whitepaper unterstützen wir Dich bei der richtigen Kalkulation und Argumentation, um Dein Betrugsmanagement nachhaltig aufzubauen.

2 KLASSISCHE BUSINESS-CASES IM RISIKOMANAGEMENT

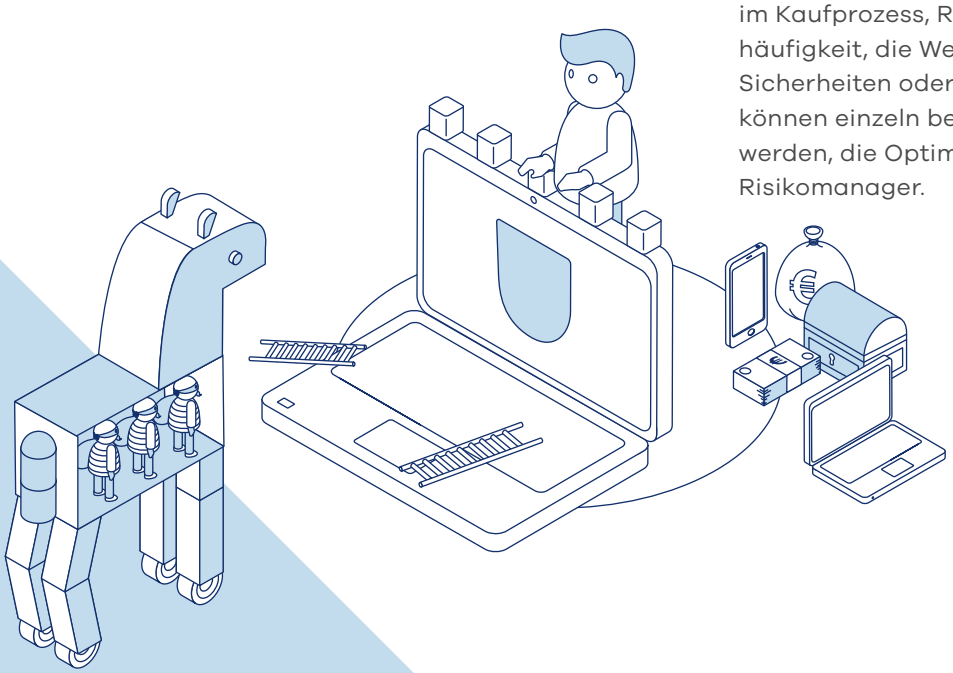
Das Ziel der traditionellen Bonitätsbeurteilung[1] ist die Optimierung des Ausfallrisikos ehrlicher Kund*innen. Die Frage lautet: Bis zu welchem Grenzwert werden Kund*innen akzeptiert und risikoreichere Zahlungsmittel zugelassen?

Ignoriert man das Thema Betrug, ist das eine einfache statistische Berechnung. Das Ausfallrisiko ehrlicher Kund*innen ist eine recht stabile Variable und verändert sich auch im Zeitablauf nur gering.[2]

Auch die Berechnung von Business-Cases für die Optimierung solcher Systeme ist vielleicht kompliziert, aber nicht komplex:

- Neue Datenquellen werden nach den Kosten für die Datenerhebung und dem Erkenntnisgewinn für das Ausfallrisiko bewertet.
- Neue Systeme liefern Kosteneinsparungen über eine bessere Automatisierung der Entscheidungs- und Reaktionsprozesse.

Komplizierter wird es, wenn weitere Parameter berücksichtigt werden: etwa die Abbruchquote im Kaufprozess, Rücksendungen oder Rückfragehäufigkeit, die Werthaltigkeit von Retouren/Sicherheiten oder Inkassokosten. All diese Faktoren können einzeln bestimmt oder valide geschätzt werden, die Optimierung ist der Alltag der Risikomanager.



3 HERAUSFORDERUNGEN IN DER BETRUGSPRÄVENTION

Auch in der Betrugsprävention werden Datenquellen auf ihre Aussagekraft hin geprüft und Kosten der Anbieter für Daten und Systeme oder der Datenerhebung verglichen.

Das Problem ist allerdings komplex, denn die Gegner sind dynamisch: Betrüger*innen verändern bei mangelndem Erfolg ihre Vorgehensweise. Datenquellen, Regeln oder Algorithmen, die heute trennscharf Betrug aufzeigen, können morgen wirkungslos sein. Und Methoden, die heute keine Treffer liefern, können morgen der Schlüssel zur Verhinderung einer großen Betrugsserie sein.

Ein ähnliches Phänomen gilt bei sich überlappenden Methoden: Kann ein Tatvorgehen (Modus Operandi) durch mehrere Methoden identifiziert werden, ist nicht automatisch die günstigste Methode sinnvoll – vielleicht lohnt sich sogar der Einsatz verschiedener Methoden, um dem Betrüger das Ausweichen zu erschweren. Methoden der Betrugsprävention scheinen manchmal wirkungslos, sind deshalb aber lange noch nicht nutzlos.

Was wir wissen: Erfolgreiche Betrugsmuster werden fortgeführt, solange keine Gegenmaßnahmen eingesetzt werden. Erkannte Lücken werden von professionellen Tätern schnell und massiv ausgenutzt, bis sie geschlossen werden. Und einmal erkannte Schwachstellen werden immer wieder getestet.

Ohne Wertbeitrag heißt noch lange nicht nutzlos

Eine Bank prüft bei Antragstellung über eine Auskunftei, ob Name und Konto übereinstimmen. In der Analyse erweist sich die Prüfung als nicht trennscharf – nahezu alle Treffer waren fehlerhaft und haben mehr Arbeit und Kosten verursacht. Die Bank schaltet die Prüfung ab. Nach einigen Monaten werden Betrugsfälle sichtbar, bei denen gestohlene Bankverbindungen verwendet wurden: Der Datenbezug hatte eine Schutzfunktion, die wenigen Treffer waren Testfälle von Betrügern. Nach Abschalten dieses Sicherungsmechanismus starteten sie einen größeren Angriff.

Redundante Verfahren verhindern das Ausweichen

Ein E-Commerce-Unternehmen stellt fest, dass automatisierte Bestellungen in seinem Shop getätigt werden. Die Betrugsversuche können über eine Geräteidentifizierung (Device-Fingerprinting), ein biometrisches Verfahren oder Verhaltensmusteranalysen identifiziert werden. Grundsätzlich ist es sinnvoll, alle drei Verfahren im Einsatz zu haben – die Reduzierung auf zwei oder ein Verfahren erhöht das Risiko, dass die Täter dieses umgehen.

Neben der Täterdynamik gibt es weitere Herausforderungen:

- Der Ausfall aufgrund von Betrug ist im Gegensatz zum Zahlungsausfall ehrlicher Kunden kein einheitliches Zielkriterium. In der Betrugsprävention müssen eine Vielzahl von Modi Operandi unterschieden werden. Die tiefere Klassifizierung von Betrugsfällen ist selten. Dies erzeugt Probleme in der Analytik und der Erfolgsmessung.
- So verschieden wie die Betrugsmuster sind die Angriffsflächen. Einfallstore sind die eigene IT-Infrastruktur, die von Zulieferern oder die der Kunden, Antragsstrecken, Bestandskundenprozesse, Mitarbeiter*innen, Transaktionen oder der / die Kund*in selbst.
- Wer trägt die Kosten? Im E-Commerce kommt regelmäßig der Händler für den Schaden auf. Bei Banken und Zahlungsdienstleistern sind zumindest bei einigen Betrugsmustern die Kunden verantwortlich.[3]
- Indirekte Kosten, z. B. durch die Bearbeitung oder entgangenen Gewinn, werden häufig nicht berücksichtigt.
- Einige Kosten sind schwer zu bestimmen: Betrug verursacht operationelle Risikokosten. Eine eingeschränkte Prävention kann z. B. zu erhöhten Strafzahlungen bei Geldwäschedelikten oder zu Reputationsschäden führen.
- In der Betrugsabwehr wird verhinderter Schaden regelmäßig unterschätzt: Oft werden nur einzelne abgewehrte Transaktionen gewertet, nicht aber mögliche Folgeschäden.[4]
- Eine gute Betrugsprävention erzeugt ein positives Feedback, d. h., die Angriffswahrscheinlichkeit nimmt ab, Täter*innen werden abgeschreckt. Eine qualitativ hochwertige Betrugsprävention zeichnet sich langfristig dadurch aus, dass nur noch wenige Betrugsversuche zu verzeichnen sind. Genauso spricht sich aber auch eine schlechte Prävention schnell unter den Tätern herum.
- Schadenshöhe und Angriffswahrscheinlichkeit variieren stark bei verschiedenen Zugangswegen, Branchen und Produkten. Benchmarking ist schwierig.
- Der Nutzen einzelner Methoden ist nicht ohne Weiteres übertragbar. Machine-Learning / künstliche Intelligenz ist in einigen Bereichen unverzichtbar, in anderen schlicht unnütz.
- Betrug wird häufig erst mit deutlichem Zeitverzug bemerkt.
- Durch die Dynamik der Täter ist die Stabilität eingesetzter Methoden schwer abzuschätzen.
- Die Fallzahlen reichen häufig nicht aus, um statistische Methoden sinnvoll einzusetzen.
- Fachlich einfache Sachverhalte werden in der Flut möglicher Analysen übersehen.
- Gegenmaßnahmen haben Opportunitätskosten: Die Anforderung zusätzlicher Daten oder einer Identifikation schreckt nicht nur Betrüger ab, sondern erhöht auch die Abbruchquote ehrlicher Kunden.
- Tests zur Beurteilung der Qualität von Verfahren unterliegen verschiedenen Einschränkungen. Z. B. dürfen keine randomisierten Fälle genutzt werden, da nur ein vollständiger Datensatz in einem definierten Zeitfenster alle Merkmale liefert.
- Neue Vertriebsmaßnahmen und Prozessveränderungen eröffnen neue Angriffsvektoren und werden nicht mit der Betrugsprävention abgestimmt.

Kosten sparen durch Expert*innen

Eine polnische Bank hat ein Betrugsproblem – immer wieder fallen Fahrzeugfinanzierungen aus, die Täter sind nicht auffindbar. Die Bank lässt eine Scorekarte entwickeln, um das Problem in den Griff zu bekommen. Die Trennschärfe der entwickelten Scorekarte ist hervorragend, und mit dem Einsatz verschwinden die Ausfälle. In der Nachprüfung wird festgestellt, dass die trennschärfsten Variablen einfach waren: Die Täter waren grenznah wohnende jüngere Männer mit geringem Einkommen und sehr geringer oder keiner Miete.

Statt der langwierigen und teuren Scorekartenentwicklung hätten hier der Blick eines / einer Expert*in und eine leicht zu implementierende Regel gereicht.

4 STRATEGIEN BEI KOMPLEXEN PROBLEMEN

Wir sprechen hier also von einem komplexen Problem, da es

- schwer oder nicht berechenbare Variablen gibt und
- Rückkopplungen zwischen Herausforderungen und Lösungsansätzen bestehen.

In dieser komplexen Gemengelage gibt es zwei übliche Handlungsoptionen:

1. Die Komplexität wird ignoriert, auf erkannte Risiken wird situativ reagiert. Da mögliche Probleme selten oder gar nicht auftauchen, hat dies den Vorteil, dass die vorhandenen Ressourcen zur Lösung anderer Probleme genutzt werden können. Die wichtigsten Risiken sind, dass neue Modi Operandi zu spät erkannt werden und / oder keine Lösungsoptionen bereitstehen. Sowohl das Eintritts-, als auch das Einschlagrisiko bleiben unverändert.
2. Der Aufbau eines umfassenden Verständnisses, um Risiken frühzeitig zu erkennen und zu begegnen. Abhängig von der Ausgangssituation kann dieses Verständnis einen erheblichen Veränderungsbedarf in der der Organisation und in den eingesetzten Methoden aufzeigen. Ohne Analyse wird häufig übersehen, dass es meist bereits gute Business-Cases bestehen, die gleichzeitig künftige Risiken reduzieren.

An dieser Stelle ist es hilfreich, sich die Ziele und den Stellenwert der Betrugsprävention im eigenen Unternehmen bewusst zu machen. Im klassischen Risikomanagement kann ein mathematisches Optimum einzelner Maßnahmen errechnet werden. In der Betrugsprävention ist dies aufgrund der Komplexität nicht möglich.

Ziele sind aus unserer Sicht:

- Die schnelle Identifizierung und die Abwehr neuer Betrugsmuster
- Die dauerhafte Abwehr von Betrug, bestenfalls die Abschreckung
- Die Reduzierung von Betrugs- und Betrugsfolgekosten
- Die Reduzierung von Opportunitätskosten

Gerade in jungen Unternehmen liegt die Priorität meist nicht auf der Betrugsabwehr, da es kritischere Risiken gibt. In diesem Fall sollten Angriffe zumindest schnell erkannt werden und rudimentäre Abwehrmaßnahmen verfügbar sein.

Das Risiko steigt mit zunehmender Größe und Bekanntheit, entsprechend wird auch eine strategische Zielplanung der Prävention wichtiger.

5 DER SCHNELLE BUSINESS-CASE: DIE KRISE NUTZEN

Du hast gerade neue Betrugsfälle entdeckt? Aktuelle betrügerische Anträge oder Transaktionen sind wahrscheinlich? Dann hast Du jetzt die Aufmerksamkeit des Managements.

Ohne Gegenmaßnahmen steigt die Angriffswahrscheinlichkeit: Wenn es sich nicht um unabhängige Fälle handelt, werden die Täter*innen die Lücke immer massiver ausnutzen, bis sie geschlossen ist. Eine „Welle" entsteht oder ist schon da.

Sofern es möglich ist, wirst Du manuell eingreifen, um weitere Schäden zu verhindern. Dennoch ist aktueller Schmerz immer die einfachste Möglichkeit, einen Business-Case zur Einführung oder Optimierung eines Fraud-Management-Systems aufzustellen und zu rechtfertigen:

	Schaden aus aktuellen Betrugsfällen
+	Angenommener Schaden ohne Handlung
=	Gesamtkosten für Betrug

	Angenommene Schadensreduzierung
./.	Kosten für Systeme/Datenquellen
./.	Kosten der Implementierung
./.	Kosten der manuellen Nachbearbeitung
=	Einsparungen

Natürlich ist das stark vereinfacht.[5] Ist der aktuelle Schaden hoch, dann hast Du bereits manuelle Maßnahmen zur Abwehr eingeleitet, bevor Du Dich um eine technische Betrugsprävention kümmerst. Der angenommene Schaden ohne Handlung ist eine Mutmaßung, bestenfalls hast Du einzelne Erfahrungswerte, denn es existieren kaum statistische Untersuchungen zum Verlauf einzelner Betrugsmuster.

Diese einfache Berechnung hat dennoch große Vorteile:

1. Jeder versteht sie.
2. Abwarten kostet mit Sicherheit Geld. Der Handlungsdruck ist groß.
3. Die Berechnung ist nicht falsch. Es gibt ausreichend Szenarien, in denen sie ausreicht.

Die Berechnung ist korrekt, solange Du eine Folge von ähnlichen Tatmustern feststellst.[6]

Die Berechnung funktioniert bei der Neueinführung von Präventionsmaßnahmen oder bei unvollständiger Betrugsabwehr. Verschwindet ein Tatmuster vollständig, scheint das System oder die Datenquelle überflüssig zu werden. Dabei wird leicht vergessen, dass Betrugsmuster wieder aufleben, wenn Schutzmaßnahmen abgeschaltet werden.

Hast Du noch kein Präventionssystem, kannst Du diese Ausgangslage nutzen, um grundlegende Maßnahmen aufzubauen. Auch in einer Krise sollte daher die Langfristplanung nicht außer Acht gelassen werden. Bestenfalls hast Du bereits eine Zielarchitektur für die Betrugsprävention geplant und ergreifst die gute Gelegenheit, um Komponenten aufzubauen, die darauf einzahlen.

Die Einzelmaßnahme: Datenquellen und einzelne Methoden ergänzen

Du hast bereits ein Fraud-Management-System oder bist mit Deinen Systemen zufrieden? Und gleichzeitig fragst Du Dich, ob nicht genau diese Datenquelle oder diese Methode Dir helfen kann, noch besser zu werden? Dann bietet sich eine Trennschärfe- und Überschneidungsanalyse an.

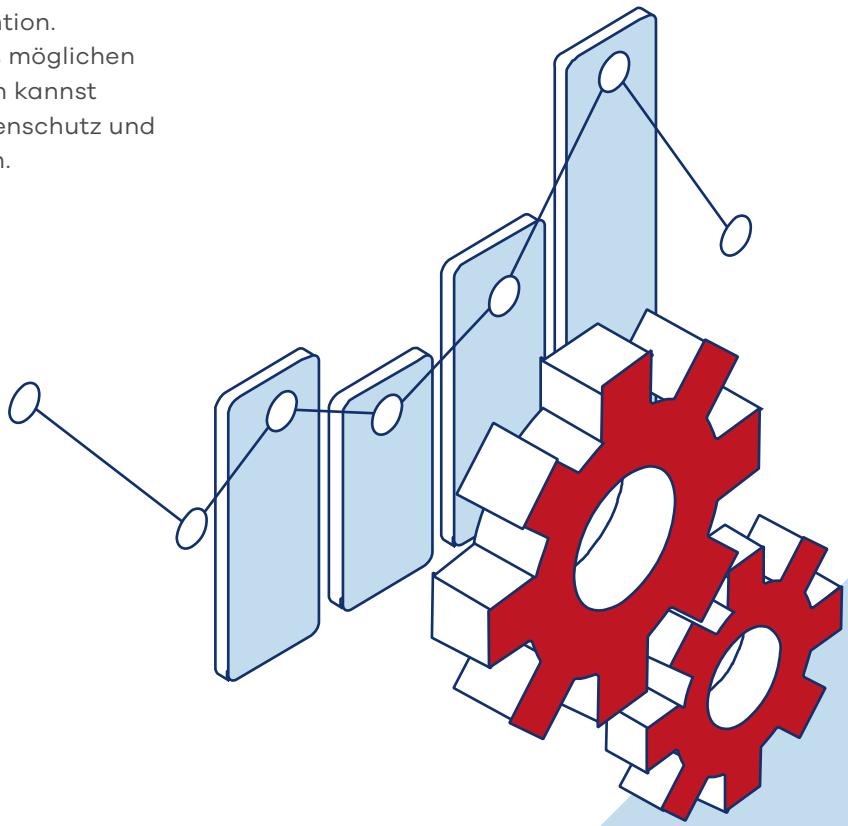
Dabei werden alle vorhandenen Datenquellen und Regeln daraufhin überprüft, welchen Mehrwert sie bei der Identifizierung einzelner Betrugsfälle liefern. Mach es Dir leicht – es reicht, wenn Du den einfachen Business-Case nutzt. Die Ausgangslage ist ähnlich, nur dass Du jetzt optimierst und der Druck nicht so hoch ist.

Unsere Empfehlung: Teste an Datenquellen, was Dein Budget und Dein Datenschutz zulassen. Die meisten Anbieter haben Tests zu Sonderkonditionen im Programm. Nur so gewinnst Du ein umfangreiches Wissen über die Wirksamkeit verschiedener Datenarten und -quellen in der Betrugsprävention. Gleichzeitig baust Du ein Repertoire aus möglichen Methoden auf, die Du jederzeit einsetzen kannst und die Eure interne Prüfung durch Datenschutz und IT-Sicherheit bereits überstanden haben.

Champion-Challenger:
Kauf Dir doch mal Betrugsfälle

In Champion-Challenger-Prozessen wird eine alternative Ankaufs-Entscheidungsstrategie an einem kleinen Teil der Neukunden ausprobiert. Normalerweise werden in diesen Antragsstrecken neue Entscheidungsstrategien oder zusätzliche Datenquellen getestet. Selten öffnet ein Unternehmen einmal alle Schleusen und prüft nach der Durchreifungszeit, was tatsächlich an Betrug hereinkommt, wenn die Schutzmaßnahmen abgeschaltet werden.

In beiden Fällen solltest Du Dir ein entsprechendes Risikobudget genehmigen lassen.



6 NEUEINFÜHRUNG VON SYSTEMEN

Jedes Unternehmen implementiert interne Maßnahmen gegen Betrug. Dies ist bereits Teil einer ordnungsgemäßen Geschäftsführung. Für die Abwehr von internem Betrug gibt es weitreichende Standards, z. B. Compliance-Regelungen oder Richtlinien der Buchführung.[7]

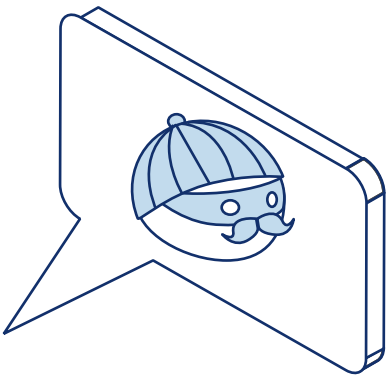
Die Abwehr von externem Betrug erfolgt dagegen meist als Reaktion auf Angriffe und ist nur selten von Beginn an strukturiert geplant. Entsprechend zerklüftet sind viele Präventionsprozesse, häufig arbeiten Mitarbeiter*innen der Betrugsprävention mit einer Vielzahl von Applikationen oder in verschiedenen Teilprozessen. Hier verbirgt sich Potenzial, nicht nur zur Reduzierung von aktuellem und zukünftigem Risiko, sondern auch in der Bearbeitung einzelner Anträge oder Orders.

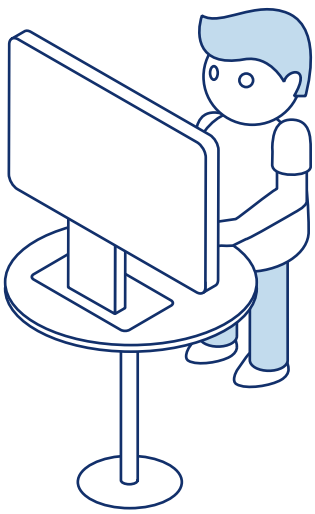
Bei der Planung sollten die laufende Überprüfung der eingesetzten Methoden und deren Wirksamkeit berücksichtigt werden, da sich die Angriffsszenarien ständig verändern können. Außerdem entwickeln sich die technischen und analytischen Möglichkeiten schnell.

Betrugsprävention ist Fitness im Risikomanagement

Betrugsprävention ist immer dann ein Thema, wenn der Schmerz gerade groß ist. Ein neuer Algorithmus oder eine neue Methode können hier Abhilfe schaffen, wenn diese genau den „Painpoint" treffen.

Betrug ist gut mit einer Infektionskrankheit zu vergleichen: Die Methode, die genau bei diesem Schmerz hilft, entspricht einem passenden Medikament. Ein gutes Betrugsmanagementsystem gleicht eher dem Immunsystem unseres Körpers. Ist dieses fit, werden wir die meisten Krankheiten nicht einmal bemerken und fast alle ohne größeren Schaden überstehen. Das heißt nicht, dass wir völlig sicher sind. Oder dass wir nie ins Krankenhaus müssen. Aber die Grundvoraussetzungen sind besser. Und genau wie beim Erhalt oder dem Aufbau körperlicher Fitness ist es schwer, den Anfang zu machen – unsere Prioritäten liegen meist an anderer Stelle.





7 EIN UMFASSENDER BUSINESS-CASE

	Kosten	Anmerkungen
	Eingesetzte Präventionssysteme	Anschaffung, Implementierung und Wartung. Es sollten nur Systeme berücksichtigt werden, die originär für die Prävention genutzt werden.
+	Überprüfung der Systeme / Analytik	Regelmäßige Überprüfung von Regelwerken und Rekalibrierung von Scores.
+	Mitarbeiter*innen	Direkt und indirekt, z. B. auch in der Analytik oder im Inkasso. Mitarbeiter*innen in der manuellen Prüfung nach Anzahl der Aussteuerungen / der erkannten Betrugsfälle. Indirekt involvierte Mitarbeiter*innen nach anteiligem Kostenschlüssel. Auch Prüfhandlungen in der Antragsprüfung können berücksichtigt werden.
+	Externe Datenquellen und Dienste	Z. B. Device Fingerprinting (DEVICE IDENT), Auskunfteidaten. Die Kosten können direkt ermittelt werden.
+	Ausfall aus bekanntem Betrug	Bestenfalls unterschieden nach Modi Operandi.
+	Ausfall aus nicht direkt identifiziertem Betrug (erhelltes Dunkelfeld)	Siehe unser Whitepaper „Dunkelfeldanalyse". Zur Vereinfachung kann ein prozentualer Anteil der Ausfälle angesetzt werden. Zur Validierung reicht eine Stichprobe.
+	Entgangener Gewinn aus fehlerhaften Entscheidungen und Kaufabbrüchen	Über Champion-Challenger-Strecken ermittelbar, teilweise analytisch zu schätzen.
+	Folgekosten von Betrug	Rücklastschriften, Chargebacks, Inkassokosten, Rechtsabteilung, Geldwäsche-Meldungen usw.
+	Operationelle Risikokosten	Kalkulatorische Strafzahlungen, Reputationsschäden.
+	Bewusster Risikoeinkauf	Insbesondere zum Test der Wirksamkeit von bestehenden Datenquellen.
=	**Kosten Betrug + Betrugsprävention**	

Die Aufstellung zeigt bereits die Herausforderung: Viele Zahlen sind nicht oder nur eingeschränkt bekannt. Einigermaßen valide Schätzungen helfen allerdings sehr. Nimm lieber einen möglichst gut geschätzten Wert, als hier gar nichts anzusetzen.

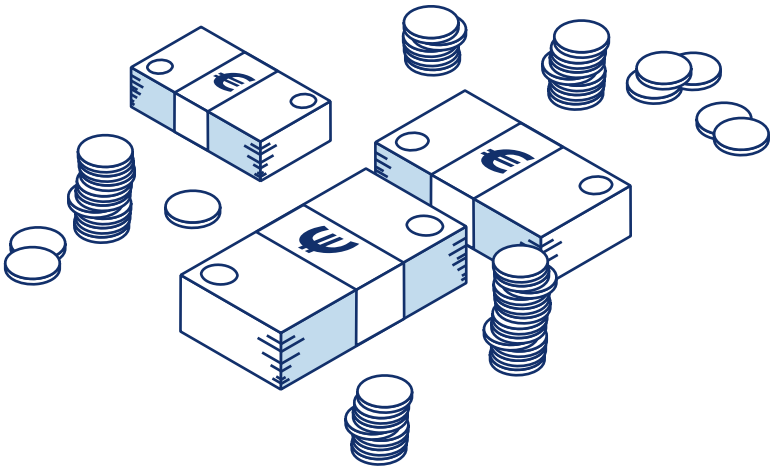
Auch die andere Seite des Business-Cases leidet unter dem gleichen Problem: Was sind „gute" erreichbare Werte? Die Gemengelage aus Branchen, Produkten, Kaufabbruch, Betrugsversuchen, Aussteuerungen, Vertriebswegen, automatisierter Prüfung, manueller Nachbearbeitung, verschiedenen Tatmustern und Reaktionen ist komplex. Allgemeingültiges Zahlenmaterial gibt es unseres Wissens nach nicht. Reports von Systemanbietern und Zahlungsdienstleistern enthalten vereinzelt Kennzahlen[8], qualitativ sind diese allerdings kaum einzuordnen, und die Übertragbarkeit auf das eigene Geschäft ist aufgrund der individuellen Prozesse schwierig. Best Practice ist die analytische Prüfung der eigenen Betrugsfälle. Müssen Benchmarks genutzt werden, kommen diese bestenfalls aus dem Austausch mit dem direkten Wettbewerb. Vorreiter sind Telekommunikationsunternehmen, Versicherungen und Banken, die sich zum fachlichen Austausch innerhalb ihrer Branchen treffen. Das Merchant Risk Council (MRC) ist eine Anlaufstelle für internationale Händler.

Payment-Service-Provider und Kreditkartenunternehmen haben einen Überblick und können Zahlenmaterial liefern. Systemanbieter wie **RISK IDENT** haben Erfahrungswerte innerhalb ihrer Kundengruppen.

In den Einsparungen haben wir Themen aus den Kosten wieder aufgenommen, daher sind einige Positionen redundant.

Uns geht es hier vor allem um Vollständigkeit. Du solltest Dich hier Deinem Hausstandard anpassen.

	Einsparungen	Anmerkungen
	Vermeidung von direktem Ausfall	Auf Basis von Analysen oder hilfsweise aus der Differenz zu Benchmarks
+	Vermeidung von Betrugsfolgekosten	Rücklastschriften & Chargebacks, Inkasso, Strafanzeigen, Geldwäsche-Verdachtsmeldungen
+	Reduzierung von Systemkosten	Kann direkt berechnet werden
+	Einsparung von Erstattungen	Sofern die Kosten für Betrug am Kunden/an der Kundin aus Kulanz übernommen werden
+	Reduzierung von Kosten aus Datenbezug	Kann direkt berechnet werden
+	Reduzierung von Kosten aus manueller Prüfung	Bearbeitung von Verdachtsmeldungen
+	Verbesserte Konditionen bei Dienstleistern/Payment-Kosten	Nichtbanken: bessere Konditionen im Payment und im Inkasso, im E-Commerce auch Kostenoptimierung im Zahlartenmix
+	Reduzierung operationeller Kosten	Reduzierung von Reputationsrisiken, Strafzahlungen wegen Geldwäsche
+	Reduzierung von Kaufabbrüchen	Reduzierung fehlerhafter Ablehnungen oder der Abbrüche im Kaufprozess: durchschnittlicher Ertrag pro Kunde / Kundin
=	**Summe der Einsparungen**	



8 ANFORDERUNGEN AN DIE ANALYTIK

Soll für die Begründung eines Business-Cases eine Datenanalyse vorgenommen werden, sind einige Punkte zu berücksichtigen:

- Nicht alle Daten können historisch angereichert werden. Geräteidentifikation und biometrische Daten müssen über Tests erhoben werden und werden nach der Durchreifung der Anträge / Bestellungen analytisch ausgewertet.
- Historisch angereicherte Daten müssen zeitlich korrekt eingeordnet werden. Dies gilt sowohl für externe Informationen wie auch für Markierungen aus der internen Betrugserkennung.
- Achte auf eine ausreichende Durchreifung des Datenbestands. Auch Betrugshinweise aus dem Inkasso sollten aufgenommen werden.
- Da die wichtigste Maßnahme zur Abwehr von Betrug die Wiedererkennung von Daten ist, sind möglichst vollständige Datensätze sinnvoll. Testverfahren mit randomisierter Auswahl[9] liefern verfälschte Ergebnisse (die Erkennungsquote ist zu niedrig).
- Der Zeitraum ist ausreichend lang zu wählen, um Wiederholungstäter anhand ihrer Daten identifizieren und Betrugsmuster wiedererkennen zu können. Üblich sind sechs bis zwölf Monate.
- Für die Entwicklung von Scorekarten und noch mehr für die Anwendung von Verfahren der künstlichen Intelligenz sind ausreichend Betrugsfälle notwendig. Im besten Fall eines Modus Operandi: 200 bis 400 gelten als verlässliche Grundlage. Bei kleineren Mengen sind Sichtprüfungen und Trennschärfeuntersuchungen verwendeter Daten sinnvoll.
- Auch Ausfälle ohne Betrugskennzeichen und Ablehnungen sollten in die Analyse einbezogen werden.
- Nichtbetrugsfälle sind einzubeziehen, um die Menge fehlerhafter Treffer zu klären.
- Es ist sinnvoll, möglichst viele verfügbare Daten zu analysieren. Selbst wenn Dir z. B. die Marketingdaten aktuell für die Prüfung nicht zur Verfügung stehen, können diese vielleicht in einem künftigen Projekt bereitgestellt werden. Der Mehraufwand ist an dieser Stelle gering.

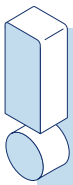
Bei dem Ergebnis der Analyse solltest Du misstrauisch sein: Insbesondere sehr trennscharfe Ergebnisse in Scoreentwicklungen und bei KI-Verfahren deuten darauf, dass ein einzelnes Betrugsmuster analytisch identifiziert wurde. Wenn Du einen solchen Case erkennst, dann schau, ob dieser

a) noch aktuell ist und

b) mit einer Regel direkt identifiziert werden kann.

Ist dies der Fall, dann nimm die betroffenen Fälle aus dem Datenbestand und lass die Analytiker den verbliebenen Datenbestand neu prüfen.

Regeln haben erhebliche Vorteile in der Betrugsprävention. Vor allem können sie einfach abgeschaltet oder ohne Auswirkung mitgeführt werden, wenn ein Betrugsmuster nicht mehr auftaucht. Das vermeidet falsche Treffer. Bei Scores oder komplexen Algorithmen geht das leider nicht ohne Weiteres, hier ist eine Rekalibrierung notwendig. Außerdem sind Regeln billiger zu implementieren und zu überwachen.



Abwarten ist keine Option: Betrugswellen

Ein deutscher Kreditkartenanbieter stellt aufgrund leicht erhöhter Ausfälle Fraud im Antragsprozess fest. Die Ausfallstückzahlen und -beträge sind moderat. Man entscheidet sich, einen Monat abzuwarten.

Die Verzögerung vom Antrag bis zur Betrugserkennung im Ausfall beträgt drei Monate – die Betrüger haben vor einem Vierteljahr entdeckt, dass die Betrugserkennung im Antragsprozess eine Lücke aufweist. Auch den Extramonat haben sie gut genutzt: Mittlerweile sind knapp 8 % aller Neuanträge betrügerisch, die Schäden steigen massiv.

Der Cybersource-Report[10] nennt als einer der wenigen konkrete Zahlen in verschiedenen Regionen und Branchen. Dennoch sollte man vorsichtig sein, diese als Benchmarks anzusehen: Der Abstraktionsgrad ist für den Vergleich mit eigenen Ausfällen bei den meisten Unternehmen deutlich zu hoch.

	Global	Nord-amerika	Latein-amerika	Mittlerer Osten & Afrika	Asiatisch-pazifischer Raum	Europa (total)	Nord-europa	Süd-europa
% des jährlichen E-Commerce-Umsatzes, der durch Zahlungsbetrug bei Inlandsbestellungen verloren geht	**1.6**	**1.5**	**1.3**	**1.8**	**1.5**	**1.9**	**1.6**	**2**
% der inländischen E-Commerce-Bestellungen, die aufgrund von Betrugsverdacht abgelehnt wurden	**2.5**	**3**	**2.8**	**3**	**2**	**3**	**2.7**	**4**
Betrugsbedingte Rückbuchungen in % des jährlichen E-Commerce-Umsatzes	**0.3**	**0.7**	**0.6**	**0.7**	**0.1**	**0.7**	**0.6**	**0.7**
% der E-Commerce-Bestellungen, die manuell auf Betrug geprüft werden	**25**	**16**	**20**	**30**	**30**	**20**	**20**	**25**

Quelle: Cybersource-Report[10] Seite 35

Mehr Personal!

Auch wenn die Automatisierung in unserem Bereich stark voranschreitet: Viele Betrugsmuster können nur durch Menschen qualifiziert geprüft und bearbeitet werden. Letztendlich ist es das Wesensmerkmal des Betrugs, dass wir Betrüger*innen für normale Kunden halten sollen – und da kommen Maschinen häufig an ihre Grenzen. In vielen Branchen ist eine gute Betrugsprävention ohne manuelle Prüfungen nicht vorstellbar.

Folgende Vorgehensweisen sind üblich:

a) Alle Aussteuerungen mit Betrugsverdacht werden geprüft. Die Anzahl der Aussteuerungen wird optimiert.

b) Es werden so viele Fälle geprüft, wie Personal vorhanden ist. Es wird die Reihenfolge der Bearbeitung optimiert.

c) Entscheidungen werden automatisiert getroffen, in der manuellen Nachbearbeitung werden neue Muster identifiziert.

In den ersten beiden Fällen ist die Berechnung des benötigten Personals einfach: Es ist zu prüfen, ob eine Ausweitung der Aussteuerungen bzw. die Bearbeitung von ausgesteuerten Fällen mit geringerer Priorisierung noch einen ausreichenden Effekt hat. Üblich ist es, die Erkennungsquote manueller Bearbeitung bei 100 % anzusetzen – tatsächlich sind die verbleibenden Betrugsquoten nach manueller Prüfung in den meisten Branchen extrem gering.

Übliche Bearbeitungszeiten im manuellen Review liegen zwischen 5 und 20 Minuten, je nach Komplexität der Einzelfälle. Es wird in der Regel ohne Belastungsspitzen gerechnet und das Personal meist unterhalb des mathematischen Optimums angesetzt.

9 SYSTEMERHALT UND -OPTIMIERUNG

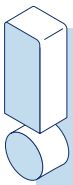
Viele Fachbereiche stehen regelmäßig vor einer Herausforderung: Das bestehende Fraud-Prevention-Tool soll optimiert werden. Oder, noch schwieriger: Die Kosten scheinen nicht mehr gerechtfertigt, und das Management fragt nach, ob man hier nicht auch einsparen könnte.

Für den Systemerhalt und die Systemoptimierung ist ein laufendes Reporting hilfreich, das den Erfolg des Systems nachweist. In der Regel wird der direkt abgewehrte Schaden abgebildet.

Das ist allerdings nicht vollständig, denn Betrugsfälle erzeugen Folgeschäden. Es ist daher korrekt, neben dem direkt abgewehrten Schaden auch den potenziell verhinderten Schaden auszuweisen. Als verhinderter Schaden wird der durchschnittliche Schaden angenommen, der durch eine/n Betrüger*in ausgelöst wird. Dieser kann, neben den direkten Kosten durch Betrug, auch indirekte Kosten und Arbeitsaufwand umfassen.

	Anzahl	Direkte Abwehr (Ø 1.000 €)	Verhinderter Schaden (Ø 2.000 €)	Kosten der Prävention in €
Alle Anträge	**100.000**			
Fraud-Management gesamt	**2.000**	**2.000.000**	**4.000.000**	**1.000.000**
Datenquelle 1: Treffer	**500**	**500.000**	**1.000.000**	**50.000**
Datenquelle 2: Treffer	**15**	**15.000**	**30.000**	**40.000**
Manueller Review	**1.800**	**1.800.000**	**3.600.000**	**320.000**

Die Abweichungen zur Gesamtsumme ergibt sich durch überschneidende Treffer in den Präventionsmaßnahmen.



Wie soll Erfolg bewertet werden?

Bei einem E-Commerce-Händler wird bei einer Erstbestellung ein Betrugsversuch festgestellt. Die Betrüger versuchten, ein Produkt im Wert von 500 € zu erhalten. Der durchschnittliche Schaden eines betrügerisch eröffneten Accounts beträgt 3.000 €. Welchen Erfolg darf das Betrugspräventionssystem für sich verbuchen?

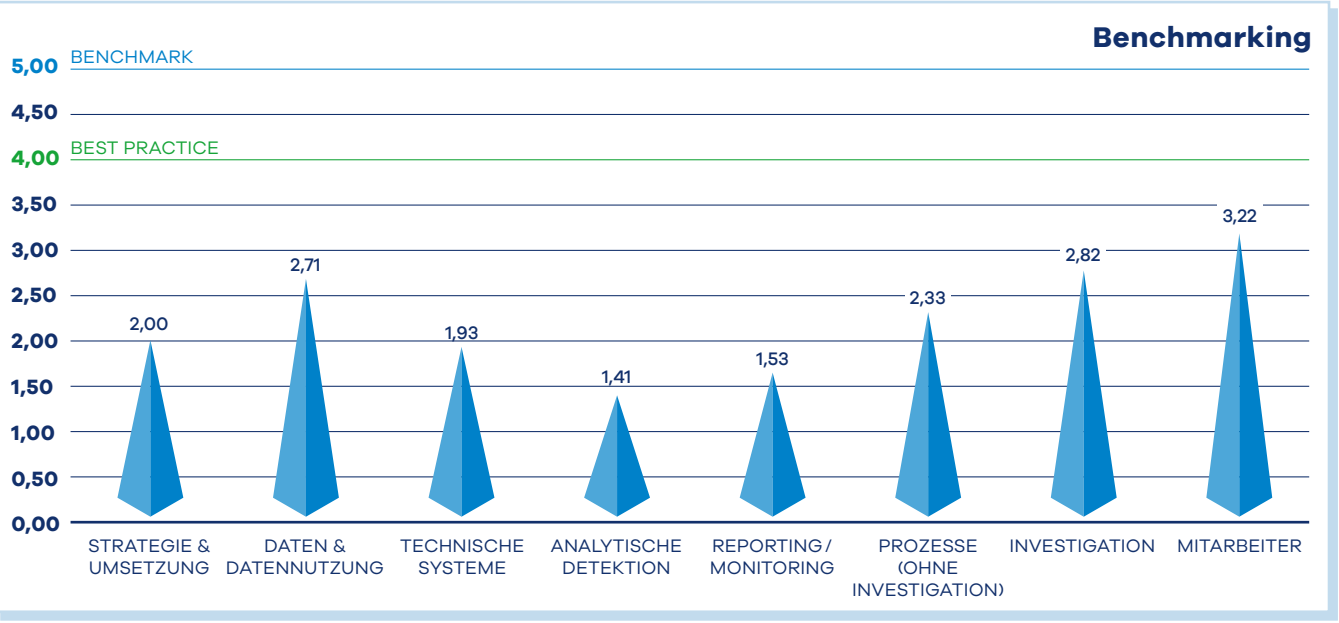
Maximalschäden durch Betrug werden außerhalb von Fachbereichen regelmäßig unterschätzt. Insbesondere professionelle Betrüger suchen nach Lücken im System, um die angedachten Grenzwerte auszuhebeln: Bestellungen werden geschickt getaktet, Geld wird einmal kurz vor und direkt nach Mitternacht abgehoben, es erfolgen zuerst Geldeingänge, um ein Limit zu erhöhen und dieses dann auszureizen usw.

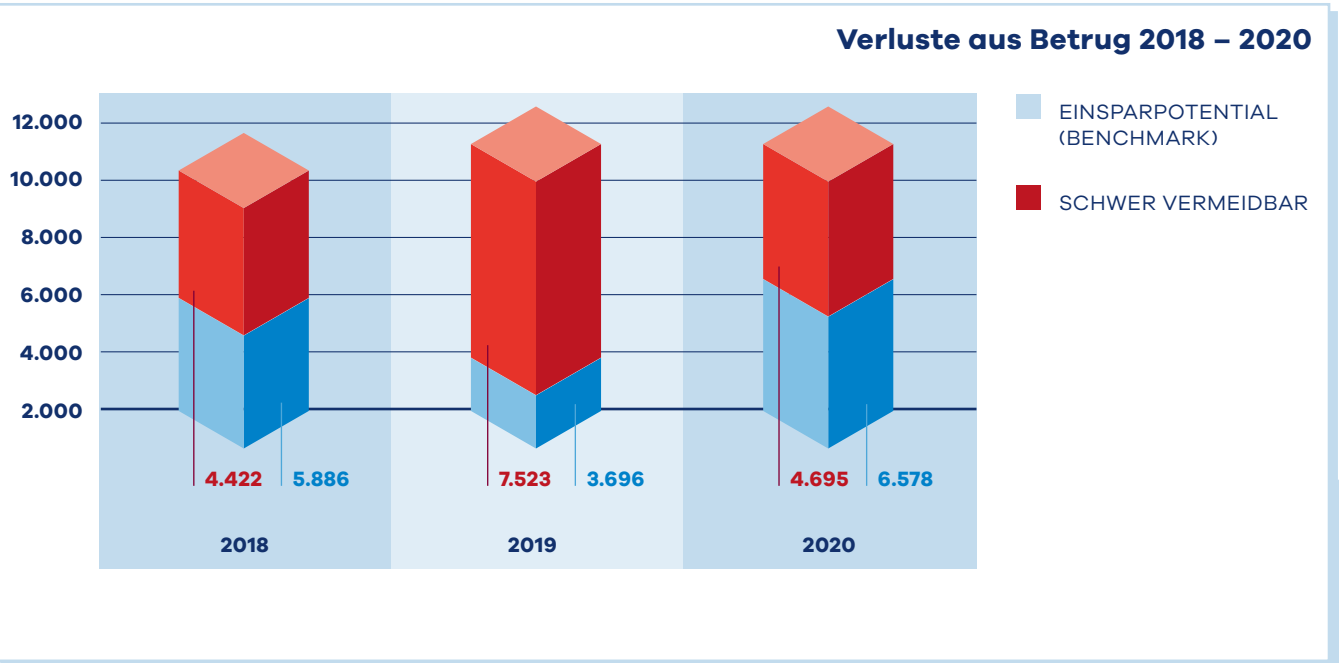
Manche Datenquellen erbringen keinen ausreichenden Wertbeitrag. Im Beispiel ist die Datenquelle 2 nur noch schwer zu rechtfertigen, denn die Kosten liegen bereits über dem verhinderten Schaden.

In der Beurteilung von bestehenden Präventionssystemen sind eine qualitative Prüfung und Argumentation mindestens so wichtig wie die Zahlen: Mit der Abschaltung von Regeln und / oder Datenquellen sollte man vorsichtig sein. Die Datenquelle im Beispiel liefert immer noch Treffer, und sollten diese „unique" sein, also nicht durch andere Quellen oder Regeln abgedeckt werden, könnte das Abschalten den Betrügern eine Lücke in der Abwehr eröffnen. Besser ist es, diese Quelle passiv mitlaufen zu lassen und genau zu überwachen. Eine Abschaltung sollte erst erfolgen, wenn die Quelle sich als dauerhaft nutzlos erweist. Übliche Fristen sind hier drei bis zwölf Monate.

Best Practice

Eine externe Überprüfung der eigenen Methoden, Systeme und der Organisation vermeidet blinde Flecken und erleichtert die Kalkulation von Business-Cases erheblich. Wir bieten Best-Practice-Analysen zur Abwehr von Antragsbetrug für Banken und E-Commerce-Unternehmen.





10 EIN AKTUELLER ANSATZPUNKT

Zum Zeitpunkt der Erstellung dieses Whitepapers gibt es einen neuen Ansatzpunkt: Im März 2021 wurde der § 261 StGB verändert. Betrug wird in vielen Fällen jetzt auch zu Geldwäsche-Verdachtsanzeigen führen. Dies hat eine erhebliche Ausweitung der operationalen Risiken bis hin zur Strafbarkeit der Geschäftsführung zur Folge. Ungenügende Präventionssysteme können im Rahmen des § 261 StGB als leichtfertige Geldwäsche angesehen werden. Dies wird zumindest eine Überprüfung und in vielen Fällen auch eine Überarbeitung der Systeme erfordern. Das Minimum sollte eine externe Überprüfung Deiner Methoden und Prozesse sein – damit kannst Du belegen, dass Dein System dem Best Practice entspricht. Falls das nicht der Fall ist, hast Du eine gute Argumentation, um Mittel zu bekommen.

Deine Chance zum Aufbau eines nachhaltigen Betrugspräventionssystems!

11 FAZIT

Betrugsprävention ist der schwierige Teil des Risikomanagements. Ein umfassendes Präventionssystem und eine fachliche und technische Systemstrategie sind (noch) selten.

Neue Angriffe und auch rechtliche Veränderungen bieten die Chance, das Thema grundlegend anzugehen und eine dauerhaft tragfähige Infrastruktur aufzubauen. Kritisch ist, dass die Täter*innen dynamisch agieren. Dies ist in der Analytik zu berücksichtigen, um schwere Fehler zu vermeiden. Außerdem sind die regelmäßige Überprüfung von Beständen und Systemen sowie der Test neuer Datenquellen und Methoden wesentliche Ansatzpunkte für eine nachhaltige Betrugsprävention. Bestenfalls wird eine Präventionsstrategie auf einem extern durchgeführten Best-Practice-Abgleich inklusive umfassender Analytik aufgebaut.

In Business-Cases gilt: Mach es Dir in Krisensituationen einfach. Rechne Dich bei der langfristigen Optimierung nicht schlecht, berücksichtige Folgeschäden, operative Prozesskosten und operationale Risiken.

Täterdynamik und Scoring / Machine-Learning

Auf Betrug ausgerichtete Scorekarten oder Machine-Learning-Modelle sind in der Entwicklung häufig sehr trennscharf.[11] Dabei wird oft übersehen, dass die Modelle nur die Vergangenheit betrachten und Erfolg prognostiziert wird, sofern das Verhalten gleich bleibt. Die entwickelten oder trainierten Modelle bilden dann meist einzelne Betrugsmuster ab. Sind die genutzten Daten nicht tatinhärent[12] oder tauchen „natürlich" immer wieder auf[13], werden Betrüger ihr Verhalten ändern, und das entwickelte Modell verliert an Trennschärfe. Transaktionsdaten sind häufig tatinhärent, Daten aus Anträgen und Bestellungen in der Regel nicht.

RISK IDENT

ÜBER RISK IDENT

RISK IDENT ist ein dynamisches, schnell wachsendes Softwareunternehmen mit Sitz im Herzen Hamburgs. Im Jahr 2012 als Tochterunternehmen der Otto Group gegründet, haben wir uns innerhalb kürzester Zeit zum Marktführer in der DACH-Region im Bereich der Betrugsprävention entwickelt. Heute können wir eine starke Kundenbasis namhafter Unternehmen vorweisen, von denen die meisten aus den Bereichen E-Commerce, Telekommunikation und Finanzdienstleistung kommen. Für unsere Kunden sichern wir jedes Jahr über 55 Milliarden € Umsatz gegen Betrug ab. Heute besteht unser Team aus über 70 Kolleginnen und Kollegen, von denen jede/r einzelne für das brennt, was wir tun.

FRIDA

FRIDA ist unsere intelligente Software gegen Online-Betrug. Dabei stellt **FRIDA** mithilfe modernster Machine-Learning-Algorithmen Verbindungen zwischen Transaktionsdaten her und erkennt Muster. Sie liefert Dir alle relevanten Informationen für eine schnelle, effiziente und zuverlässige Entscheidungsfindung.

FRIDA stellt sich auf Deine individuellen Herausforderungen in der Betrugserkennung und -bekämpfung ein, bietet intuitive Oberflächen für Deine Spezialisten und verhindert False Positives, um neben Deinem Umsatz auch Deine guten Kunden zu schützen.

In 90 Sekunden FRIDA verstehen!

Schau Dir das Produktvideo an: **riskident.com/frida**

DEVICE IDENT

Online-Betrüger hinterlassen ebenso Fingerabdrücke wie Verbrecher in der realen Welt. **DEVICE IDENT** sammelt Erkennungsmerkmale der Endgeräte, die Transaktionen auf Deiner Website durchführen – PC, Smartphone und Tablet. Diese Daten gleichen wir mit unserer globalen Datenbank ab und bewerten sie in Echtzeit, um Betrugsversuche zu stoppen, bevor überhaupt ein Schaden entsteht. Device-Fingerprinting ist das wichtigste Tool zur Fraud-Bekämpfung, bestätigt auch der MRC Fraud Report 2019.

In 90 Sekunden DEVICE IDENT verstehen!

Schau Dir das Produktvideo an: **riskident.com/device-ident**

KÖNNEN WIR DIR WEITERHELFEN?

Kontaktiere uns gerne jederzeit!

DIRK +49 151 20 10 60 68

Dirk Mayer
Fraud Expert and Catalyst
dirk.mayer@riskident.com

RISK IDENT

Risk.Ident GmbH
Am Sandtorkai 50
20457 Hamburg
www.riskident.com

12 QUELLENANGABEN

	zurück zur Seite
[01] Typischerweise wird in der Bonitätsberechnung Betrug ignoriert, bestenfalls herausgerechnet.	3
[02] Sofern keine Extremereignisse im wirtschaftlichen Umfeld eintreten. Wir werden abwarten müssen, was die Maßnahmen aufgrund von COVID-19 ausmachen.	3
[03] Z. B. Lovescam, CEO-Fraud, Boilerroom-Fraud	5
[04] Ein als betrügerisch abgewehrter Kreditkartenantrag kann mit dem Erfolg null bewertet werden, da kein Schaden entstanden ist. Alternativ kann das Kartenlimit angesetzt werden, z. B. 1.000 €. Bei typischen Betrugsfällen liegt der Schaden jedoch regelmäßig bei einem Vielfachen des Limits – eher bei 3.000 €.	5
[05] Zur Vereinfachung verzichten wir auf Abschreibungen. Und auf die Möglichkeit, dass Einsparungen von Ausfällen überhaupt nicht positiv in Business-Cases berücksichtigt werden dürfen. Findest Du unsinnig? Wir auch. Dennoch gibt es Firmen, die dies so handhaben.	7
[06] Z. B. Missbrauch von Identitäten zur Kontoeröffnung oder einzelne Tatmuster im Warenkreditbetrug	7
[07] Unserer Erfahrung nach ist der Ausbau von Maßnahmen zur Abwehr von internen Betrug (ohne Kollusion) meist eine strategische Entscheidung, die nur eingeschränkt durch Business-Cases gestützt werden muss.	9
[08] Cybersource, Global Fraud Report 2019	10
[09] D. h., aus dem Datenbestand werden zufällig Daten ausgewählt und in Gruppen für Entwicklung und Prüfung aufgeteilt. Dieses Testverfahren setzt unabhängige Datensätze voraus, dies ist in der Betrugsprävention nicht gegeben.	12
[10] Cybersource, Global Fraud Report 2019	13
[11] Gerade bei der Berechnung von Business-Cases ist diese Form der Augenwischerei häufig. Sei vorsichtig, wenn mit extrem trennscharfen Modellen geworben wird.	16
[12] Tatinhärente Daten können durch den Betrüger / die Betrügerin nicht verändert werden, da sie notwendiger Teil des Tatmusters sind. Beispiel Betrug mit Mehrwertrufnummern: Die starke Nutzung dieser Nummern ist grundlegend für dieses Betrugsmuster und kann daher auch langfristig genutzt werden.	16
[13] Verschiedene Gründe, u. a. Verfälschungen, starke Verbreitung von Mustern über das Internet	16