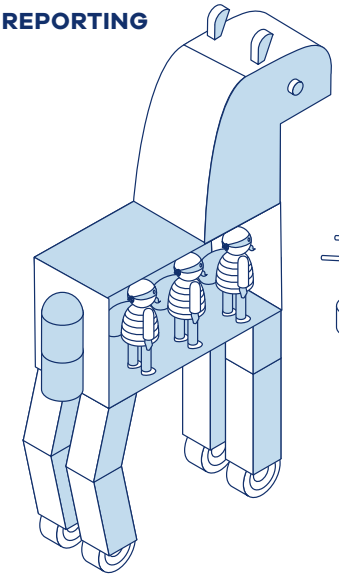
RISK IDENT

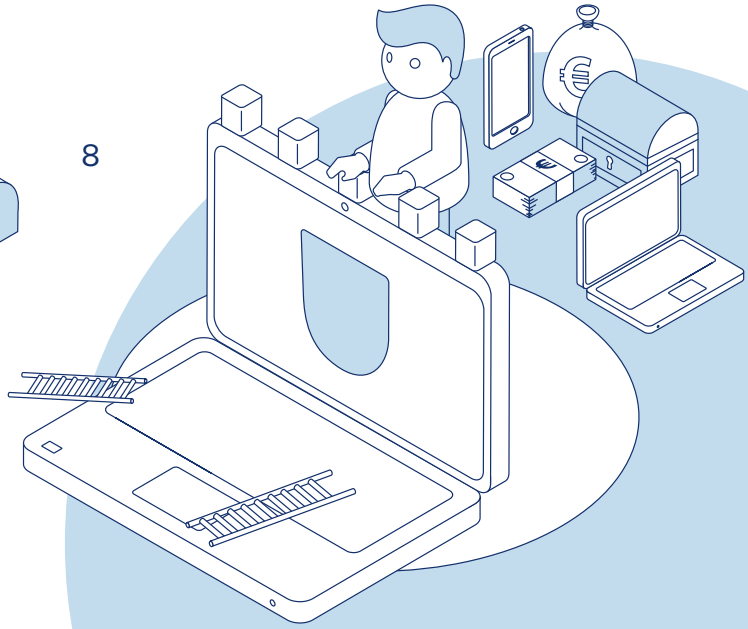
WIE SICH UNERKANNTER BETRUG ENTDECKEN UND VERHINDERN LÄSST

Eine Guideline zur Dunkelfeldanalyse

INHALT

Du kannst mich anklicken und direkt zum Kapitel gelangen!





1 EINLEITUNG

Laut Polizeilicher Kriminalstatistik ist die Kriminalitätsrate in Deutschland gesunken, allerdings nicht in allen Fällen. Die Zahl der Straftaten im Bereich Cyberkriminalität ist stark angestiegen. Die Statistik zeigt jedoch nur einen Ausschnitt, nämlich alle erfassten Straftaten. Die Dunkelziffer liegt viel höher, da laut Sicherheitsmonitor der Polizei nur 14 % der Befragten tatsächlich eine Anzeige erstattet haben. Das Gleiche gilt für Unternehmen: wir messen erkannte Betrugsfälle.

Bei Unternehmen im E-Commerce ist die Anzeigequote nach unseren Erfahrungen allerdings noch deutlich geringer: realistisch werden weniger als 1 % aller Straftaten angezeigt.[1]

Doch wieviel Betrug haben wir wirklich? Herausfinden lässt sich das mit einer Dunkelfeldanalyse.

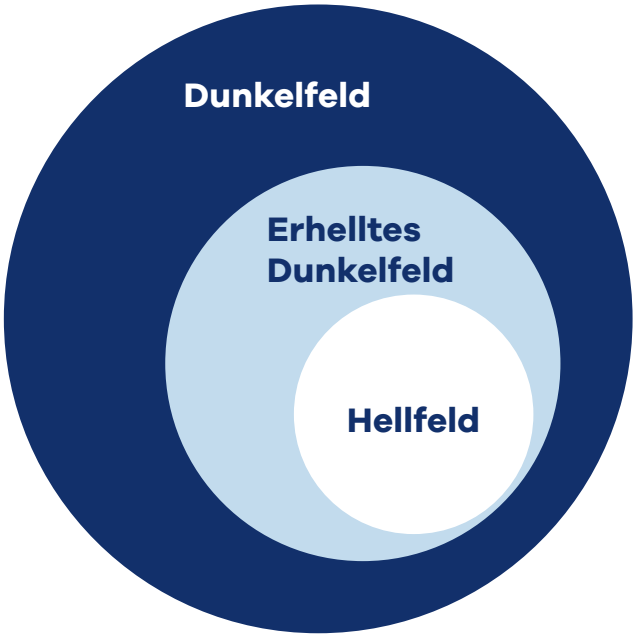
Die Betrugsversuche, die bekannt werden, sind das sogenannte „Hellfeld". Wir wissen, dass nicht jeder Betrug – und schon gar nicht alle Betrugsversuche – erkannt werden. Denn: Betrug ist ein Ermittlungsdelikt – dort, wo mehr gesucht wird, steigt die Zahl der Fälle. Und häufig gibt es viel mehr zu finden, wenn man genau hinschaut. In der Dunkelfeldanalyse untersuchen wir Daten, in denen sich weitere Betrugsfälle verstecken können. Die Ergebnisse sind vorher kaum abzuschätzen: das Dunkelfeld beträgt zwischen 5 und 95 %.[1]

2 DIE ZIELE DER DUNKELFELDANALYSE

Eine Dunkelfeldanalyse ist ein wesentlicher Teil des Risikomanagements. Die Ziele sind:

- Identifizierung möglichst aller Betrugsfälle
- Prüfung und Optimierung von neuen und bestehenden Präventionsmethoden auf ihre Wirksamkeit
- Erkennen von neuen Angriffsmustern
- Berechnung von Business Cases für Datenquellen, Systeme oder neue Prüfmechanismen

Insgesamt ist die Dunkelfeldanalyse eine analytische Methode, bei der eine idealtypische Betrugsprävention simuliert wird. Sie kann in vier Schritte unterteilt werden.



[1] Quelle: Eigene Auswertungen

3 MIT VIER SCHRITTEN DAS DUNKELFELD ERHELLEN

3.1 Die Betrugsdefinition

Die Dunkelfeldanalyse beginnt meist mit einer spezifischen Betrugsdefinition für das jeweilige Unternehmen. Was so klar aussieht, ist es selten – denken wir an nicht erreichbare Kunden, unbrauchbare Rücksendungen oder den Missbrauch von Vorteilsprogrammen. Ist das Betrug für das jeweilige Unternehmen?

In der Betrugsprävention wird daher häufig mit einer Musterdefinition gearbeitet. Dieses Muster lässt sich auf die Bedürfnisse des jeweiligen Unternehmens anpassen. Das gemeinsame Verständnis von Betrug hilft dabei nicht nur in der Analyse, sondern schafft auch eine Basis für die Zusammenarbeit verschiedener Abteilungen.

3.2 Daten, Daten, Daten

Als nächstes folgt die Zusammenstellung der Datengrundlage. Mindestinformationen für die Datenfelder sind Namen, Anschriften und Beträge. Alles darüber hinaus verbessert die Analysequalität. Übliche Datenarten sind:

- Erweiterte Personendaten:
  Geburtsdatum, Geburtsname, Geburtsort
- Kontaktdaten:
  Telefonnummer, Emailadresse, zusätzliche Adressen
- Daten zu Zahlarten, z. B. Bankverbindungen
- Produkt- und Warenkorbinformationen
- Bestandskundendaten mit Bestellhistorie, Rücksendungen, Erstattungen
- Metadaten zu Bestellungen oder Anträgen, z. B. Zeitstempel oder Geolokation des Geräts
- Zahlungsinformationen
- Informationen zur Herkunft des Kunden aus dem Marketing
- Gerätedaten
- Legitimationsdaten
- Auskunfteidaten
- Kontakte und Kontaktversuche
- Liefer- und Logistikinformationen
- Die Markierung unterschiedlicher Tatmuster, z. B. Eingehungs- oder Identitätsbetrug
- Änderungen am Kundenkonto
- Opferinformationen bei Identitätsübernahme und Account-Takeover

Typische Datenquellen, die dabei helfen können, weitere Betrugsfälle zu identifizieren, sind:

- Erkannte Betrugsfälle (Hellfeld)
- Alle weiteren Ausfälle
- Rückständige Konten
- Alle Anträge/Bestellungen inklusive abgelehnter/abgebrochener Kauf-/Antragsprozesse
- Informationen aus dem Inkasso

Soll ein Business Case für eine neue Software oder neue Datenquellen gerechnet werden, sind dazu noch Informationen über die Prozesse notwendig. Betrugsfälle erzeugen Folgekosten, die teilweise höher als die eigentlichen Schadenssummen sind. Das Optimierungspotential kann hier erheblich sein.

Ein weiterer Vorteil: neue Datenquellen testen

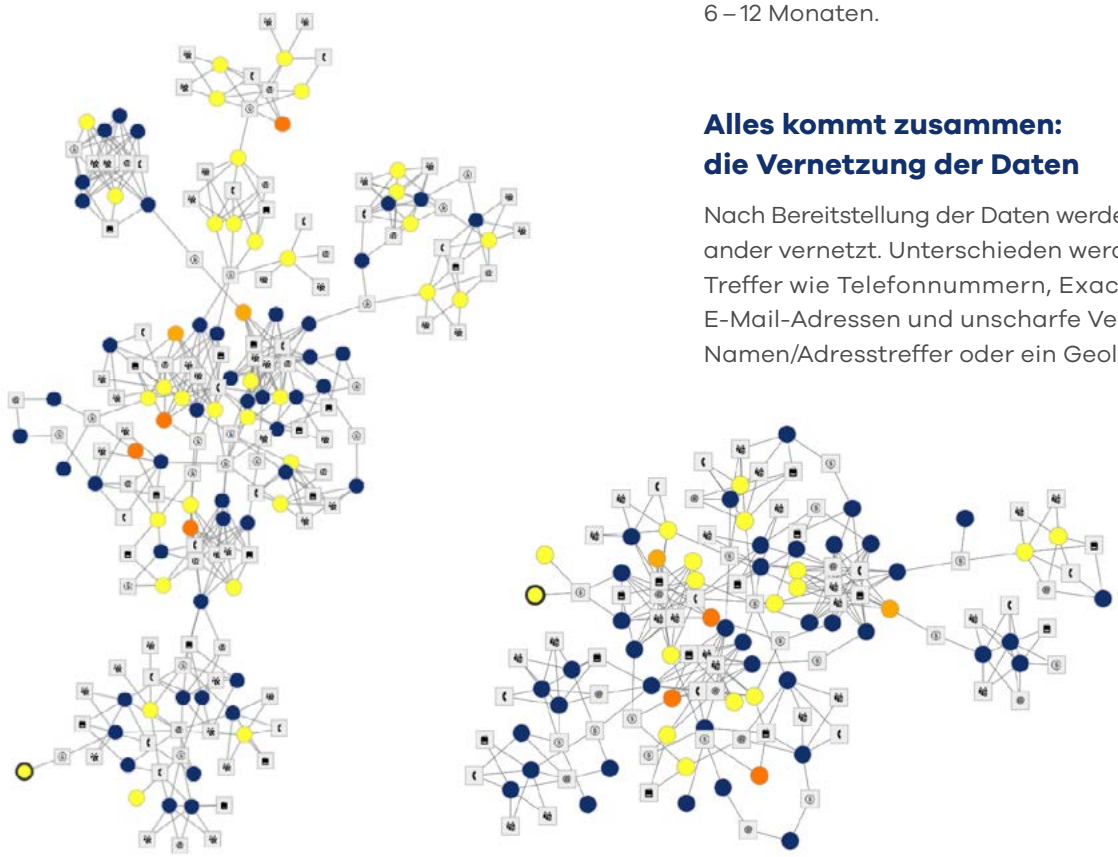
Eine Dunkelfeldanalyse ist ideal für den Test neuer Datenquellen. Einige können auch im Nachhinein angereichert werden. Dazu müssen die Quellen in der Lage sein, den Datenbestand zum Zeitpunkt des Antrags / der Bestellung auszugeben („retrospektive Anreicherung"). Bei Datenarten, die nur im Prozess selbst zu erheben sind, ist dies nicht möglich. Hierzu zählen z. B. Device Fingerprinting, Verhaltensdaten oder biometrischen Informationen. Bei der Konzeption einer Dunkelfeldanalyse ist es daher zielführend, die Erhebung angedachter Daten möglichst schnell zu starten, damit diese in der Analyse vorliegen.

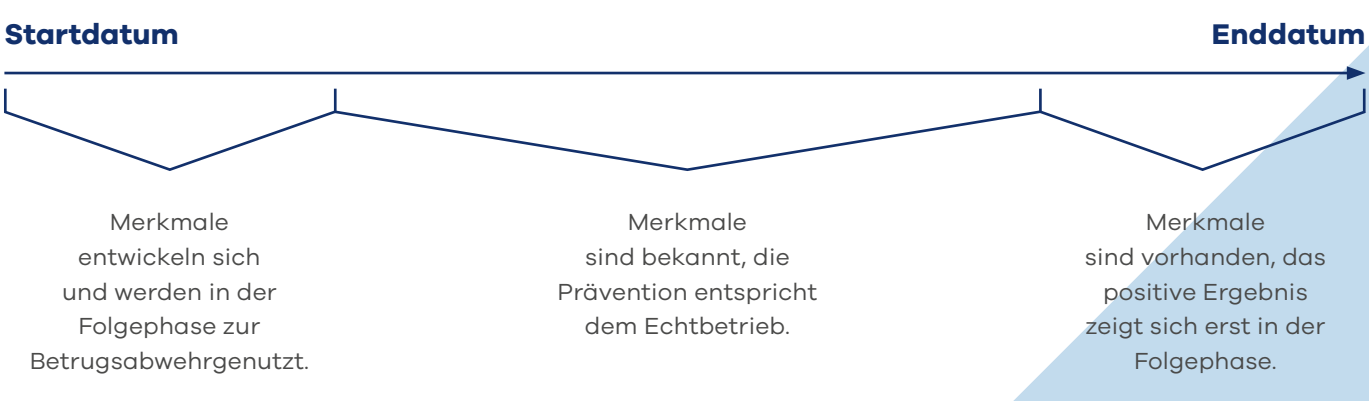
Achtung beim zeitlichen Umfang der Daten

Die Analytik der Betrugsprävention unterscheidet sich von der Berechnung bonitätsorientierter Ausfallwahrscheinlichkeiten. Die Vollständigkeit und die zeitliche Abfolge von Anträgen / Bestellungen sind in der Betrugsanalytik wichtiger: Ein neu erkannter Betrugsfall kann eine ganze Kette anderer Verdachtsfälle aufzeigen. Denn betrügerisches Verhalten zeigt sich eventuell nur im Zeitverlauf mehrerer Anträge / Bestellungen. Aus diesen Gründen sind Zufallsstichproben für die Dunkelfeldanalyse nicht geeignet. Beim zeitlichen Umfang müssen wir berücksichtigen, dass in den Daten am Anfang und am Ende nur ein Teil des Potentials gezeigt werden kann. Üblich sind Tests mit einem Datenumfang von 6 – 12 Monaten.

Alles kommt zusammen: die Vernetzung der Daten

Nach Bereitstellung der Daten werden diese miteinander vernetzt. Unterschieden werden eindeutige Treffer wie Telefonnummern, Exact-Device-IDs oder E-Mail-Adressen und unscharfe Verbindungen, z. B. Namen/Adresstreffer oder ein Geolokations-Umkreis.





3.3 Die Identifizierung zusätzlicher Verdachtsfälle

Auf Basis der Definition und der vorhandenen Daten werden Regeln definiert, mit denen wir erste zusätzliche Verdachtsfälle im Datenbestand identifizieren können. Einige Beispiele hierfür sind:

- Bei einer Kreditherauslage zahlt der Kunde weniger als drei Raten („early default")
- Ein rückständiger Kunde ist mehr als drei Monate nicht auffindbar
- Ein Kundenkontakt ist über die angegebenen Daten nicht möglich
- Es erfolgen weniger als fünf bezahlte Bestellungen mit einer Summe kleiner als 100 € gefolgt von einer Zahlung / Bestellung größer als 1.000 €, die dann nicht bezahlt wird
- Der Kunde gibt an, die Ware nicht erhalten zu haben, will aber keine Strafanzeige stellen

Die Beispiele zeigen die Bedeutung der Betrugsdefinition: nur mit einer klaren Vorstellung, was als betrügerisches Verhalten angesehen wird, können solche Regeln aufgestellt werden.

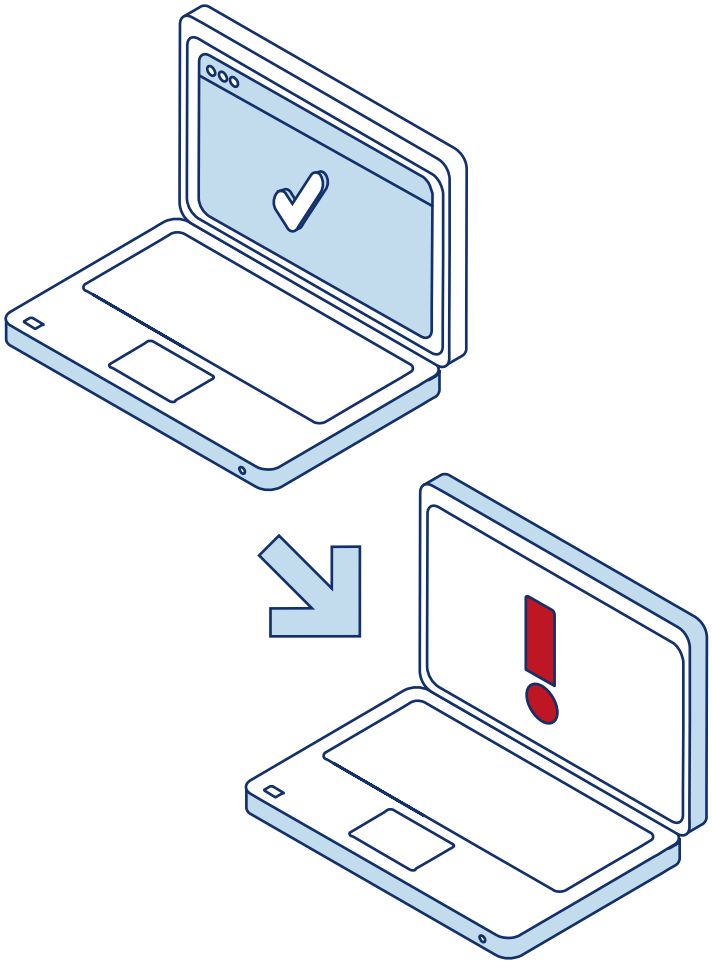
Sinnvoll ist es, diese Fälle einem konkreten Tatmuster zuzuordnen. Dadurch lassen sich später im Bestand Veränderungen, Schwerpunkte und Trends feststellen. Für verschiedene Angriffe können wir so unterschiedliche Abwehrstrategien entwickeln.

Ein zweites Set an Regeln zielt auf die Anträge / Bestellungen ab, die mit allen bisher markierten Anträgen / Bestellungen im Datennetz verbunden sind:

- Verbindungen zu erkannten Betrugsfällen
- Verbindungen zu Verdachtsfällen
- Plausibilitätsfehler in verbundenen Anträgen / Bestellungen, z. B. gleiches Gerät und unterschiedliche Personen

Bei Verwendung unscharfer Verbindungen können Wahrscheinlichkeiten genutzt werden, um das gesamte Risiko korrekt einzuschätzen. Eine Adresse kennzeichnet nicht eindeutig eine Person!

Auch diese Anträge / Bestellungen werden als Verdachtsfälle markiert. Alle jetzt markierten Anträge / Bestellungen stellen das sogenannte „erhellte Dunkelfeld" dar.



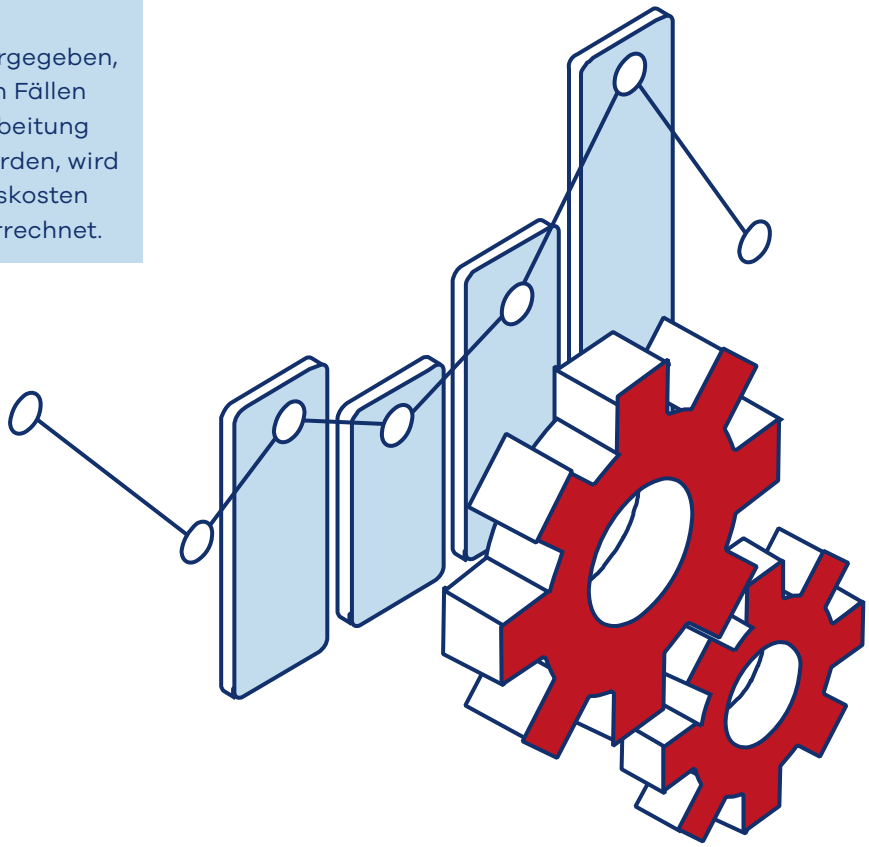
3.4 Die Königsklasse der Analytik

In dem entwickelten Datenbestand können sich nun die Analytiker austoben. Anomalie-Erkennung, Cluster-Analysen und Machine-Learning-Verfahren liefern trennscharfe Parameter und Algorithmen. Diese können mit Kreuzanalysen und Regelkombinationen optimiert werden.

Die wichtigste Kennzahl ist die False / Positive-Quote: Für jede Regel, jeden Algorithmus und jedes Entscheidungsset kann angegeben werden, wie viele „falsche" Treffer auf einen erkannten Betrugsfall kommen.

Den Abschluss bildet die Feststellung des Wertbeitrags einzelner Datenquellen und die Berechnung von Business Cases für Software und Umsetzungsmaßnahmen. Es gibt dazu keine Universallösung, da die Ergebnisse von den Prozessen, den vorhandenen Systemen und der Strategie des Unternehmens abhängt.

Ein Beispiel für unterschiedliche Berechnungen eines Wertbeitrags:
Ist die Anzahl der Mitarbeiter fest vorgegeben, kann nur eine beschränkte Menge an Fällen geprüft werden. Können für die Bearbeitung auch neue Mitarbeiter eingestellt werden, wird das Optimum zwischen den Prüfungskosten und den erwarteten Einsparungen errechnet.



4 RISIKEN DER DUNKELFELDANALYSE

Ein besonderes Risiko der Dunkelfeldanalyse ist, dass bereits vorhandene Datenquellen oder Systeme keinen ausreichenden Wertbeitrag liefern und daraufhin abgeschaltet werden. Hierbei muss aber berücksichtigt werden, dass bei Methoden der Betrugsprävention ein Abschreckungseffekt entsteht und damit effektive Methoden rückblickend nutzlos erscheinen mögen: Die Betrüger haben nicht angegriffen, weil die Methode vorhanden ist. Grundsätzlich ist ein „Abrüsten" von Datenquellen in der Betrugsprävention schwierig, da die Folgen kaum absehbar sind. Und auch hier gibt es sinnvolle Maßnahmen, die jedoch individuell festzulegen sind.

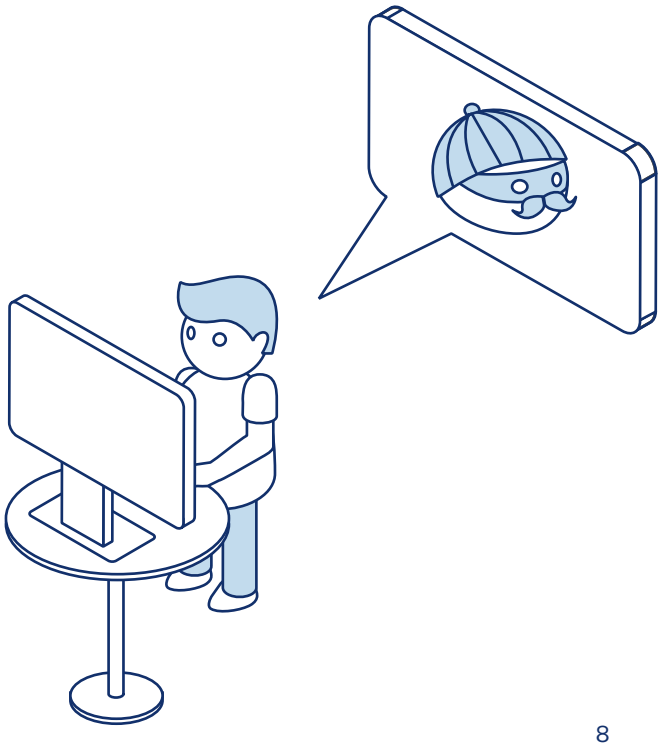
Ein Beispiel für ein Risiko beim Abschalten von Präventionsmaßnahmen:
Die bisher eingesetzte Überprüfung von Kontoverbindungen zeigt keinen ausreichenden Wertbeitrag, die Abfrage ist teuer und liefert zu viele fehlerhafte Treffer. Die Abfrage wird abgeschaltet. Im nächsten Quartal gibt es dann unerwartet viele Betrugsfälle – denn mit dem Abschalten der Präventionsmaßnahme wurde Lastschriftbetrug wieder möglich.

5 INTEGRATION IN DAS REPORTING

Die Methoden der Dunkelfeldanalyse können meist einfach in ein laufendes, internes Monitoring überführt werden. Auf dieser Basis werden dann auch dauerhaft neue Trends und Risiken erkannt und können bekämpft werden, bevor ein großer Schaden entsteht.

Die Dunkelfeldanalyse ist eine der wichtigsten Methoden der Betrugsprävention, denn Betrug ist ein Spiel mit dynamischen Gegnern, die sich auf unsere Methoden einstellen.

Du fragst dich, wie viel Betrug ihr tatsächlich habt? Vereinbare einen unverbindlichen Termin mit unseren Experten und bring Licht ins Dunkel.



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.

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