fraud prevention

So schützen Sie Ihr Business vor Betrügern!

Dossier
unter Mitwirkung von CRIF

Herausgeber
Oliver Jonke
[o.jonke@medianet.at]

Editorial

Bad News für Betrüger

Sehr geehrte Leserinnen und Leser,
falsche Identitäten, Missbrauch von existierenden Identitäten, Never Payer uvm – die kriminelle Energie so mancher Täter scheint ungebrochen zu sein. Vielleicht, weil sie noch nicht wissen, dass sich in zahlreichen Unternehmen superprofessionelle Task Forces gebildet haben, die sehr erfolgreich einen Betrüger nach dem anderen zur Strecke bringen.

Ist Fraud unterhaltsam?
Ob Thomas Manns Roman „Bekenntnisse des Hochstaplers Felix Krull" oder Spielbergs „Catch me if you can" – Betrug entwickelt manchmal einen hohen Unterhaltungswert. Betrugsopfer sehen das wohl mit weniger romantischer Verklärung.

Vielleicht sind auch Sie sogar schon einmal betroffen gewesen und haben es nicht gleich gemerkt? Das wäre in unserer digitalen Welt kein Wunder. So berichtet die *New York Times* am 3. Oktober 2017, dass laut dem neuen Yahoo-Eigentümer Verizon Communications im Jahr 2013 alle drei Milliarden (!) Yahoo-Accounts von Hackern abgegriffen wurden.

Können Sie sich noch an das Riesenmalheur der oberösterreichischen FACC erinnern? Der renommierte Luftfahrtzulieferer wurde um 50 Mio. Euro betrogen, hier jedoch nicht durch Cyberbetrug, sondern in diesem Fall, weil ein Mitarbeiter bei FACC betrügerisch ‚benutzt' wurde.

Einen hohen Unterhaltungswert können aber auch manche Aufklärungsberichte zu Betrugsfällen entwickeln. Viele Betrüger werden ja mitunter deswegen erwischt, weil sie eben nicht gerade genial sind.

Es hat sich zum Beispiel bei Online-Käufen als nicht sonderlich weise erwiesen, Video- Identifikation mit falschen Dokumenten auszuprobieren … Videos mit den dümmsten Betrügern erfreuen sich auch zum Beispiel auf YouTube einer entsprechenden Beliebtheit.

Gegen Betrug ist man nicht machtlos. Das hier vorliegende Dossier beleuchtet das Thema aus der Sicht von Finanzinstituten und Unternehmen, die mit Betrug im Rahmen von Online-Geschäftsabschlüssen konfrontiert sind. Es beschäftigt sich mit verschiedenen Zahlen, Daten und Fakten sowie wesentlichen Aspekten zur Vorkehrung und Aufdeckung rund um dieses Thema. Es entstand im Auftrag und unter Mitwirkung des in Österreich und international im Kampf gegen Fraud erfolgreichen Dienstleisters CRIF. Weiters haben bei diesem Dossier führende Fraud-Experten aus österreichischen Unternehmen und Finanzinstituten mitgewirkt.

Eine anregende Lektüre wünscht Ihnen
Oliver Jonke

Dossier: fraud prevention

Coverfoto:
© PantherMedia/Elnur_

Inhalt

© medianet/Joe Haider (2)

Impressum

Medieninhaber:
medianet Verlag GmbH
1110 Wien, Brehmstraße 10/4. OG
http://www.medianet.at

Diese Sonderausgabe wurde von **media**net unter Mitwirkung von CRIF erstellt.

Konzept: Oliver Jonke (Herausgeber)
Kontakt: o.jonke@medianet.at

Leitende Redakteurin dieser Ausgabe:
Helga Krémer (hk)

Lektorat: Christoph Strolz ***Grafik/Produktion:*** Raimund Appl, Peter Farkas ***Fotoredaktion/Lithografie:*** Beate Schmid ***Druck:*** Ferdinand Berger & Söhne Ges.m.b.H., 3580 Horn
Erscheinungsort: Wien ***Stand:*** Juli 2018

Für den Inhalt verantwortlich:
CRIF GmbH, 1150 Wien, Diefenbachgasse 35

Abo, Zustellungs- und Adressänderungswünsche:

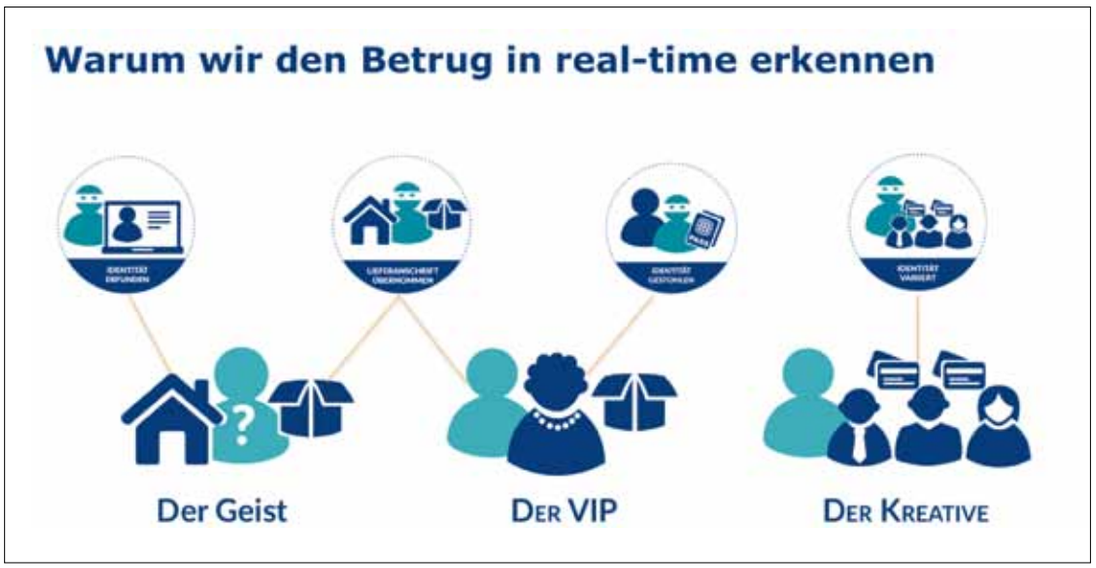
abo@medianet.at
oder Tel. 01/919 20-2100

Betrug rechtzeitig orten

Online-Fraud nimmt immer mehr zu – in der Häufigkeit, aber auch in der Schadenssumme. Das sind die häufigsten Betrugsmuster.

••• *Von Helga Krémer*

WIEN. Online-Betrugsfälle nehmen zu und werden zudem gefinkelter. Die Schäden sind enorm, uneinbringliche Inkassofälle machen Unternehmen das Leben schwer. Die „Kopf-in-den-Sand-steck"-Einstellung ist da genauso nicht empfehlenswert wie Großspur-Attitüden à la „so-was-passiert-doch-mir-nicht". Der Ansatz „Vertrauen ist gut. Kontrolle ist besser.", ist da schon hilfreicher. Hier die Vorstellung der besonders dreisten Betrugstypen:



© CRIF

Online-Fraud 1: „Der Geist"
Der Betrüger bestellt bei der Variante „der Geist" online ein Produkt mit einer realen Anschrift als Lieferadresse. Die Rechnung geht allerdings an eine erfundene Person an eine erfundene Adresse – „der Geist" ist erfunden und spukt ab sofort in der Buchhaltung des Online-Händlers. Mahnungen gehen ins Leere. Im Schadensfall kann der Online-Händler genau gar nichts machen, im Fachjargon nennt sich das dann „Inkassofall – uneinbringlich". Der Betrüger hat mittlerweile seine Bestellung abgefangen.

Online-Fraud 2: „Der VIP"
Die Vorgangsweise beim „VIP" ist der des „Geistes" nicht unähnlich. Wieder wird mit einer von der Rechnungsadresse abweichenden Lieferanschrift bestellt.

Die Besonderheit am „VIP"-Fraud ist, wie der Name richtigerweise vermuten lässt, Name und Adresse auf der Rechnung gehören einer bekannten Persönlichkeit. Der Betrüger erhält die Bestellung, die Rechnung geht an den VIP. Damit werden bei dieser Betrugsart nicht nur Waren, sondern auch Identitäten berühmter Personen gestohlen. Auf dem Schaden bleibt der Händler, genauso wie beim „Geist", mit einem „Inkassofall – uneinbringlich", sitzen.

VIP-Betrug
Was so mancher VIP im Laufe seines VIP-Lebens schon alles vermeintlich bestellt hat, darüber gibt es keine Aufzeichnungen. Die berühmte Person wird es auch nicht wissen wollen.

Online-Fraud 3: „Der Kreative"
Dieser Betrüger vertraut auf seine Kreativität – in dem Sinne, dass er mit *seinem* Namen und/oder *seiner* Adresse „spielt". So wird aus einer „Anna" bei der Bestellung eine „Anne" gemacht, aus einem „Stephan" ein „Stefan", aus der „Teichgasse" wird „Reich-", „Taich-" oder „Tiechgasse": Die Antragsdaten variieren. Und schon wieder kann sich der Händler nur ärgern: „Inkassofall – uneinbringlich", Klappe, die dritte.

Wie man anhand dieser Betrugsarten erkennt, gehen Betrüger sehr kreativ mit Bestell- bzw. Antragsdaten um und verursachen damit bei Händlern große Schäden. Glücklicherweise gibt es Wirtschaftsauskunfteien wie CRIF, die jetzt eine Lösung zur Betrugsbekämpfung entwickelt haben.

In Österreich ist die CRIF GmbH der führende Anbieter von Kreditrisikomanagement-Lösungen, Fraud Prevention und Entscheidungsmanagement entlang des gesamten Kundenlebenszyklus.


© PantherMedia/zurijeta

Online-Fraud
Die Wirtschaftsauskunftei CRIF hat diese drei Betrugstypen herausgearbeitet: „der Geist", „der VIP" und „der Kreative".

Betrugsbekämpfung
CRIF sammelt, strukturiert und kombiniert Kredit- und Wirtschaftsinformation von Privatpersonen und Unternehmen und bietet eine Identifikationsquote von 95%.

„Vertraue, aber prüfe nach", lautet ein altes russisches Sprichwort. Im Laufe der Zeit wurde daraus die Redewendung „Vertrauen ist gut. Kontrolle ist besser.", sie beschreibt eindrucksvoll das Verhältnis des Unternehmers zu seinem Kunden. Grundsätzlich ihrer Kundschaft vertrauend, sind Online-Händler besser beraten bei den Bestellerdaten Vorsicht walten zu lassen. Damit sich kein „kreativer-VIP-Geist-Betrüger" einschleichen kann.

„Wir können Online Fraud gemeinsam, wirksam und professionell bekämpfen", heißt es bei CRIF. Wie die Wirtschaftsauskunftei im Detail vor Betrügereien in der Welt des Online-Handels schützen kann, will dieses Dossier zeigen.

© CRIF

Better safe than sorry

Wie man sich vor dem Hintergrund steigender Online-Transaktionen vor Betrügern schützen kann, diskutierte der **media**net Round-Table.

Vertrauen ist gut, Kontrolle ist besser. Die Fälle von Identitätsdiebstahl und vorsätzlichen Betrug im Online Handel steigen. Betroffen sind nahezu alle Branchen, besonders aber e-Commerce und Telekommunikationsunternehmen, Leasing- und Kreditinstitute. Allerdings, so vielfältig die Betrügereien, so vielfältig sind die Maßnahmen, die ein Unternehmen setzen kann.

Laut einer CRIF-Umfrage im DACH-Raum wird als Betrugsprävention am meisten auf die „Manuelle Prüfung" vertraut. Bei CRIF hat man drei Betrugsmuster isoliert: den Geist, den VIP und den Kreativen

Betrugsformen
Laut einer CRIF-Umfrage werden die verschiedenen Formen des Identitätsbetrugs nur mehr von der Zahlungsunfähigkeit „getoppt"; Die Plätze 2 bis 4: die variierende, die gestohlene, die erfundene Identität.

Man braucht einen gesunden Menschenverstand. Hilfreich ist es, wie ein Betrüger zu denken, um einen Betrüger zu finden.

Daniela Jordanich

© medianet/Joe Haider (2)

Es ist ja auch für Unternehmen ein großer Wettbewerbsvorteil, wenn sie auf offene Rechnung anbieten können.

Boris Recsey

(*siehe Seite 3*). „Aufgrund unseres Datenuniversums erkennen wir erfundene Identitäten und abweichende Lieferadressen. Bei diesen abweichenden Lieferadressen können wir zudem anzeigen, ob sie belastet sind. Zusätzlich können wir kritische Adressen hervorheben.“, erklärt Gerald Sebastian Eder, Business Development Manager bei CRIF. Anschriften von Männerwohnheimen seien leider immer wieder Treffer, weiß man bei CRIF. Hier zeigt sich eine Schwachstelle der manuellen Antrags- oder Bestellüberprüfung: Einem Wiener Onlinehändler würde der „Generaldirektor XY in der Meldemannstraße“ wahrscheinlich auffallen. „Dieses Wissen hat aber ein Händler in, zum Beispiel, Hamburg nicht. Im reinen Distanz- oder Onlinehandel weiß er das nur über eine Auskunftei“, gibt Boris Recsey, Geschäftsführer bei CRIF, zu bedenken und kommt auf eine „Spezialität“ des DACH-Raums im eCommerce zu sprechen, die Lieferung auf offene Rechnung: „In Tschechien, Polen oder der Slowakei ist das nicht so üblich, dass der Konsument oder Verbraucher die Möglichkeit hat, die Ware erst nach der Lieferung zu bezahlen. Ich denke, das ist ein großer Service der kreditgebenden Wirtschaft, diese Zahlungsmethode anzubieten. Aufgrund der Erfahrungen, die wir gemeinsam mit unseren Kunden im DACH-Raum machen, können wir auch Händler in anderen Ländern beim Ausrollen neuer Geschäftsmodelle beraten. Es ist erwiesenermaßen ein großer Wettbewerbsvorteil für Unternehmen, wenn sie auf offene Rechnung anbieten können, da die Conversion Rate steigt. “

Möglichkeiten der Prävention

Was also tun? „Im Shop, am Point-of-Sale, ist die Hemmschwelle im Vergleich zum Internet für einen Betrüger schon noch zu hoch“, erläutert Mohamed Ibrahim, Head of Costumer Finance bei T-Mobile Austria; die Angst, mit gefälschten Dokumenten im Shop „aufzufliegen“, sei einfach zu groß.

„Am einfachsten und derzeit effizientesten ist für uns, das via Upload hochgeladene Dokument automatisch, in Echtzeit mittels Fraud Prevention Kit von CRIF zu überprüfen“, ergänzt Ibrahim. Wer treibt bei T-Mobile am ehesten sein Unwesen? „Der Kreative – mit bestimmten E-Mail-Adressen, Anschriften, oder IP-Adressen – der Kit deckt dies in Echtzeit ab.“

„Bei Online-Vertagsabschlüssen gilt es daher, weitere Barrieren gegen Betrug aufzubauen. Eine Möglichkeit ist zum Beispiel die Identifikation mittels Video-Call“, betont **media**net-Herausgeber Oliver Jonke.

Bei Raiffeisen hat man gute Erfahrungen mit der Legitimierung mittels Video-Identifikation gemacht. „Es ist besser als

Aufgrund unseres Datenuniversums erkennen wir erfundene Identitäten und abweichende Lieferadressen.

Gerald Sebastian Eder

Eine gute Betrugsprävention erhöht das Kundenvertrauen – und ist daher sehr wirkungsvoll für die Kundenbindung.

Christoph Nissl

Kein Betrüger möchte sein Gesicht zeigen, kein Betrüger möchte sein Gesicht gespeichert wissen. Daher ist die Video-Legitimation generell gut.

Doris Brandt Kalla

© medianet/Joe Haider (7)

der Mensch, weil der Mensch einfach nicht alle Ausweismerkmale erkennen kann. Das schafft das System sehr viel einfacher. Der Mensch ist überfordert, wenn er einen ihm unbekannten Ausweis sieht. Der Mensch ist auch überfordert, das Bild im Ausweis mit dem Antragsteller zu vergleichen. Wir verändern uns, werden älter, das kann das System besser abgleichen", sagt Doris Brandt-Kalla, Fraud Risk Manager bei der Raiffeisen Bank International.

Die Video-Identifikation allein sei auch schon Abschreckung genug, sagt Recsey. Dieses Feedback hat Brandt-Kalla auch schon bekommen: „Kein Betrüger möchte sein Gesicht zeigen, kein Betrüger möchte sein Gesicht gespeichert wissen. Daher ist die Video-Legitimation generell gut zur Betrugsprävention."

Kunden glücklich machen

„Eine gute Betrugsprävention über eine Auskunftei, wie zum Beispiel CRIF oder auch über andere Wege, verhindert ja nicht nur den Schaden, sondern macht auch unsere Kunden glücklich", bringt Christoph Nissl, Leiter der Abteilung Betrugsprävention und -management der BAWAG P.S.K., eine weitere Facette in die Diskussion ein. „Wenn ich das gut mache, wenn ich das ‚trennscharf' und zielsicher mache, dann haben meine Kunden bei mir ein gutes Gefühl. Wir schauen bei uns ganz genau, dass wir, wenn wir Betrugsprävention einsetzen, eine gute Balance zwischen erfolgreicher Prävention und geringer Kundeneinschränkung haben."

Schließlich ginge es auch darum, dass der ehrliche Kunde *rasch* zu seiner Dienstleistung kommt, erinnert Boris Recsey, oder auch gute Konditionen bekäme.

Zwischen Betrug und Geschäft

Von allen Seiten hat es die Versicherungsbranche mit Betrug zu tun: als Assekuranz, aber auch bei den Schadensfällen – sowohl vom Versicherten als auch vom Vertragspartner und von Dritten. „Wir haben da keine validen Zahlen, aber es gibt Schätzungen, die besagen, dass bis zu 20 Prozent der Schadensfälle zumindest teilweise Betrug beinhalten", meint Alexander Gorth, Leiter Kfz der ERGO Versicherung; es sei des öfteren der Fall, dass echte Schäden

Die Teilnehmer

Doris Brandt-Kalla
Fraud Risk Manager,
Raiffeisen Bank International

Gerald Sebastian Eder
Business Development Manager,
CRIF

Alexander Gorth
Leiter Kfz,
ERGO Versicherung

Mohamed Ibrahim
Head of Customer Finance,
T-Mobile Austria

Daniela Jordanich
Senior Fraud Investigator,
Erste Group Bank

Christoph Nissl
Abteilungsleiter Betrugsprävention und -management,
BAWAG P.S.K.

Boris Recsey
Geschäftsführer CRIF

Moderation: Oliver Jonke
Herausgeber **media**net

„ausgedehnt" würden, und es würden auch Schadensfälle komplett erfunden, „aber man darf nie vergessen: die Mehrheit der Kunden ist ehrlich".

Auf der anderen Seite? „Wir arbeiten gerade an einem neuen Gewerbeprodukt, wo solche Bestandteile wie Cyberbetrug auch berücksichtigt werden. Zielgruppe sind kleine und mittlere Unternehmen", erklärt Gorth.

Wer ist jetzt besser? Mensch? Maschine? Technik? „Die Unterstützung durch die Technik oder bestimmte Dienstleister, die man zukauft, ist sicher da, aber im Endeffekt zählt letztendlich die Man-Power. Am Schluss muss bei uns ein *Mensch* ‚drüberschauen' und man braucht ja auch die Manpower, um die Maschine zu ‚füttern'", meint Daniela Jordanich, Senior Fraud Investigator der Erste Group Bank, und beschreibt die Notwendigkeiten ihres Berufsbilds: „Man braucht einen gesunden Menschenverstand. Hilfreich ist es, wie ein Betrüger zu denken, um einen Betrüger zu finden."

„Wir unterstützen unsere Kunden bei der Automatisierung und Digitalisierung des kompletten Kundenantragsprozesses und liefern dabei Daten zur Identitäts-, Bonitäts- und Fraud Prüfung. Dabei ist es wichtig, wirklich jeden Kauf, unabhängig von Größe und Art des Warenkorbs, zu prüfen, um Betrügern keine Chance zu geben", so Eder abschließend.

Wir haben da keine validen Zahlen, aber es gibt Schätzungen, die besagen, dass bis zu 20 Prozent der Schadensfälle zumindest teilweise Betrug beinhalten.

Alexander Gorth

Bei Online-Vertragsabschlüssen gilt es daher, weitere Barrieren gegen Betrug aufzubauen. Eine Möglichkeit ist etwa die Identifikation mittels Video-Call.

Oliver Jonke

Im Shop, am Point-of-Sale, ist die Hemmschwelle im Vergleich zum Internet für einen Betrüger schon noch zu hoch.

Mohamed Ibrahim

CRIF hat die Lösung

Die Verhinderung von Betrugsfällen muss noch stärker in den Fokus rücken. Mit dem richtigen Partner ganz leicht.

WIEN. Die Zahl der Online-Transaktionen steigt und steigt, die Digitalisierung nimmt mehr und mehr zu. Damit treten leider vermehrt Fälle von Identitätsdiebstahl und vorsätzlichem Betrug auf – sehr zum Leidwesen der Unternehmen, die mit dieser Thematik zu kämpfen haben. Besonders stark betroffen sind dabei die Branchen eCommerce und Telekommunikation, aber auch die Branchen Leasing und Kreditinstitute berichten von Betrugsfällen.

Wie schön wäre es, könnte man schon vorher wissen, mit wem man sich gleich vertrags- und zahlungstechnisch „ins Bett legt".

Überprüfung in Echtzeit

Mit dem Fraud Prevention Kit von CRIF kann man genau das: CRIF überprüft und analysiert anhand ausgewählter Kriterien in Echtzeit (!) den Antrag des potentiellen Kunden auf bekannte Betrugsmuster. Das Unternehmen erhält *sofort* die Information, ob es sich um einen möglichen Betrugsversuch handelt, oder eben nicht. Damit stellt CRIF nicht nur ein einfaches und zugleich effektives Instrument zur Betrugsbekämpfung zur Verfügung – auch Forderungsausfälle lassen sich so vermeiden.

Rot–gelb–grün

Das Fraud Prevention Kit gilt als Erweiterung zum bestehenden „Credit Check Consumer" und liefert daher zusätzliche Informationen zur abgefragten Person. So stellt die sogenannte Bonitätsampel das Gesamtergebnis dar, in einer separaten Darstellung wird das jeweilige Betrugsrisiko angezeigt. Auf einen Blick kann damit in Sekundenschnelle die Entscheidung über die weitere Vorgangsweise getroffen werden.

© PantherMedia/stevanovicigor

Nicht mit mir! Betrügern endlich aktiv entgegentreten: das CRIF Fraud Prevention Kit macht's möglich.

Die Key-Features

Das Endgerät, von dem aus der Kauf durchgeführt oder der Antrag verschickt wird, verfügt über eine Geräte-ID. Durch diesen eindeutigen Fingerabdruck können in Kombination mit den Personendaten des Unternehmens allfällige Betrugsmuster schnell erkannt werden.

Mithilfe des Verification Scores erhält das Unternehmen den Hinweis, wie gut und wie lange die Identität der infrage stehenden Person bei CRIF bekannt ist. Der Score wird in Kategorien zwischen „A" und „D" zugeordnet und ermöglicht die Erkennung von Risikokunden, auch wenn keine negativen Zahlungserfahrungen bekannt sind.

Die Fraud-Kategorie gibt an, wie kritisch eine Bestellung in Bezug auf einen möglichen Betrugsversuch ist. Auch Fraud wird in Kategorien von „A" bis „D" eingeteilt und regelbasiert berechnet. Hier werden sowohl Antragswiederholungen, als auch die wiederholte Verwendung selbiger Antragsdaten geprüft, um Betrugsfälle zu erkennen.

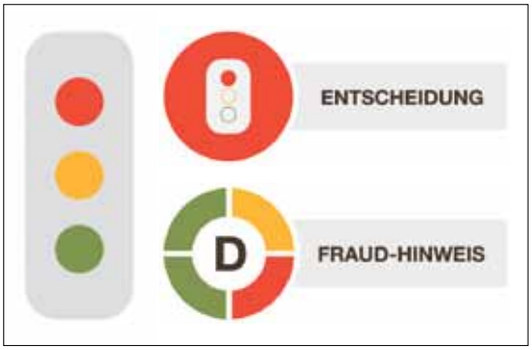
Schließlich wird durch die Kombination von Informationen aus dem Unternehmen und aus dem Datenuniversum von CRIF die Lieferadresse auf Existenz und kritische Merkmale überprüft. Bekannte Betrugsfälle an der besagten Zustelladresse werden ebenfalls berücksichtigt und weisen dementsprechend ein erhöhtes Risiko auf.

Modulares System

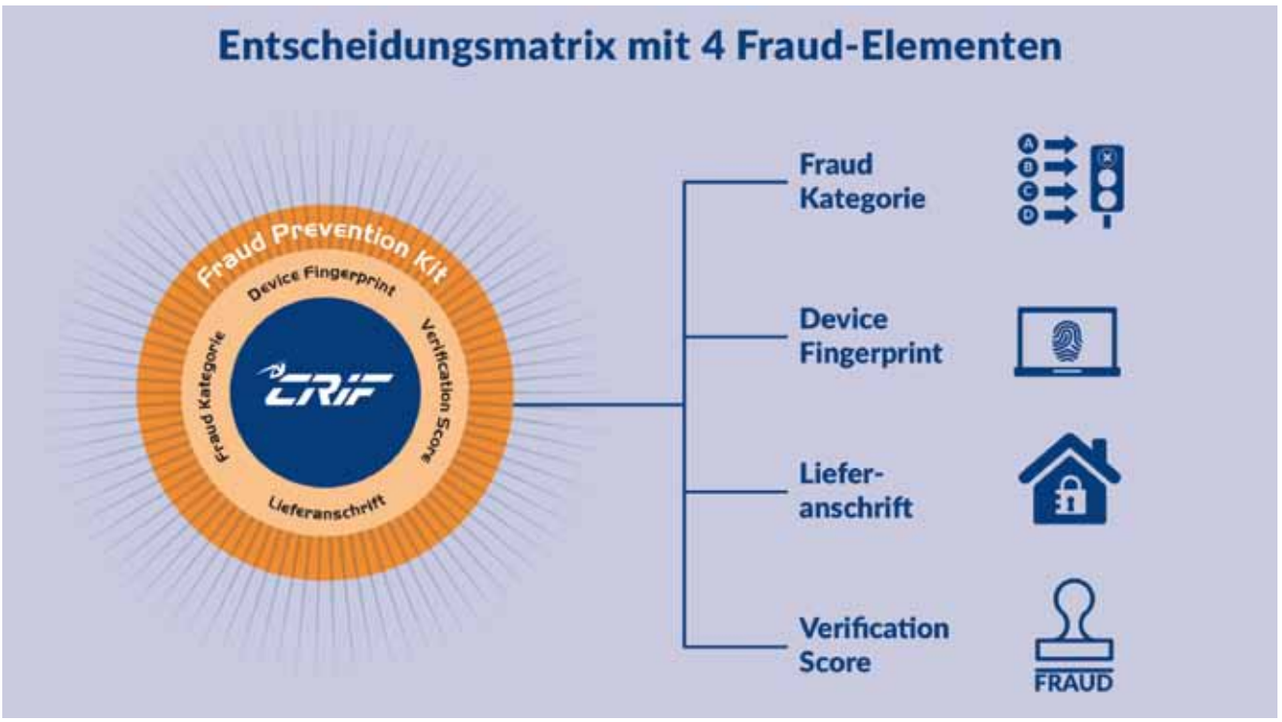
Die Key-Features des Fraud Prevention Kits sind frei miteinander kombinierbar. Jedes Unternehmen bestimmt für sich, welches Feature es einsetzen will. Es ist auch eine individuelle Konfiguration je nach Branche und Kunde möglich. Der Fraud-Hinweis passt sich diesen Einstellungen an und spiegelt dann in der Entscheidung nur die ausgewählten Elemente wider.

Unternehmen, die sich mit dem Fraud Prevention Kit aktiv schützen, können Betrugstypen wie der „Geist", der „VIP" oder der „Kreative" von Seite 3 rasch erkennen und rechtzeitig geeignete Maßnahmen setzen.

Der Fraud-Hinweis Rot: Hohes Betrugsrisiko, Gelb: Verdächtige Merkmale, Grün: kein Betrugsverdacht.



© CRIF



© CRIF

Entscheidungs-Matrix
In vier Richtungen überprüft das Fraud Prevention Kit Bestellungen oder Anträge auf Unregelmäßigkeiten.

Betrug in Echtzeit bekämpfen

T-Mobile vertraut bei der Betrugsbekämpfung auf die Lösung von CRIF.

WIEN. Wie viele Telekommunikations-Unternehmen ist auch T-Mobile durch den Anstieg der Online-Transaktionen vermehrt von Identitätsdiebstahl und vorsätzlichem Betrug betroffen.

Seriöse Bestellungen von Betrugsfällen zu unterscheiden, ist für Unternehmen in den vergangenen Jahren immer mehr zur Herausforderung geworden.

Betrug kommt teuer

Eine von CRIF durchgeführte Studie mit eCommerce-Kunden aus Deutschland, Österreich und der Schweiz hat ergeben, dass 56% der Befragten Unternehmen von Betrug durch Namens- oder Adressvariationen, 47% durch falsche Identitätsvorgaben betroffen waren. 16% dieser Unternehmen erlitten durch Betrugsfälle einen jährlichen Verlust von mehr als 50.000 €, bei 9% überstiegen die betrugsbedingten Einbußen sogar 100.000 €. Betrugsfälle zu verhindern, ist für Betriebe wirtschaftlich *notwendig* – manuelle Präventionsmaßnahmen wie Überprüfungen von Kundenanträgen durch Mitarbeiter sind jedoch sehr zeitintensiv.

In der rund 20-jährigen Zusammenarbeit von CRIF und T-Mobile wurde der Betrugsprävention seit 2011 immer mehr Beachtung geschenkt.

T-Mobile schützt sich

„Die größte Herausforderung für uns ist, die Balance zwischen maximalen Annahmeraten und einer Minimierung von uneinbringlichen Forderungen durch nichtzahlende Kunden und Betrüger zu finden", bringt Mohamed Ibrahim, Senior Manager Customer Finance bei T-Mobile, die Problematik auf den Punkt.

Aktuell nutzt T-Mobile das neueste, von CRIF entwickelte, automatisierte Instrument zur Betrugsbekämpfung: das Fraud Prevention Kit, das direkt als Erweiterung des Credit Check Consumer in den Prozess integriert werden kann. Damit werden Kundenanträge anhand ausgewählter Kriterien auf bekannte Betrugsmuster in Echtzeit überprüft.

Vier Module (Device Fingerprint, Verification Score, Fraud Kategorie, Lieferadresse), die individuell ausgewählt und miteinander kombiniert werden können, dienen zur Betrugsanalyse. Ob im jeweiligen Fall ein Betrugs-Risiko vorliegt oder nicht, wird nach der Analyse sofort mittels entsprechender farblicher Codierung angezeigt.

„Gleich nach dem Go-live der Lösung wurden zwei Prozent der T-Mobile-Webshop-Anträge im Juni 2017 vom Fraud Prevention Kit als verdächtig identifiziert, davon stellten sich wiederum 17,5 Prozent als Betrugsfälle heraus und konnten verhindert werden – was umgerechnet einer Ersparnis von 15.000 Euro pro Monat entspricht", fasst Ibrahim den wirtschaftlichen Effekt zusammen.

© medianet/Joe Haider

Mohamed Ibrahim, T-Mobile, setzt auf das Fraud Prevention Kit von CRIF.

CRIF fragte nach

Der Betrug im Online-Handel in der DACH-Region nimmt weiter zu. Die Details der aktuellen CRIF-Studie.

WIEN. Mit der kontinuierlich steigenden Zahl an Online-Shops, der zunehmenden Nachfrage und dem wachsenden Umsatzvolumen geht auch eine Zunahme an professionellen und organisierten Betrugsversuchen einher. Diese sind meist schwer zu durchschauen, und die Auswirkungen für die Händler reichen von finanziellen Einbußen über hohe juristische Kosten bis hin zu Reputationsschäden.

Um das Ausmaß zu erfassen, hat CRIF eine Umfrage unter rund 130 Online- und Versandhändlern in Deutschland, Österreich und der Schweiz (DACH-Region) zum Thema Betrug durchgeführt. Das traurige Ergebnis: Durchschnittlich 90% der Befragten gaben an, bereits einmal Opfer von Betrug bzw. eines Betrugsversuchs geworden zu sein; genauer waren es 97% in Deutschland, 93% in der Schweiz und 79% in Österreich.

© PantherMedia/Kiyoshi Takahase Segundo

Reale Bedrohung

Zwar gab es im Vergleich zum Vorjahr einen Rückgang um acht Prozentpunkte, das Ergebnis ist dennoch alarmierend und zeigt deutlich auf, dass Online-Betrug eine reale Bedrohung darstellt, die *jeden* treffen kann. Die Täter agieren zunehmend professionell, und der entstehende Schaden kann enorme Ausmaße annehmen. Potenzielle Betrüger anhand von verdächtigen Verhaltensmustern schon im Vorhinein identifizieren zu können, wird immer wichtiger werden.

Fingerabdruck
Jedes Gerät, ob Computer, Smartphone oder Tablet, verfügt über eine eindeutige Geräte-ID. Damit kann, ähnlich wie bei einem Fingerabdruck, das jeweilige Device eindeutig erkannt werden.

Dazu gilt es, mit der Zeit zu gehen und entsprechende Methoden anzuwenden. Dass technische Tools wie der Device Fingerprint noch verhältnismäßig selten zum Einsatz kommen, zeigt, dass es in dieser Hinsicht noch Aufholbedarf gibt.

Betrugsfälle steigen an

Wirft man einen Blick auf die Entwicklung im letzten Jahr, so zeigt sich, dass etwa die Hälfte der Befragten aus Deutschland (52%) und Österreich (50%) während der letzten zwölf Monate einen Anstieg der Betrugsfälle erkennt. In der Schweiz teilt nur ein Viertel diese Einschätzung – während hier knapp die Hälfte (49%) kaum eine Veränderung sieht, sagen 19% der deutschen und 13% der österreichischen Online-Händler, dass die Betrugsfälle sogar stark zugenommen haben.

Verschiedene Betrugsformen

In der Schweiz (88%) und Deutschland (67%) stellt die Zahlungsunfähigkeit von Kunden das größte Problem dar; dabei ist es den Bestellern bereits beim Kauf einer Ware bewusst, dass sie die Rechnung nicht begleichen können (Zahlungsunfähigkeit) – in Österreich liegt hier der Anteil bei 43%.

Mit der Angabe verfälschter Namens- oder Adressdaten (Identität variiert) mussten sich bereits 63% der Befragten in der Schweiz, 62% der deutschen und 43% der österreichischen Unternehmen auseinandersetzen. Die befragten österreichischen Online- und Versandhändler sind am häufigsten von Identitätsdiebstahl betroffen. So war die Hälfte von ihnen bereits damit konfrontiert, dass sich ein Kunde als komplett andere reale Person ausgegeben hatte (Deutschland 51%, Schweiz 40%).

Enorme Schadenshöhe

Für den Großteil der befragten Unternehmen aus der DACH-Region lag – wie bereits im Vor-

Entwicklung 2017 –> 2018

Der Betrug ist …	D	A	CH
… viel weniger geworden	3%	0%	4%
… weniger geworden	19%	13%	10%
… nahezu unverändert	6%	25%	49%
… angestiegen	52%	50%	25%
… stark angestiegen	19%	13%	10%

Quelle: CRIF

Womit waren Sie konfrontiert?

Betrugsform	D	A	CH
Zahlungsunfähigkeit	67%	43%	88%
Identität gestohlen	51%	50%	40%
Identität variiert	62%	43%	63%
Kunde betreitet Zustellung	28%	29%	28%
Identität erfunden	49%	36%	22%
Zahlungsdaten gestohlen	23%	21%	10%
Kunde bestreitet Bestellung	18%	21%	15%
Zahlungsdaten fiktiv	13%	0%	10%

Quelle: CRIF


© PantherMedia/Wavebreakmedia ltd.

jahr – der höchste, je erlittene Einzelverlustbetrag durch Betrugsfälle unter 5.000 EUR bzw. CHF (Schweiz 81%, Deutschland 70%, Österreich 50%).

Allerdings haben sowohl in Österreich (2018: 25%, 2017: 8%) als auch in Deutschland (2018: 20%, 2017: 12%) und der Schweiz (2018: 14%, 2017: 10%) heuer deutlich mehr Unternehmen angegeben, auch Verluste zwischen 5.000 und 10.000 EUR bzw. CHF erlitten zu haben.

Während im Jahr 2017 keiner der österreichischen Befragten den höchsten Verlust mit einem Betrag zwischen 10.000 und 25.000 EUR angab, waren es heuer 13%.

Gefragt nach der gesamten Schadenssumme, die in den letzten zwölf Monaten entstanden ist, lag diese für 74% der Schweizer, 50% der Österreicher und 34% der Deutschen unter 5.000 EUR bzw. CHF. Allerdings erlitten in Deutschland insgesamt 52% der Online-Händler einen Verlust von mehr als 10.000 EUR, in Österreich waren es 39% und in der Schweiz 10% .

Wie hoch war Ihr größter Verlust?

Einzelverlustbetrag	D	A	CH
< 5.000 EUR/CHF	70%	50%	81%
5.000–10.000 EUR/CHF	20%	25%	14%
10.000–25.000 EUR/CHF	3%	13%	2%
> 25.000 EUR/CHF	7%	13%	3%

Quelle: CRIF

Schwierigkeiten

Im Zuge der Umfrage wurden die Online- und Versandhändler auch nach den drei größten Schwierigkeiten in Bezug auf Betrug im Online-Handel gefragt. Dabei stellten sich insgesamt die Bestimmung von Methoden zur Betrugsvorbeugung, das Erkennen von Risiken und das Finden des richtigen Kosten-Nutzen-Verhältnisses als die größten Herausforderung für die Befragten heraus.

Das größte Problem für die Schweiz ist es heuer – mit 62% –, das richtige Kosten-Nutzen-Verhältnis zu finden. Im letzten Jahr lag der Wert nur bei 51%. Die Bestimmung von Methoden zur Vorbeugung gegen Betrug erweist sich sowohl für deutsche (46%) als auch für österreichische (50%) Online-Händler als größte Schwierigkeit.

Gesetzte Maßnahmen

In vielen Fällen können Betrugsfälle verhindert werden, vorausgesetzt, dass Auffälligkeiten *rechtzeitig* erkannt werden. Der Großteil der befragten Onlineshop-Betreiber führt deshalb Maßnahmen zur Erkennung von Online-Betrug durch – 97% in Deutschland und 96% in der Schweiz, in Österreich sind es nur 78%.

In allen drei Ländern ist es nach wie vor gängige Praxis, dass Mitarbeiter verdächtige Bestellungen manuell überprüfen (Schweiz: 79%, Deutschland: 64%, Österreich 50%). Zudem wird häufig mit eigenen Kundenlisten gearbeitet; Device Fingerprint und Transaktionstools kommen hingegen nur in vergleichsweise geringem Maße zum Einsatz.

Insgesamt geben rund 43% der befragten Online- und Versandhändler an, weitere Maßnahmen zur Betrugserkennung zu planen. In Österreich sind es 56%, gefolgt von Deutschland mit 53% und der Schweiz mit nur 19%. Einen Rückgang gegenüber dem Vorjahr gab es dabei in Österreich, nämlich um 27 Prozentpunkte und in der Schweiz um 29 Prozentpunkte. Mehr als die Hälfte der Händler in Österreich (56%) und der Schweiz (54%) führen die Maßnahmen zur Betrugsbekämpfung firmenintern durch, in Deutschland sind es 30%.

Fazit für die Online-Händler

Durch eine Verknüpfung und Auswertung unterschiedlicher Kundendaten ist es möglich, gewisse Muster zu erkennen, die von der Norm abweichen und somit schon im Vorhinein auf etwaige Auffälligkeiten im Verhalten des Kunden hinweisen. Mit dem Credit Check Consumer und dem Fraud Prevention Kit verfügt CRIF über die passenden Werkzeuge, um unterschiedliche Typen von Betrügern in Echtzeit zu identifizieren. Das erlaubt es den Betreibern von Online-Shops, reagieren zu können, noch bevor ein Schaden entsteht.

130

Die Teilnehmer
Die Studie zum Betrug im Online-Handel wurde von CRIF im Oktober 2017 bzw. im Februar und März 2018 im gesamten DACH-Raum durchgeführt. Befragt wurden rund 130 Online- und Versandhändler aus dem Kundenuniversum von CRIF – in Deutschland rund 40, in Österreich rund 20 und in der Schweiz rund 70.

Welche Maßnahmen setzen Sie?

Methode	D	A	CH
Manuelle Prüfung	64%	50%	79%
Kundenliste	33%	50%	56%
Device Fingerprint	10%	14%	3%
Transaktionstool	10%	0%	10%

Quelle: CRIF

Gemeinsam sind wir stärker!

Die Poollösung DSPortal läuft unter dem Motto „Einer für alle, alle für einen!“ Und alle zusammen gegen Betrüger.

Schütze dich!
Betrugsprävention ist für nahezu jedes Unternehmen unverzichtbar. Bevor die Bonität geprüft werden kann, muss noch die Existenz des Antragstellers geklärt werden.


© panthermedia.net/Andreus

WIEN. Wo es Anträge gibt, gibt es auch Betrüger. Und die machen auch vor der Finanzbranche nicht Halt. Mit dem neu entwickelten DSPortal (Deutsches Schutz Portal) bietet CRIFBÜRGEL (quasi die deutsche Schwester von CRIF Österreich, Anm.) ein System, das der Abwehr von Antragsbetrug bei Banken, Leasing- und Finanzdienstleistern dient. Das DSPortal ist eine Poollösung; alle Teilnehmer profitieren von einem einfachen und datenschutzkonformen (!) Datenaustausch untereinander.

Lösung steht auf drei Säulen
Die erste Säule bildet die Hinweisdatenbank, die von den Teilnehmern mit jeder Merkmalmeldung mit weiteren relevanten Informationen gespeist wird. Zwei weitere Säulen des DSPortals rücken strafbare Handlungen und Verhaltensweisen in den Fokus, die oft erst im Zeitverlauf deutlich werden: Die Prüfung von Plausibilitäten und Verhaltensregeln. Diese Regeln können im System individuell konfiguriert werden, um eine aus der Sicht des Anwenders optimale Betrugsprüfung durchzuführen.

Ob Hinweis-, Plausibilitäts- oder Verhaltensprüfung: Das DSPortal lässt sich genau so nutzen, wie es am besten zur individuellen Betrugspräventionsstrategie des teilnehmenden Unternehmens passt.

Regelwerk und Erfolgsfaktor
Dabei hat CRIFBÜRGEL gemeinsam mit den 18 Startteilnehmern folgende Regeln entwickelt:

- Strenge Gegenseitigkeit. Informationen werden nur in dem Umfang ausgetauscht, die der Teilnehmer auch selbst liefert.
- Fairness. Es gibt keine automatisierte Ablehnung.
- Klarheit. Definierte Meldemerkmale weisen immer eine hohe Praktikabilität auf. In etwa „Einkommensnachweis unplausibel, ge- oder verfälscht“, „Person nicht existent (Alias)“.

Die investigative Kraft einer Poollösung steht und fällt mit den Teilnehmern. Wobei eine hohe Anzahl allein noch keinen Erfolg bringt – entscheidend ist vielmehr, dass unter den Teilnehmenden möglichst viele Gemeinsamkeiten, vor allem in puncto Kundschaft, existieren.

Genau dies ist bei den Teilnehmern der Fall. Essenziell ist auch der Datenumfang, der zur Prüfung z.B. des Kreditantrags übermittelt wird. Je mehr Daten vorliegen, desto intensiver die Prüfung, umso besser der Schutz gegen Betrug.

Verluste merklich reduzieren
Ziel des DSPortals ist der bestmögliche Schutz vor externem Betrug und damit einhergehend die spürbare Reduzierung von Verlusten.

Eine besondere Rolle nimmt der *Opferschutz* ein: Mit einer Meldung an das DSPortal können sich Opfer vor Identitätsmissbrauch schützen – denn die Teilnehmer prüfen bei einem Opferhinweis mit besonderer Sensibilität.

Betrugsglossar

Betrug
Die Verschleierung von Zahlungsunwilligkeit und Zahlungsunfähigkeit.

Bonitätsbetrug
Eine existente Person verheimlicht die eigene, schlechte Kreditwürdigkeit (per Täuschung, Fälschung oder Verschleierung).

Identitätsbetrug
Eine Person tritt unter einer anderen Identität auf (per Alias, Identitätsfälschung oder -übernahme).

Wussten Sie schon?

Dass durch die einfache Verfügbarkeit von persönlichen Daten im Internet vor allem die **Identitätsübernahme** weiter zunimmt? Nach einer Studie in UK macht diese Form mittlerweile bereits mehr als 50% aller Betrugsstraftaten gegen Finanzdienstleister aus.

Dass gut **gefälschte Ausweise**, genauso wie Telefonnummern, Anschriften und Bankverbindungen, im Durchschnitt fünf Mal verwendet werden?

Ehrenwerte Unternehmer? Auch im B2B-Bereich lässt der Fraud Prevention Kit Betrügereien und Unstimmigkeiten auffliegen.

Betrug im B2B-Geschäft

Betrugsfälle sind auch im B2B-Bereich nicht mehr selten. Die Muster unterscheiden sich aber deutlich von B2C.

WIEN. Fraud findet nicht allein im Privatkunden Geschäft statt. Der Business-to-Business-Sektor ist ebenfalls davon betroffen, besonders die Finanzindustrie und der Online-Handel.

Die B2B-Betrugsarten

Die Varianten, mit denen Unternehmen betrügen, sind vielfältig und für den Laien schwer zu durchschauen. Da wäre zum Beispiel die Gründung eines Unternehmens, das vorrangig darauf ausgerichtet ist, Verpflichtungen aus Lohnabgaben, Zuschlägen oder sonstigen Beiträgen nicht nachzukommen sowie Personen allein zum Zweck der Beziehung von Sozial- oder sonstigen Tarifleistungen zu beschäftigen.

Der sogenannte Anschleichbetrug ist eine weitere Art des Betrugs. Hierbei tätigt der Unternehmer bei mehreren Anbietern kleine Käufe, die allesamt nicht bezahlt werden. Durch den jeweils kleinen Auftrag schöpfen die Lieferanten jedoch keinen Verdacht. Das gleiche Vorgehen kann auch bei Finanzierungsanträgen beobachtet werden.

In einer anderen Variante des Anschleichbetrugs tätigt der Unternehmer zunächst nur kleine Käufe. Diese werden fristgerecht und in voller Höhe bezahlt, allerdings nur, um so eine positive Credit History aufzubauen. Sobald das Unternehmen eine gute Bonität aufweist und auf Rechnung bestellen kann, werden in kürzester Zeit teure Anschaffungen getätigt, die in weiterer Folge nicht bezahlt werden.

Eine weitere Form des Betrugs ist der „Mantelbetrug". Der Mantelbetrug nutzt die positive Bonität eines mittlerweile stillgelegten Unternehmens, um in großem Stil Betrug zu betreiben. Anders als beim Anschleichbetrug wird hier nicht erst eine positive Credit History aufgebaut. Die gute Bonität „des Mantels" fungiert in dieser Konstellation regelrecht als USP (Unique Selling Proposition, Alleinstellungsmerkmal, Anm.) für den Käufer des stillgelegten Unternehmens.

Fraud Prevention Kit für B2B

So weit, so fies – jedoch lässt sich diesen Business-to-Business-Betrügereien auch mittels Fraud Prevention Kit von CRIF beikommen. Ähnlich wie bei der B2C Lösung, wird mithilfe des Device Fingerprints das Endgerät identifiziert und auffällige Verhaltensmuster erkannt. Die Überprüfung der Lieferadresse auf kritische Merkmale ist ebenfalls Teil der B2B Lösung.

Anhand der Fraud Kategorie werden Antragswiederholungen und Antragsvariationen geprüft.

Weiters wird der jeweilige Kundenantrag mit der offiziellen Liste für Scheinunternehmen des Bundesministeriums für Finanzen abgeglichen.

Vom Erkennen der Mäntel

Außerdem gibt es für den „Mantelbetrug" den dazu passenden, aufschlussreichen „Mantelhinweis"; hier wird auf Veränderungen im Unternehmen (Gesellschafterwechsel, Sitzwechsel, etc.) hingewiesen. Weiters wird die Beteiligung der Funktionsträger in Drittunternehmen und das Zahlungsverhalten dieser Firmen geprüft. Damit kann festgestellt werden, ob die gleichen Funktionsträger bereits in der Vergangenheit andere Unternehmen in die Insolvenz geführt haben oder nicht.

All dies natürlich in Echtzeit, damit das „angegriffene" Unternehmen zur rechten Zeit die richtigen Schritte setzen kann.

Bitte lächeln! Binnen weniger Minuten ist die Identifikation mittel Video-Call abgeschlossen – und auch die Echtheit des Kunden überprüft.

Video-Call zur Authentifizierung

Ausweiserfassung und Video-Identifikation lassen sich auch zur Betrugsbekämpfung bestens nutzen.

WIEN. Ab 1. Jänner 2019 sind anonyme Prepaid-Karten für Handys verboten. Telekommunikationsanbieter werden aufgrund der zu erwartenden praktischen Umsetzung neue Möglichkeiten zur Identifikation und Legitimation von Personen anbieten müssen.

Kundendaten richtig?
Wie bereits in Deutschland der Fall, werden sich Anbieter von Prepaid-Mobilfunkdiensten vor der endgültigen Freischaltung der SIM-Karte über die Richtigkeit der Kundendaten zu vergewissern haben.

Die Daten sollen entweder durch die Vorlage „eines amtlichen Lichtbildausweises" oder mithilfe eines „videounterstützten, elektronischen Verfahrens" eingesammelt werden, heißt es im Sicherheitspaket.

OCR-Technologie
Ein probates Mittel dazu ist die digitale Ausweiserfassung. Hiebei bietet CRIF eine App-Lösung, basierend auf der OCR-Technologie (Optical Character Recognition, deutsch: optische Zeichenerkennung). Diese ersetzt die manuelle und daher fehleranfällige Dateneingabe durch eine schnelle und intelligente Datenerfassung mit der Kamera eines mobilen Geräts.

Die Ausweiserfassung nutzt die OCR-Technologie, um Informationen von Reisepässen, Personalausweisen oder Führerscheinen auslesen zu können. Diese Informationen, wie Vorname, Nachname und Geburtsdatum, werden dann serverseitig verarbeitet und wie gewohnt mit den Daten von CRIF abgeglichen, überprüft und ausgewertet.

Video- oder Webchat
Etwas aufwendiger, aber auch gründlicher ist da schon die Videokonferenz zur Personenauthentifizierung, kurz Video-Identifikation. Was sich auf den ersten Blick kompliziert anhört, ist in Wirklichkeit ganz einfach und dauert auch nur ein paar Minuten: Nachdem der Kunde seine persönlichen Daten in eine Eingabemaske eingegeben hat, erfolgt ein Video-Call mit einem Servicemitarbeiter von WebID Solutions, einem der führenden Anbieter im Bereich der Online-Identifikation.

Im weiteren Verlauf der Identitätsprüfung hält der Kunde seinen Lichtbildausweis in die Kamera. Dabei wird das Ausweisdokument auf verschiedene Sicherheitsmerkmale überprüft. Nach weiteren Angaben, wie der Seriennummer kann die Echtheit des Dokuments verifiziert werden.

Betrug im Vorfeld verhindert
Anschließend erhält der Kunde eine Transaktionsnummer (TAN), die er auf der Vorgangsseite eingibt. Damit ist der Kunde als Nutzer bestätigt und der Vorgang abgeschlossen. Die Sicherheit der Daten wird durch die verwendeten Verschlüsselungsverfahren gewährleistet.

Beide Produkte, die Ausweiserfassung sowie die Video-Identifikation, ermöglichen einen medienbruchfreien Antragsprozess und eignen sich ebenfalls zur Prävention von Identitätsbetrug.

In Österreich kooperiert CRIF exklusiv mit WebID Solutions als Technologiepartner.

Bestes Alter: 30 Jahre CRIF

Boris Recsey zur Geschichte, Blockchain, EU-Verordnungen und digitalen Lösungen bei CRIF.

WIEN. 1988 – in Australien wird der erste Kunststoffgeldschein in Umlauf gebracht, in Deutschland der Leitindex DAX eingeführt und im italienischen Bologna CRIF gegründet. Seit der Gründung als Banking Credit Bureau hat sich CRIF zu einem der führenden Anbieter von Kreditrisikomanagement-, Fraud Prevention und Entscheidungsmanagement-Lösungen entwickelt.

2011 akquiriert CRIF Deltavista Schweiz und Deltavista Österreich – die Geburtsstunde von CRIF Österreich. Heute nutzen täglich mehr als 6.300 Banken und Finanzinstitute und 55.000 gewerbliche Kunden in 50 Ländern die Lösungen von CRIF. Boris Recsey, Geschäftsführer von CRIF Österreich, sprach mit **media**net über Geschichte und Zukunft der Wirtschaftsauskunftei CRIF.

© medianet/Joe Haider

IT-Visionär Boris Recsey, Geschäftsführer von CRIF Österreich, über 30 Jahre CRIF, Blockchain-Technologie und die PSD2-Richtlinie der EU.

medianet: *30 Jahre CRIF – was ist das Erfolgsgeheimnis?*
Boris Recsey: Die Kombination aus strategischen Allianzen und gewinnbringenden Akquisitionen. Sie hatte eine stetige Expansion auf vier Kontinenten zur Folge und hat somit maßgeblich zum Erfolg unseres Unternehmens beigetragen. ‚Immer in Bewegung bleiben' war und ist unser Motto – das gilt sowohl für unser geografisches und wirtschaftliches Wachstum als auch für unsere innovativen Lösungen, welche längst über das klassische Kreditrisikomanagement hinausgehen:

medianet: *Die Digitalisierung schreitet ja munter voran. Gibt es bei CRIF diesbezüglich besondere Lösungsansätze?*
Recsey: Die fortschreitende Digitalisierung verlangt auch nach neuen digitalen Lösungen, ganz klar. So ist die Authentifizierung von Personen ohne physischen Kontakt – beispielsweise mittels webbasierten Video-Calls – ein aktuell stark wachsender Trend in der DACH-Region. In Kooperation mit der deutschen WebID Solutions GmbH bieten wir eine Lösung an, die diesem Trend entspricht.

medianet: *Apropos Trends, was halten Sie von der Blockchain-Technologie?*
Recsey: Das Thema Blockchain birgt ein spannendes Potenzial. Eine von CRIF und dem Handelsverband in Auftrag gegebene Studie des AIT Austrian Institute of Technology hat untersucht, wie die Technologie hinter Bitcoin im Supply-Chain-Management eingesetzt werden kann. Der Hund in der Blockchain-Technologie liegt im Detail begraben, auf jeden Fall ist es ein spannendes Thema, das uns auch in Zukunft beschäftigen wird.

medianet: *Richtlinien und Verordnungen sind auch ein spannendes Thema …*
Recsey: Stimmt. Aktuell beschäftigen wir uns beispielsweise auch mit dem Thema PSD2, der zweiten Payment Services Directive. Als eine der entscheidenden Neuerungen bringt diese Richtlinie eine Öffnung der Möglichkeiten des Zugriffs auf Kontodaten. Bisher waren diese Informationen den kontoführenden Banken vorbehalten, nunmehr sind diese grundsätzlich verpflichtet, auch Drittanbietern Zugang zu den technischen Infrastrukturdiensten von Zahlungssystemen zu gewähren.

Hier kommen sogenannte Access to Account-Lösungen, abgekürzt XS2A, ins Spiel, mit denen Zahlungsdienstleister Kontobewegungen von Bankkunden monitoren und daraus Informationen über deren Konsumverhalten und Kreditwürdigkeit ableiten können.

Als eine der führenden Kreditauskunfteien Österreichs kann auch CRIF seinen Kunden eine XS2A-Lösung zur Verfügung stellen.

medianet: *Abgesehen von den technischen Lösungen, wohin wird sich CRIF entwickeln?*
Recsey: Wir streben danach, immer neue, optimierte Lösungen und Services für unsere Kunden zu entwickeln, wobei das Verständnis des individuellen Geschäftsmodells, welches jedes Unternehmen einzigartig macht, von zentraler Bedeutung ist.

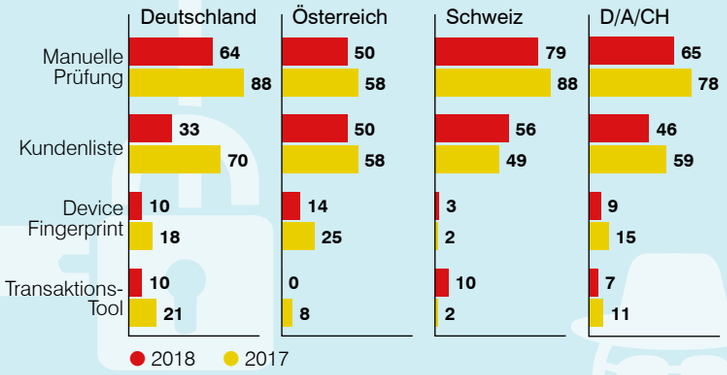
medianet: *Wollen Sie uns zum Abschluss noch ein paar Geschäftszahlen verraten?*
Recsey: Im Jahr 2017 erwirtschaftete CRIF einen Gesamtertrag von 511,2 Millionen Euro. Das Eigenkapital beläuft sich derzeit auf 178,3 Millionen Euro. Die Mitarbeiterzahl von CRIF ist in den Niederlassungen und Tochtergesellschaften rund um den Globus auf über 4.400 gestiegen.

Fraud im Online-Handel

Zahlen, Daten und Fakten der CRIF-Studie „Whitepaper: Zunahme von Betrug im Online- und Versandhandel" – grafisch aufbereitet.

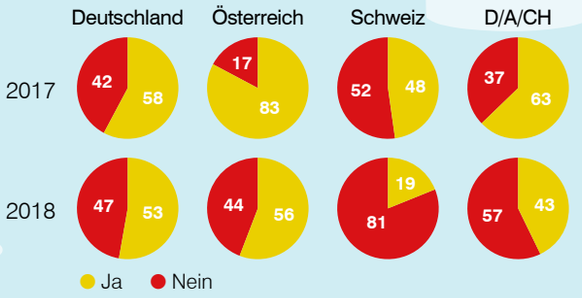
Betrugsprävention

Die meisten Unternehmen setzen auf die manuelle Prüfung – ein sehr zeitintensives und daher teures Unterfangen. Deutlich besser geeignet: Der Fraud Prevention Kit von CRIF. Er prüft in Echtzeit.



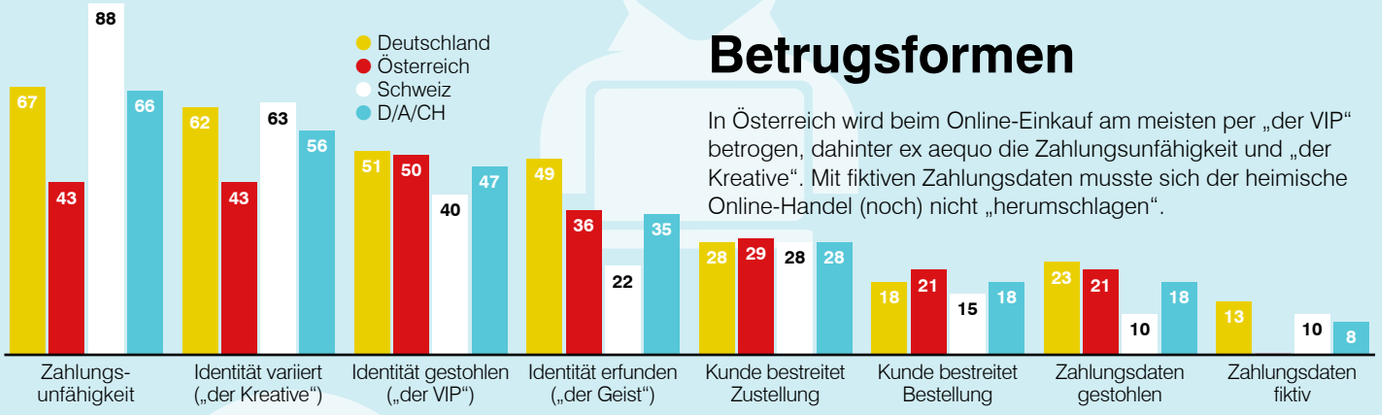
Planung weiterer Maßnahmen

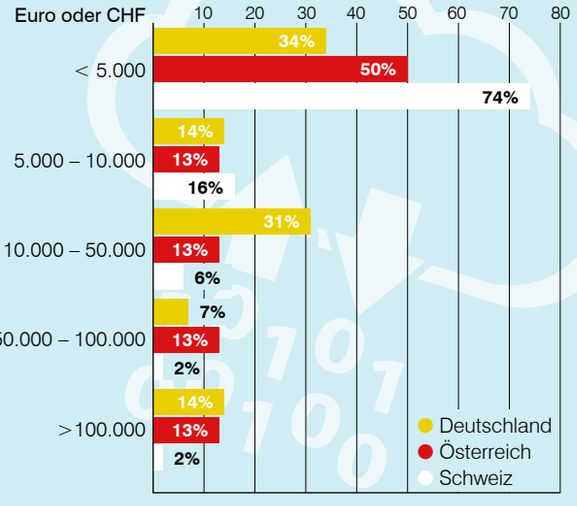
In Deutschland und Österreich planen jeweils mehr als die Hälfte der befragten Online- und Versandhändler weitere Maßnahmen zur Betrugserkennung. In der Schweiz ging dieser Anteil signifikant von rund 48% (2017) auf rund 19% (2018) zurück.



Betrugsformen

In Österreich wird beim Online-Einkauf am meisten per „der VIP" betrogen, dahinter ex aequo die Zahlungsunfähigkeit und „der Kreative". Mit fiktiven Zahlungsdaten musste sich der heimische Online-Handel (noch) nicht „herumschlagen".





Ausfall

Die letzten 12 Monate

Befragt nach der Höhe des Verlustbetrags der letzten zwölf Monate, gab der überwiegende Teil der Online- und Versandhändler einen Schaden von unter 5.000 Euro/CHF an. Erschreckend aus deutscher Sicht: Die Schadenshöhe 10.000 bis 50.000 Euro liegt mit 31% nur mehr drei Prozentpunkte unter der 5.000 Euro-Marke.

***Whitepaper:** Zunahme von Betrug im Online- und Versandhandel*

Über die Studie

- Durchgeführt von CRIF
- Wann? Oktober 2017 bzw. Februar und März 2018
- Wo? Gesamter D/A/CH-Raum
- Wer? 130 Online- und Versandhändler aus dem Kundenuniversum von CRIF.

Alle Angaben in %; * D/A/CH-Daten aggregiert/Mehrfachnennungen möglich