White paper

FRAUD IM E-COMMERCE

DACH UMFRAGE 2020/2021

CRIF BÜRGEL
Together to the next level

INHALT

Summary **3**

Gastkommentar Handelsverband **4**

1. Zunahme von Betrug im Online-Handel **6**

2. Online-Betrug als reale Gefahr – DACH **7**

2.1. Entwicklung 7

2.2. Betrugsformen 7

2.3. Schadenshöhe 8

2.4. Schwierigkeiten 9

2.5. Maßnahmen 10

3. Fokus Deutschland – Österreich **11**

3.1. Neue Netrugsformen 11

3.2. Betrug über verschiedenste Kanäle 12

3.3. Weitere Maßnahmen 13

3.4. Veränderungen durch Corona 13

4. Fokus Schweiz **14**

5. Lösungen zur Identifizierung von Betrugsversuchen **15**

5.1. Mehr Automatisierung 15

5.2. Digitale Identität 15

5.3. Alles aus einer Hand 15

Über die Studie **16**

CRIFBÜRGEL
Together to the next level

CRIFBÜRGEL ist in Deutschland einer der führenden Informationsdienstleister und bietet Lösungen für Identifikation, Bonitätsprüfung, Kreditrisiko- und Adressmanagement, Betrugsprävention und Digitalisierung für Finanzinstitute und Unternehmen.

Das Unternehmen gehört zur weltweit tätigen CRIF Gruppe mit Hauptsitz in Bologna, Italien. Das Netzwerk ist heute mit über 5.500 Experten und 70+ Unternehmen in 30+ Ländern auf vier Kontinenten für über 6.300 Finanzinstitute und 55.000 gewerbliche Kunden tätig.

www.crifbuergel.de

White paper

CRIF Bürgel GmbH, Leopoldstraße 244, 80807 München, Deutschland
Telefon +49 40 89803-0, Fax +49 40 89803-777/778, E-Mail info@crifbuergel.de

©CRIF Bürgel GmbH

SUMMARY

Der Onlinehandel hat in den letzten Jahren einen wahren Boom erfahren – im World Wide Web einzukaufen ist mittlerweile ganz normaler Alltag. Die Corona-Krise und die damit verbundene zeitweilige Schließung von Geschäften haben der Branche einen weiteren Boost verschafft.

Mit dem Siegeszug des E-Commerce stiegen allerdings auch betrügerische Aktivitäten merklich an. So wurden bereits neun von zehn Online- und Versandhändler in Deutschland, Österreich und in der Schweiz Opfer von Betrug bzw. Betrugsversuchen – ein Rekordwert im DACH-Raum.

41 Prozent der Befragten bemerkten im Vorjahr einen Anstieg betrügerischer Aktivitäten, lediglich 10 Prozent erlebten einen Rückgang der Betrugsfälle. Zu den häufigsten Betrugsformen zählen mit 76 Prozent die Angabe falscher Namens- und/oder Adressdaten, die Angabe einer anderen Identität (75 Prozent) sowie der Fall, dass Kunden eine Bestellung tätigen, obwohl sie wissen die Rechnung nicht bezahlen zu können (71 Prozent). Die höchsten Einzelverluste, die Unternehmen im DACH-Raum durch Online-Betrug erlitten, lagen in 66 Prozent der Fälle unter 5.000 EUR/CHF.

Als größte Schwierigkeiten beim Thema Online-Betrug sehen die Befragten die Bestimmung risiko- und kundengerechter Methoden zur Betrugsvorbeugung (52 Prozent), das Finden des richtigen Kosten-Nutzenverhältnisses (48 Prozent) und das Vermeiden von manuellen Prüfungsaufwänden (47 Prozent). Trotzdem setzen 70 Prozent der DACH-Händler auf die Kombination aus Betrugsvermeidungs-Tool plus zusätzlicher manueller Prüfung verdächtiger Bestellungen. Insgesamt 80 Prozent der Befragten gaben an, Maßnahmen zur Betrugserkennung zu ergreifen. Während 46 Prozent planen, bestehende Maßnahmen noch zu erweitern, wollen 54 Prozent ihrem Status Quo treu bleiben. Um Onlinebetrug zu vermeiden, reicht die manuelle Überprüfung verdächtiger Bestellungen nicht aus. Hier empfiehlt sich der Einsatz digitaler und automatisierter Abläufe. Datenbasierte Technologien erfassen Risiken in Echtzeit, länderübergreifend, vernetzt und automatisiert. So werden verdächtige Muster im Vorhinein erkannt und der Händler kann zeitnah reagieren, noch bevor überhaupt ein Schaden entsteht. Da viele Online-Betrugsmethoden mit verschleierten Identitäten einhergehen, stellt die eindeutige Identifizierung ebenfalls einen wichtigen Aspekt in der Betrugsvermeidung dar.

Der Einsatz effektiver Maßnahmen geht einher mit dem Gesetz der Usability. Es gilt dem Kunden ein angenehmes, unkompliziertes Shopping-Erlebnis zu bieten und Kaufabbrüche zu vermeiden. Hier punkten Online-Shops, die die eingesetzten Lösungen in bestehende Strukturen und Prozesse integrieren und somit die Customer Journey nicht beeinträchtigen.

White paper

GASTKOMMENTAR

Die Digitalisierung hat unser Einkaufsverhalten nachhaltig verändert. Neue Technologien ermöglichen uns Konsum in jeder Lebenslage. Wir kaufen ein, wann, wo und wie wir wollen – sei es unterwegs am Smartphone, im Wohnzimmer per Sprachbefehl an Alexa oder klassisch im Supermarkt ums Eck.

Gemeinsam Sicher im Online-Handel

HANDELS VERBAND

Ing. Mag. Rainer Will
Geschäftsführer Handelsverband Österreich
Board of Directors EMOTA - European eCommerce Association

Die Auswirkungen auf den Handel sind beispiellos und die Customer Journey ist so komplex geworden wie nie zuvor. Gleichzeitig wird unsere Aufmerksamkeitsspanne immer kürzer. Sie liegt mittlerweile unter jener eines Goldfisches von neun Sekunden.

Den Kern dieses Wandels bildet das Internet, mit allen positiven wie negativen Begleiterscheinungen für den Handel. E-Commerce boomt und die Corona-Krise wirkt wie ein Brandbeschleuniger. Allein im Vorjahr ist der Online-Handel in Österreich um mehr als 17 Prozent gewachsen, heuer dürfte das Wachstum sogar die 20-Prozent-Marke überspringen. Mit steigendem Umsatz wächst aber auch das Risiko für Betrug.

Die brandaktuellen Zahlen dieses Whitepapers von CRIF über Fraud im E-Commerce sprechen für sich selbst. Neun von zehn Onlinehändler:innen in der DACH-Region waren bereits Opfer von Betrugsversuchen, fast die Hälfte der Betriebe haben während der Pandemie einen Anstieg krimineller Aktivitäten erlebt. Damit steht Cyberkriminalität im Handel ganz weit oben auf der Liste potenzieller Bedrohungen. Die Schäden gehen teilweise in die Millionen, wie bereits die Österreichische Sicherheitsstudie 2020 von Handelsverband, Bundeskriminalamt und CRIF gezeigt hat. Immerhin setzen 80 Prozent der heimischen Webshops konkrete Maßnahmen zur Fraud Prevention ein.

Ganz ähnlich ist die Situation auf Konsumentenseite: Jede:r Zweite schätzt die Gefahren von Cyberkriminalität auf dem eigenen Computer als hoch ein, besonders bei sensiblen Kontodaten ist die Angst vor einem Angriff weit verbreitet. Generell stellt die Abwehr von Datendiebstahl, Identitätsmissbrauch und Bestellbetrug viele Webshops und Marktplätze vor immer größere Herausforderungen. Vor allem KMU-Händler:innen zählen zu den beliebtesten Zielen von Betrüger:innen, da viele davon ausgehen, kleine Webshops seien nicht ausreichend geschützt.

Die Europäische Union hat auf die Gefahr von Online-Betrug reagiert und mit ihrer Zahlungsdienste-Richtlinie (PSD2) eine 2-Faktor-Authentifizierung (2FA) implementiert. Seit Jänner 2021 müssen sich Kund:innen bei Bezahlung über das Internet zumindest doppelt identifizieren – etwa mittels Passwort und SMS TAN. Das soll für mehr Sicherheit im Zahlungsverkehr sorgen. Hierzulande haben das Bundeskriminalamt und der Handelsverband mit der Initiative **„GEMEINSAM SICHER IM ONLINE-HANDEL“** eine neue Plattform geschaffen, die es den heimischen Händlern ermöglicht, Sicherheitsaspekte bei der Etablierung ihrer digitalen Filiale bis hin zum laufenden Betrieb stets mitzudenken.

Die Digitalisierung hat unser Einkaufsverhalten nachhaltig verändert. Neue Technologien ermöglichen uns Konsum in jeder Lebenslage. Wir kaufen ein, wann, wo und wie wir wollen – sei es unterwegs am Smartphone, im Wohnzimmer per Sprachbefehl an Alexa oder klassisch im Supermarkt ums Eck.

Fazit:

Die Händler:innen haben längst gelernt, ihre stationären Geschäfte sicher zu machen. Es ist aber auch dringend nötig, die digitale Filiale entsprechend abzusichern.

Zumindest ein Viertel der Onlinehändler hat im Bereich der Sicherheit noch Aufholbedarf, denn viele Kriminelle agieren im Netz hochprofessionell. Der Handel muss darauf entsprechend reagieren – mit ebenso professionellen Schutzmechanismen. Kompetente Dienstleister wie CRIF, ein langjähriger Partner des österreichischen Handelsverbandes, bieten hierfür modernste Lösungen, um potenzielle Betrüger:innen automatisiert und in Echtzeit identifizieren zu können. Der Bedarf an derartigen Tools wird in den kommenden Jahren deutlich steigen. Wir müssen uns der Tragweite dieser Bedrohung bewusst werden und proaktiv darauf reagieren. Der Handelsverband unterstützt Sie mit dem eCommerce-Gütesiegel **TRUSTMARK AUSTRIA** sowie im Rahmen der Initiative **GEMEINSAM SICHER IM ONLINE-HANDEL** mit kompetenten Partnern dabei, sich digital optimal aufzustellen. Worauf es besonders ankommt, erfahren Sie im vorliegenden Whitepaper von CRIF.

1. ZUNAHME VON BETRUG IM ONLINE-HANDEL

Mittlerweile ist das Internet in allen Bereichen des Lebens zugegen – immer mehr Arbeits- und Alltagsabläufe erfolgen mit einem Klick. Je mehr sich das Leben in die digitale Welt verlagert, desto besser der Nährboden für Betrüger.

Fast täglich finden sich in den Medien Meldungen über den Diebstahl von Daten und deren missbräuchliche Verwendung. Während die polizeilichen Kriminalstatistiken in Deutschland und Österreich für 2020 einen Rückgang der Gesamtanzeigen verzeichnet, stieg die Cyber-Kriminalität im Vergleich zu 2019 an – nicht zuletzt bedingt durch die Schließungen des stationären Handels. In Österreich wurden um 26 Prozent mehr Delikte im Zusammenhang mit Internetkriminalität verzeichnet, in Deutschland um 8 Prozent.

Neben Privatpersonen werden auch zunehmend Unternehmen Opfer von Online-Betrug. Da die Täter in ihrer Vorgangsweise immer professioneller und kreativer werden, wird es immer schwieriger, sich vor betrügerischen Aktivitäten zu schützen. Die Methoden der Betrüger reichen vom Identitätsmissbrauch über die Angabe falscher Namens- und Adressdaten bis hin zur Angabe fiktiver Zahlungsdaten. Dem Online-Handel entstehen dadurch nicht nur finanzielle Verluste in Millionenhöhe, sondern auch hohe juristische Kosten sowie nachhaltige Reputationsschäden. Um das Ausmaß und den Umgang der Unternehmen mit dem Problem zu erfassen, hat CRIF eine Umfrage unter rund 100 Online- und Versandhändlern in Deutschland, Österreich und der Schweiz (DACH-Region) durchgeführt.

Das Ergebnis: Durchschnittlich 90 Prozent der befragten Firmen wurden bereits einmal Opfer von Betrug bzw. Betrugsversuchen. Was einmal mehr verdeutlicht, wie allgegenwärtig die Gefahr von Online-Betrug ist. Kriminelle agieren professionell und organisiert – und genauso professionell gilt es bei der Abwehr von Betrugsversuchen vorzugehen. Viele der gängigen Methoden – zum Beispiel die manuelle Kontrolle verdächtiger Bestellungen –, werden dem allerdings nicht gerecht. Um verdächtige Verhaltensmuster bereits im Vorhinein zu erkennen, gilt es auf zeitgemäße Methode zu setzen. Die Ergebnisse der Umfrage zeigen deutlich, dass es bei der Betrugsprävention in den Unternehmen noch viel Aufholbedarf gibt.

2. ONLINE-BETRUG ALS REALE GEFAHR - DACH

Laut der im DACH-Raum durchgeführten CRIF-Umfrage waren bereits mehr als 90 Prozent der befragten Händler einmal mit Betrug oder Betrugsversuchen konfrontiert. In Österreich waren es 88 Prozent, in Deutschland 89 Prozent und in der Schweiz sogar 95 Prozent.

2.1. Entwicklung

Hinsichtlich der Entwicklung im letzten Jahr verzeichneten 41 Prozent der Befragten einen Anstieg betrügerischer Aktivitäten, 7 Prozent stellten sogar einen starken Anstieg fest. 49 Prozent gaben an, kaum eine Veränderung bemerkt zu haben. Nur wenige der befragten Händler (8 Prozent) erlebten einen Rückgang bzw. einen starken Rückgang (2 Prozent) der Betrugsfälle.

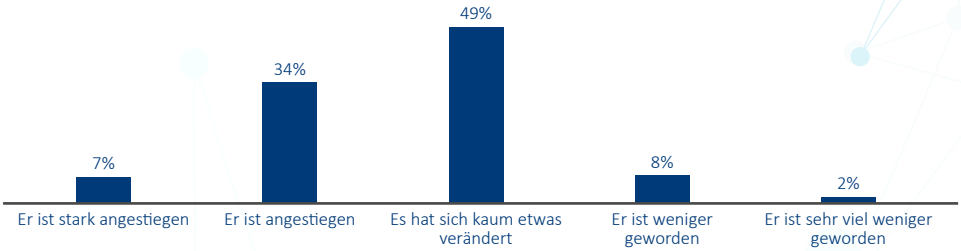


Abb.1: Wie sehen Sie die Entwicklung des Betrugs im vergangenen Jahr? (DACH Ergebnisse)

2.2. Betrugsformen

Betrachtet man die Vorgangsweise der Online-Betrüger, zeigt sich: Die Methodik reicht hier von simpel bis hochprofessionell. Zu den häufigsten Betrugsformen im DACH-Raum zählen laut Umfrage die Angabe verfälschter Namens- und/oder Anschriftsdaten (76 Prozent), die Angabe einer anderen Identität (75 Prozent) sowie Bestellungen, die trotz der Kenntnis der Zahlungsunfähigkeit getätigt werden (71 Prozent). Dass Kunden den Erhalt der Ware abstreiten, obwohl sie bei ihnen eingelangt ist, haben bereits 52 Prozent der befragten Händler erlebt. Auch mit der Angabe einer fiktiven Identität waren bereits 50 Prozent konfrontiert. Lediglich 21 Prozent der Umfrageteilnehmer waren bereits von Betrug durch fiktive Zahlungsdaten betroffen.

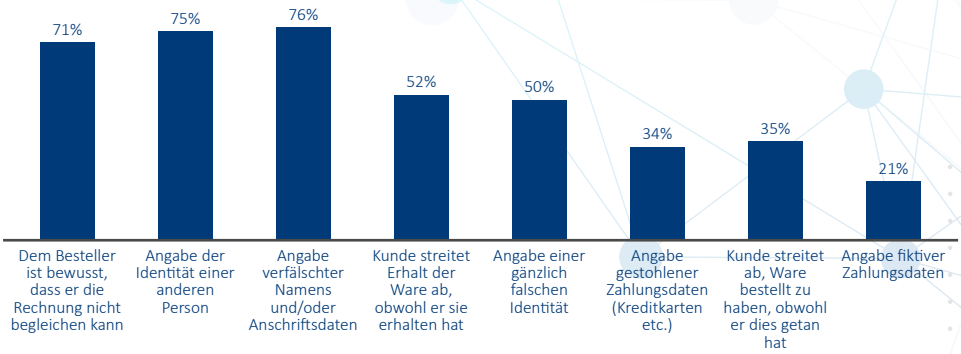


Abb. 2: Mit welchen Formen des Betruges waren Sie konfrontiert? (DACH Ergebnisse, Mehrfachnennungen möglich)

2.3. Schadenshöhe

Für 66 Prozent der befragten Händler aus der DACH-Region lag der höchste je erlittene Einzelverlustbetrag unter 5.000 EUR/CHF. Für 8 Prozent betrug der Verlust sogar über 25.000 EUR/CHF. Betrachtet man die gesamte Schadenssumme der vergangenen 12 Monate, mussten 63 Prozent der Umfrageteilnehmer Gesamtverluste von bis zu 10.000 EUR/CHF hinnehmen. Bei 11 Prozent belief sich der Gesamtausfall durch Onlinebetrug sogar auf mehr als 100.000 EUR/CHF.

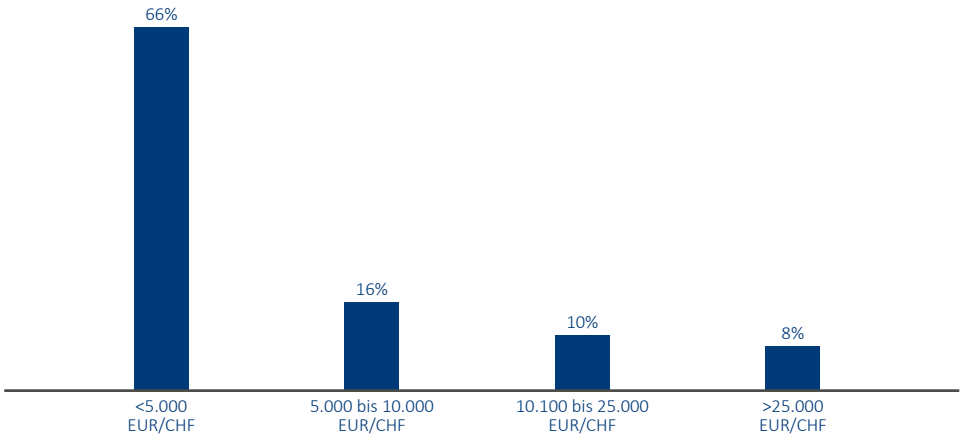


Abb.3.: Schadenshöhe: höchster Einzelverlustbetrag? (DACH Ergebnisse)

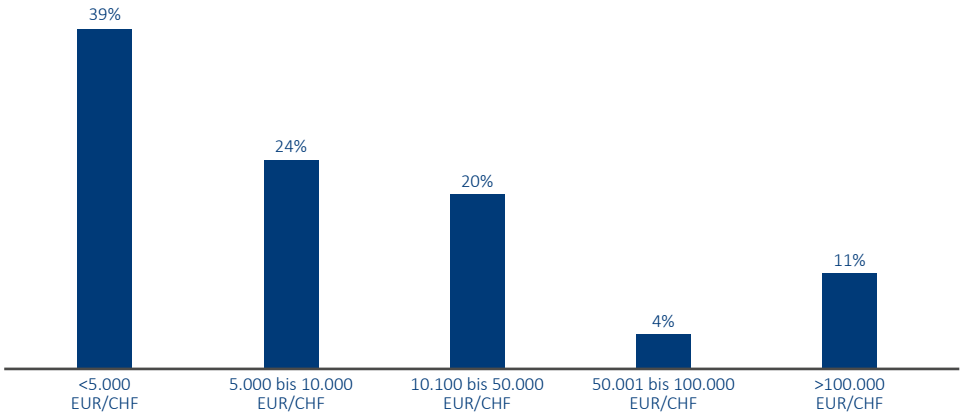
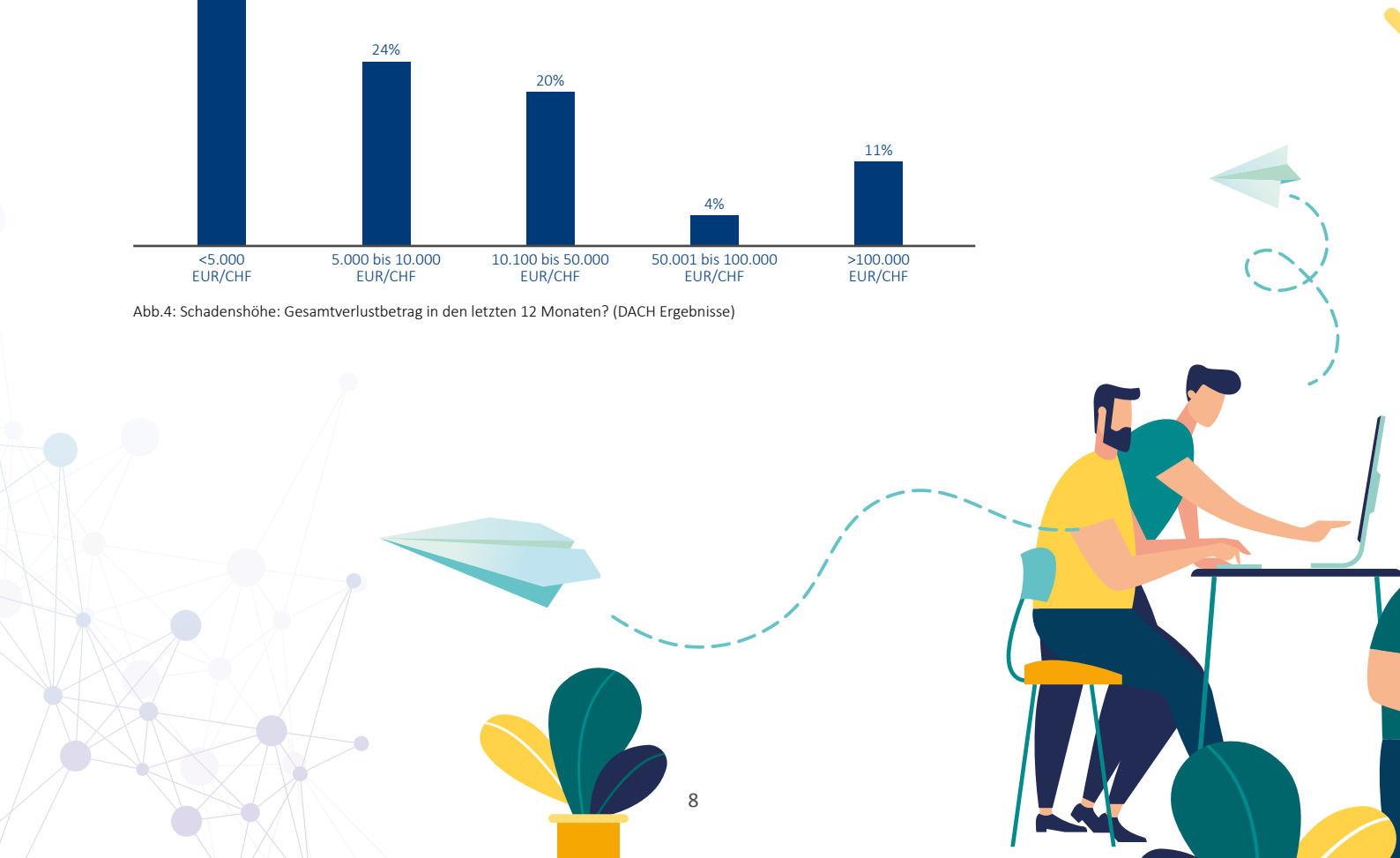


Abb.4: Schadenshöhe: Gesamtverlustbetrag in den letzten 12 Monaten? (DACH Ergebnisse)



2.4. Schwierigkeiten

Im Rahmen der Studie wurden die Händler auch nach den für sie drei größten Schwierigkeiten hinsichtlich Betrugs im Online-Handel gefragt. Hier zeigt sich deutlich: Am herausforderndsten ist, eine Betrugsvermeidung zu finden, die die Conversion nicht gefährdet – sprich, die trotz Risikominimierung ein userfreundliches Shoppingerlebnis aufrechterhält.

Diese Bestimmung risiko- und kundengerechter Methoden zur Betrugsvorbeugung stellt für 52 Prozent der Händler die größte Schwierigkeit dar. An zweiter Stelle folgt mit 48 Prozent das Finden des richtigen Kosten-Nutzenverhältnisses. Insgesamt 47 Prozent der Händler im DACH-Raum gaben an, mit dem Vermeiden von Prüfungsaufwänden ein Problem zu haben. 17 Prozent der Händler wissen nicht genau, wie sie mit bereits eingetretenen Betrugsfällen umgehen sollen, und 12 Prozent fehlt es an notwendigem Know-how.

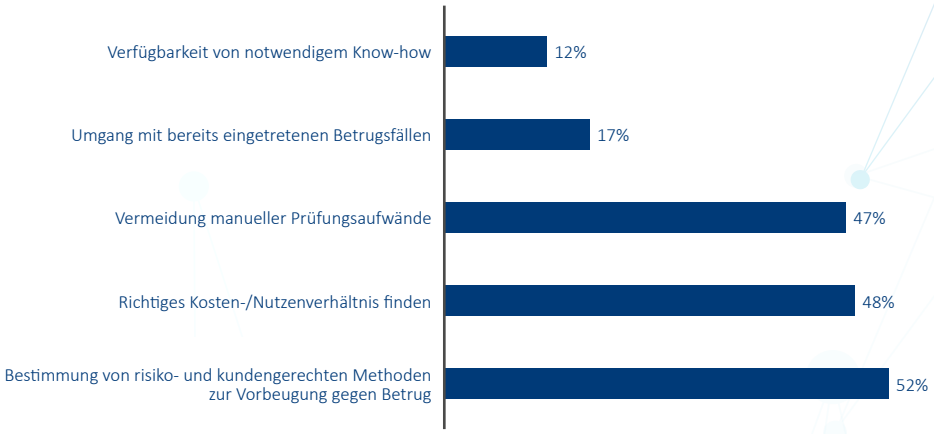


Abb.5: Was sind aus Ihrer Sicht die drei größten Schwierigkeiten beim Thema Betrug im Online-Handel? (DACH Ergebnisse)

2.5. Maßnahmen

Das A und O, um vor Onlinebetrug geschützt zu sein: der richtige Mix an vorbeugenden Maßnahmen. Früh genug erkannt, können betrügerische Aktivitäten und deren Folgen vermieden werden. Um gegen Internet-Kriminalität gerüstet zu sein, ergreifen 80 Prozent der befragten Händler Maßnahmen zur Betrugserkennung. 70 Prozent setzen auf die Kombination aus Betrugsvermeidungs-Tool und zusätzlicher manueller Prüfung verdächtiger Bestellungen. 79 Prozent prüfen mit mehr als einer Maßnahme, und wiederum 13 Prozent verlassen sich ausschließlich auf manuelle Prüfungen.

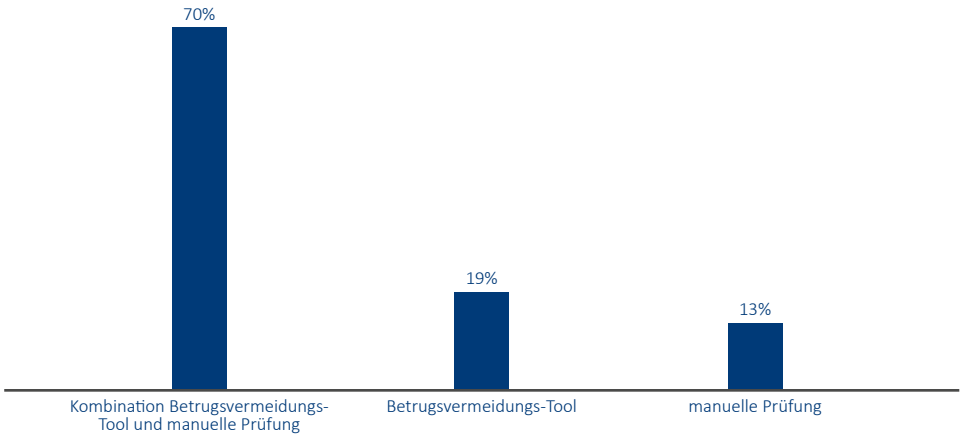


Abb.6: Welche Maßnahmen führen Sie durch? (DACH Ergebnisse)

Die richtige Methode zur Betrugsvermeidung zu finden, zählt zu den größten Herausforderungen für Online- und Versand-Händler (siehe Punkt 2.4.). Neben der Vielfalt an Methoden stellt sich auch noch die Frage: Lässt man alle Betrugserkennungsmaßnahmen im Haus oder lagert man sie teilweise bzw. sogar komplett aus? Mehr als die Hälfte der Befragten (51 Prozent) gaben an, bestimmte Maßnahmen zur Betrugserkennung selbst durchzuführen, jedoch gleichzeitig externe Dienstleister in Anspruch zu nehmen. 41 Prozent führen alle Maßnahmen selbst durch und 8 Prozent haben sämtliche Überprüfungen an einen Dienstleister übergeben.

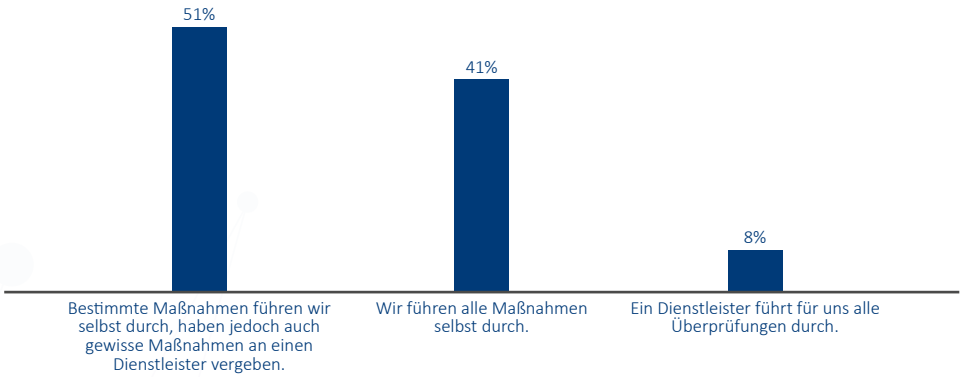


Abb.7: Führen Sie die Maßnahmen zur Betrugserkennung selbst durch oder haben Sie diese (teilweise) an einen Dienstleister vergeben? (DACH Ergebnisse)

Auf die Frage, ob sie Maßnahmen bzw. weitere Maßnahmen zur Betrugserkennung planen, antworteten 46 Prozent der Händler im DACH-Raum mit „ja“, 54 Prozent wollen ihrem Status Quo treu bleiben und planen keine Veränderung.

3. FOKUS DEUTSCHLAND – ÖSTERREICH

Betrachtet man die Ergebnisse aus Deutschland und Österreich näher, ergibt sich vor allem bei der Frage „Wie sehen Sie die Entwicklung des Betrugs bei Ihnen im letzten Jahr“ ein deutlicher Unterschied: Während 65 Prozent der deutschen Onlinehändler einen Anstieg bestätigten, waren es in Österreich nur rund 11 Prozent.

In den Erhebungen der letzten Jahre haben die österreichischen Händler stets eine Steigerung des Betrugsniveaus verzeichnet. Dies hat sich heuer zum ersten Mal verändert, sodass für 72 Prozent der österreichischen Onlinehändler das Betrugsniveau im Vergleich zum Vorjahr gleichgeblieben ist.

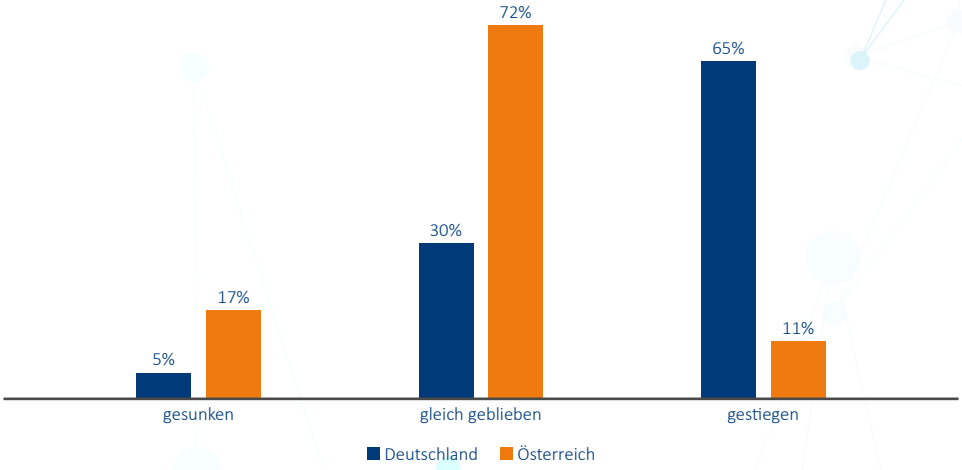


Abb.8: Wie sehen Sie die Entwicklung des Betrugs im vergangenen Jahr? (DE &AT Ergebnisse)

62 Prozent der deutschen E-Commerce-Händler, die einen Anstieg des Betrugsniveaus im letzten Jahr verzeichnet haben, führen die Steigerung auf die Corona-Pandemie zurück. In Österreich können die Händler diese Einschätzung allerdings nicht bestätigen.

3.1. Neue Betrugsformen

Je stärker der Online-Handel wächst, desto kreativer wird auch die Vorgangsweise von Betrügern. Es gibt kaum eine Methode, mit der man als Händler nicht früher oder später konfrontiert wird. Interessant sind hier allerdings die teils stark abweichenden Ergebnisse in Deutschland und Österreich. So waren 58 Prozent der österreichischen Händler 2020 erstmals mit Betrug durch Angabe einer falschen Identität betroffen, bei den deutschen Händlern war diese Betrugsform nur für 20 Prozent neu. Am deutlichsten sind die Unterschiede allerdings beim Betrug durch Angabe der Identität einer anderen Person: 42 Prozent der österreichischen Händler wurden 2020 erstmals Opfer dieser Betrugsmethode – im Gegensatz zu den deutschen Umfrageteilnehmern, die damit bereits Erfahrungen gemacht hatten. Auch die Angabe verfälschter Namens- bzw. Adressdaten

zählt mit 42 Prozent zu den häufigsten neu aufgetretenen Betrugsformen in Österreich. Immerhin 30 Prozent der deutschen Onlinehändler kamen mit dieser Betrugsform erstmals 2020 in Kontakt. Markante Unterschiede zeigen sich auch bei der Methodik des Account Takeover – sprich, der Besteller benutzt das Kundenkonto einer anderen Person. Österreichweit war diese Betrugsform 2020 nur für 8 Prozent der Onlinehändler neu, in Deutschland dagegen für 40 Prozent. Mit dem Account Takeover konfrontiert waren in Österreich insgesamt bereits 44 Prozent, in Deutschland 40 Prozent.

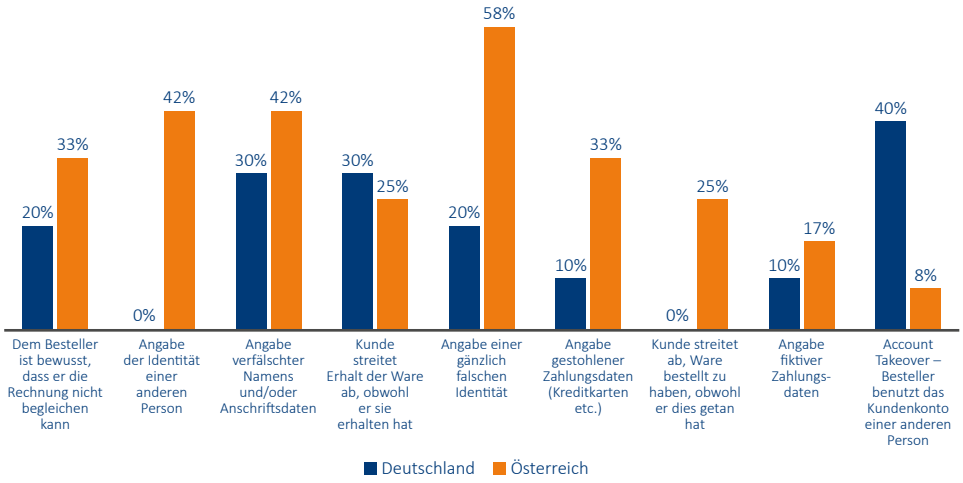


Abb.9: Welche Betrugsformen sind das erste Mal 2020 aufgetreten?

3.2. Betrug über verschiedenste Kanäle

Leider sind betrügerische Aktivitäten nicht nur in Online-Shops gang und gäbe, sondern betreffen auch andere Kanäle – vom Point Of Sale über Call Center bis hin zu Apps. Auch hier weichen die Ergebnisse in Deutschland und Österreich teils stark voneinander ab. Während Betrugsversuche über Mobile Apps in Deutschland mit 80 Prozent hoch im Kurs stehen, waren bislang nur 33 Prozent der österreichischen Händler damit konfrontiert. Mit Betrug im Point Of Sale haben in Österreich hingegen bereits 56 Prozent Erfahrungen gemacht, in Deutschland nur 20 Prozent. Betrugsversuche über Call Center bzw. über telefonische Bestellungen sind mit 79 Prozent (Österreich) und 60 Prozent (Deutschland) die zweithäufigste Methode in beiden Ländern.

3.3. Weitere Maßnahmen

57 Prozent der deutschen und 29 Prozent der österreichischen Onlinehändler wollen ihr Betrugsvermeidungs-Konzept noch weiter ausbauen, sprich weitere Maßnahmen ergreifen. Die Frage, in welchen Bereichen die Händler dabei Investitionen planen, zeigt interessante Unterschiede zwischen Österreich und Deutschland auf. Während der Bereich Technologie in beiden Ländern ähnlich hoch im Kurs steht (Deutschland 67 Prozent, Österreich 60 Prozent), wollen nur 20 Prozent der österreichischen Befragten in den Bereich Mitarbeiter investieren – in Deutschland immerhin 58 Prozent. Hingegen wollen 60 Prozent der österreichischen Händler in Zukunft vermehrt auf externe Betrugsprävention setzen, in Deutschland wiederum nur 42 Prozent. Die Hälfte der Befragten in Deutschland gab an, Investitionen im Rahmen der Prozessoptimierung zu planen – in Österreich sind es lediglich 20 Prozent.

3.4. Veränderungen durch Corona

Geschlossene Geschäfte im Rahmen der Corona-Lockdowns haben sowohl die Deutschen, aber noch mehr die Österreicher zum Online-Shopping verleitet. Während 65 Prozent der Onlinehändler durch die Corona-Krise ein Umsatzplus verzeichneten, waren es in Österreich sogar 95 Prozent. Nur 5 Prozent der österreichischen Händler gaben an, durch Corona Kunden verloren zu haben – in Deutschland immerhin 20 Prozent. Auch hinsichtlich neuer Kunden haben die österreichischen Shops die Nase vorn: 63 Prozent konnten während der Pandemie neue Kunden gewinnen, in Deutschland waren es 55 Prozent. 15 Prozent der deutschen sowie 11 Prozent der österreichischen Händler setzten in der Krise auf eine Ausweitung ihres Liefergebiets. Verstärkt von Betrugsversuchen während Corona betroffen waren in Deutschland 20 Prozent der Befragten, in Österreich 11 Prozent.

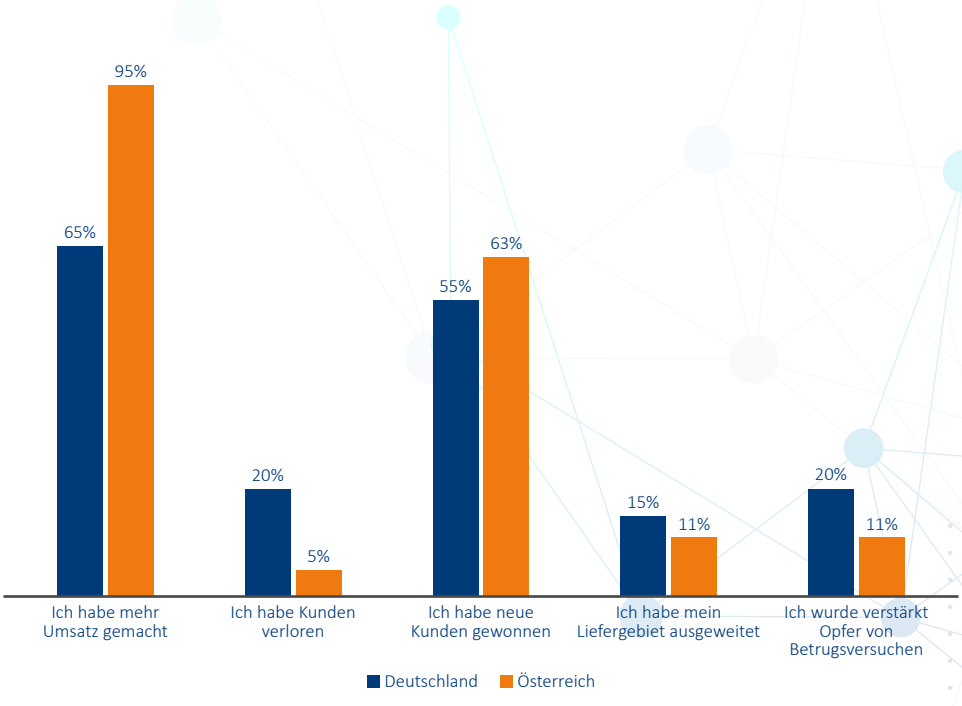


Abb.10: Was hat sich in Ihrem Online-Shop letztes Jahr durch die Corona Pandemie verändert?

4. FOKUS SCHWEIZ

Mit 95 Prozent waren in der Schweiz bislang die meisten Händler von Online-Betrug betroffen. 48 Prozent bemerkten 2020 einen Anstieg betrügerischer Aktivitäten, während 46 Prozent kaum eine Veränderung feststellten. Ein Drittel verzeichnete vermehrte Betrugsversuche während des Lockdowns.

Für 71 Prozent der Befragten belief sich der höchste durch Online-Betrug erlittene Verlust auf Beträge unter 5.000 CHF. In 17 Prozent der Fälle betrug die Verlustsumme zwischen 5.000 und 10.000 CHF. Betrachtet man den Gesamtverlust der letzten 12 Monate, verloren 41 Prozent der Schweizer Händler durch Online-Betrug bis zu 5.000 CHF und immerhin 7 Prozent mehr als 100.000 CHF. Als eine der häufigsten Online-Betrugsformen in der Schweiz ist die Angabe einer anderen Identität, mit dem bereits 71 Prozent der Händler konfrontiert waren. Ebenso häufig vor kommen Bestellungen mit dem Wissen, dass die Ware nicht bezahlt werden kann sowie Bestellungen unter verfälschten Angaben. Mit Betrug durch erfundene Identitäten waren bislang 39 Prozent der Schweizer Händler konfrontiert, und 36 Prozent haben bereits erlebt, dass Kunden eine erfolgte Zustellung bestreiten.

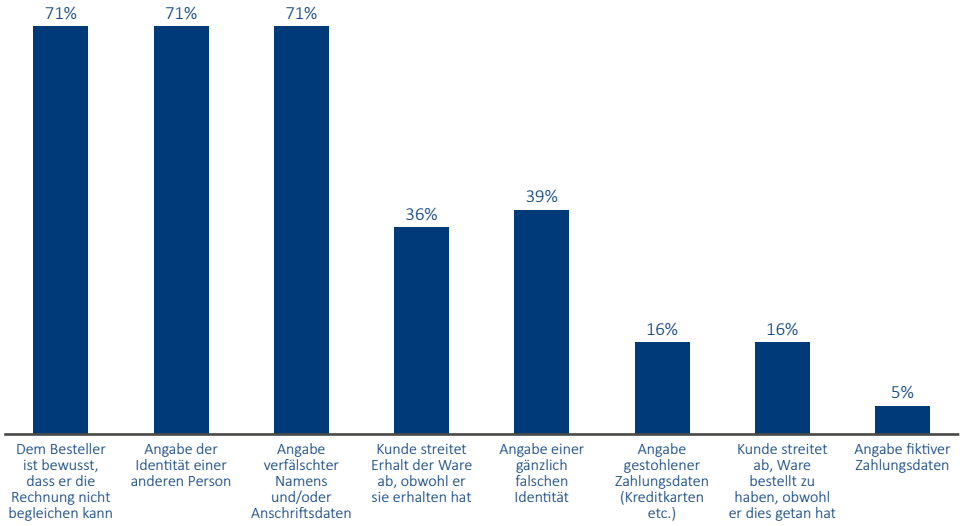


Abb.11: Mit welchen Formen des Betrugs waren Sie konfrontiert? (CH Ergebnisse, Mehrfachnennung möglich)

Als größte Herausforderungen beim Thema Online-Betrug sehen die Schweizer Händler, das richtige Kosten-Nutzen-Verhältnis sowie risiko- und kundengerechte Methoden zur Betrugsvorbeugung zu bestimmen (52 bzw. 48 Prozent) sowie manuelle Prüfungsaufwände zu vermeiden (36 Prozent).

Über 93 Prozent der Befragten setzen auf Maßnahmen zur Betrugserkennung. 71 Prozent nutzen eine Kombination aus manueller Prüfung und Betrugsvermeidungs-Tool. Hingegen verlassen sich 20 Prozent ausschließlich auf manuelles Prüfen und 16% verzichten auf eine manuelle Prüfung verdächtiger Bestellungen. Die Hälfte der Befragten führt einen Teil der Maßnahmen teils selbst durch und lagert bestimmte Aspekte an Dienstleister aus. 45 Prozent setzen alle Maßnahmen selbst um, wiederum 5 Prozent haben diesen Bereich komplett an einen Dienstleister ausgelagert. Auf die Frage, ob sie weitere Maßnahmen zur Betrugserkennung planen, antworteten 51 Prozent der Schweizer Händler mit „ja“, 49 Prozent wollen bei ihren bestehenden Maßnahmen bleiben.

5. LÖSUNGEN ZUR IDENTIFIZIERUNG VON BETRUGSVERSUCHEN

5.1. Mehr Automatisierung

Bei mehr als 2/3 der befragten Online- und Versandhändler im DACH-Raum werden verdächtige Bestellungen von Mitarbeitern unter anderem manuell überprüft, 13 Prozent sogar ausschließlich. Gleichzeitig stellt es für die Befragten eine große Herausforderung dar, diesen manuellen Prüfaufwand zu vermeiden, da er hohen zeitlichen und personellen Einsatz mit sich bringt. Um Kunden zu identifizieren und Betrugsversuche zu vermeiden, empfehlen sich datenbasierte Technologien, die Risiken in Echtzeit, länderübergreifend, vernetzt und automatisiert erkennen. Die Verknüpfung und Auswertung unterschiedlicher Kundendaten zeigen gewisse Muster auf, die von der Norm abweichen und somit schon im Vorhinein auf etwaige Auffälligkeiten im Kundenverhalten hinweisen. So haben Onlinehändler die Möglichkeit, zeitnah zu reagieren, noch bevor überhaupt ein Schaden entstehen kann.

Zusätzlich besteht der Anspruch, dem Kunden ein angenehmes, ungestörtes Shopping-Erlebnis zu bieten. Kaufabbrüche, die sich negativ auf die Conversion auswirken, gilt es so weit wie möglich zu vermeiden. Um die Customer Journey nicht zu beeinträchtigen, muss die eingesetzte Lösung daher in die Strukturen und Prozesse integriert werden, sprich für den Kunden möglichst wenig spürbar sein.

5.2. Digitale Identität

Da viele Online-Betrugsmethoden mittlerweile mit der Verschleierung der Identität einhergehen, wird es zunehmend essentiell, die Identität eines Kunden online eindeutig festzustellen. Der Markt bietet inzwischen eine Vielzahl an Identitätsmethoden und -verfahren – von Video-Ident und Ausweiserfassung bis hin zur Banken-Identität, die eine rechtskonforme Bestätigung der Identität ermöglicht. Auch hier gilt das Gesetz der Usability: Wird der Kunde in seiner Shoppinglaune durch ein kompliziertes Identitätsverfahren gestört, besteht die Gefahr des Kaufabbruchs. Somit punkten Onlineshops mit mehreren Identifikationsmöglichkeiten, aus denen der Kunde selbst wählen kann.

5.3. Alles aus einer Hand

Als führender Lösungsanbieter ermöglicht CRIF zum einen ein vernetztes und automatisiertes Risiko- und Betrugsvermeidungsmanagement. Zum anderen agiert CRIF als Identification Service Provider, der alle gewünschten Identifikationsverfahren im DACH-Raum und in weiteren europäischen Ländern anbietet. So profitieren Onlinehändler von einer ganzheitlichen Lösung, die ihr Online-Business bestmöglich absichert.

Zurück zum Inhaltsverzeichnis

ÜBER DIE STUDIE

Die Studie zum Thema „Betrug im Online-Handel“ wurde von CRIF im gesamten DACH-Raum durchgeführt. Rund 100 Online- und Versandhändler verschiedenster Branchen und Größenordnungen in Deutschland, Österreich und der Schweiz nahmen an der Online-Umfrage im Erhebungszeitraum September 2020 bis April 2021 teil.

FRAUD IM E-COMMERCE

DACH UMFRAGE 2020/2021

CRIF Bürgel GmbH
Leopoldstraße 244
80807 München
Tel: +49 40 89803-0
E-Mail: info@crifbuergel.de

www.crifbuergel.de

CRIF BÜRGEL
Together to the next level