

# Disruption im Handel dank Corona – Neue Erfolgsfaktoren für On- und Offline-Kanäle

Bei bargeldlosen Zahlungen war Deutschland im europäischen Vergleich lange das Schlusslicht. Doch nun greifen Konsumenten, wenn auch gezwungen durch Distanz- und Hygieneregeln, immer häufiger zu kontaktlosen Zahlungsmitteln wie Kredit- und Debitkarten. Im E-Commerce ist, trotz Umsatzboom, von diesem veränderten Verhalten wenig zu spüren. Hier ist der Rechnungskauf weiter die beliebteste Zahlart der Deutschen, was große Herausforderungen für Händler bedeutet.

Die Coronakrise hat das Kaufverhalten deutlich verändert. So kaufen 49 % der Europäer seit dem Ausbruch von COVID-19 seltener im stationären Handel ein, so eine Studie von PwC. Der Onlinehandel ist klarer Gewinner und verzeichnete zweistellige Wachstumsraten allein im zweiten Quartal 2020. Gerade der Lebensmittelhandel hat – nach längerem Anlauf – nun den Durchbruch geschafft: Mehr als ein Viertel der europäischen Einwohner in urbanen Ballungsräumen kauft Lebensmittel bereits vorwiegend online. Die Verbraucher schätzen Komfort und Sicherheit und arbeiten auch häufiger von zu Hause, wo sie problemlos Lieferungen empfangen können. Onlineshopping ist also quer über alle Segmente hinweg klar auf dem Vormarsch.

Auch hierzulande hat es einen deutlichen Wandel gegeben. Fast jeder Deutsche kauft heute im Internet ein. Laut neuesten Umfragen des Digitalverbands Bitkom sind es bereits 96 %, also 57 Mio. potenzielle Kunden. Danach bestellen 4 von 10 Personen (37 %) mindestens einmal pro Woche im Netz. Und wie das EHI Retail Institute in seiner Studie „Online Payment 2020“ ermittelt hat, kaufen 2 von 3 Kunden im Netz auf Rechnung ein: Mit rund 33 % aller Onlinekäufe liegt der Rechnungskauf damit auf Platz 1 der Zahlungsarten und hat diese Position im Vergleich zum Vorjahr sogar noch um 1,5 Prozentpunkte ausgebaut (Abb. 1).

Beim Onlineshopping gilt also der sogenannte Pay-Later-Ansatz: Erst die Ware, dann das Geld – so kaufen deutsche Konsumenten am liebsten ein. Allerdings birgt dieses Vor-



**Thomas Wernet** (✉)

verantwortet seit September 2020 die Vertriebsaktivitäten in den Branchen der Finanz- und Energiewirtschaft, der Versicherungen, der Telekommunikation und des E-Commerce. Er hatte zuletzt als Senior Vice President Sales & Account Management die Verantwortung für Neu- und Bestandskunden im Bereich Risk- und Fraud-Management bei Arvato Financial Solutions inne. Dank diverser Sales-Positionen in Unternehmen wie Wirecard, Billpay, Telefonica und Vodafone verfügt er über ein ausgedehntes Netzwerk sowie profunde Branchenerfahrung in den Bereichen Risikomanagement, Fraud Prevention und Payment. [info@crifbuergel.de](mailto:info@crifbuergel.de). Die CRIF Bürgel GmbH ist in Deutschland einer der führenden Informationsdienstleister für Firmen und Privatpersonen. Das Unternehmen bietet passgenaue Lösungen für die Identifikation, Bonitätsprüfung und Betrugsprävention, für Kreditrisiko- und Adressmanagement sowie zu Digitalisierung und Predictive Analytics für Unternehmen und Finanzinstitute. Weitere Infos unter: [www.crifbuergel.de](http://www.crifbuergel.de). [info@crifbuergel.de](mailto:info@crifbuergel.de)

Karlsruhe, Deutschland

Wirtschaftsinformatik & Management 2021 • 13 (2): 160–163  
<https://doi.org/10.1365/s35764-020-00311-w>

Angenommen: 1. Dezember 2020

Online publiziert: 21. Januar 2021

© Springer Fachmedien Wiesbaden GmbH, ein Teil von Springer Nature 2021

gehen ein hohes Risiko für Anbieter, gerade bei hochwertigen Gütern. So wurden zum Beispiel E-Bikes in der Vergangenheit kaum online auf Rechnung verkauft. Das Risiko eines Zahlungsausfalls ist vielen Händlern schlicht zu hoch.

Der Kauf auf Rechnung ist aber nur ein Aspekt der vielfältigen Kundenwünsche: So verschmelzen der stationäre und der Onlinehandel immer mehr. Kunden verschaffen sich im Netz die nötigen Produktinformationen und kaufen dann offline – oder umgekehrt. Sie erwarten daher über alle Kanäle hinweg identische Produktangebote, Preise und Zahlungsmöglichkeiten – eben einen integrierten Multi-Channel-Vertrieb. Eine gelungene Kombination der Kanäle haben etwa Händler wie Breuninger bereits geschaffen, andere arbeiten daran. Eine große Herausforderung für die Anbieter besteht darin, die Vorzüge des Webshops mit den Möglichkeiten am Point of Sale zu vereinen: Wenn Kunden ihren Lieblingsduft on-

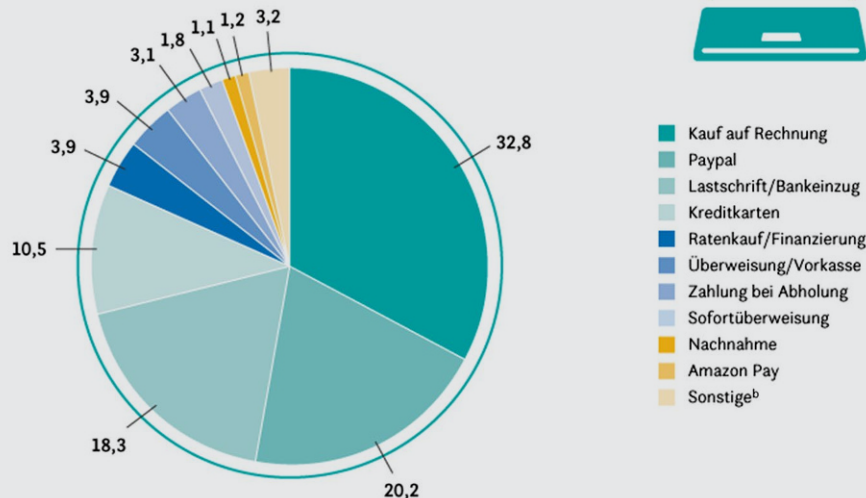
line auf Rechnung bezahlen können, warum dann nicht auch beim Besuch in der Parfümerie?

Aus Sicht des Kunden ist Bezahlen ja kein Vergnügen, sondern eher lästige Pflicht. Darum ist eine hohe Nutzerfreundlichkeit hier enorm wichtig. Gerade im Onlinehandel hat der Check-out eine ganz besondere Bedeutung. Er muss möglichst rasch und einfach gehen. Die Zukunft des Bezahlens wird wohl ohnehin so aussehen, dass Käufer und Verkäufer ganz ohne Rechnung oder Zahlungsmittel auskommen. Einen Vorgeschmack dazu liefert etwa Amazon Go: Die Geschäfte der Supermarktkette des US-Konzerns Amazon haben keine Kassen. Die Kunden gehen nach Auswahl der Waren ohne Kassiervorgang aus dem Geschäft, die gekauften Artikel werden durch Sensoren und Kameras erfasst und ihnen nach Verlassen des Ladens automatisch berechnet. Zukunftsmusik? Im Jahr 2019 gab es bereits 26 Filialen.

**Abb. 1** Erst die Ware, dann das Geld – so kaufen deutsche Konsumenten am liebsten ein.  
<sup>a</sup>Top-1000-Onlineshops laut Studie „E-Commerce-Markt Deutschland 2019“ EHI und Statista: 46,0 Mrd. Euro. <sup>b</sup> Sonstige: Alipay, Apple Pay, Debitkarten, Giropay, Google Pay, Paydirekt, Post-pay, Mastercard, Kryptowährungen, [Barzahlen.de](#), Kundenkarte, Gutscheinkarte, Prepaidkarte und WeChat Pay. Quelle: EHI-Studie Online-Payment 2020. EHI [handelsdaten.de](#); EHI Retail Institute®

## Gesamtmarkt<sup>a</sup>

Anteile in Prozent



Quelle: EHI-Studie Online-Payment 2020

EHI [handelsdaten.de](#)

EHI Retail Institute®

Für solche innovativen Zahlungswege muss der Anbieter den Kunden sehr gut kennen beziehungsweise zweifelsfrei identifizieren können. Das ist gerade im Online-Business sehr schwer: Kein Online-Anbieter kann all seine Kunden so gut kennen wie damals Tante Emma in ihrem Eckladen. Selbst wenn er sehr gut gepflegte Kundenbeziehungen hat, ist er gegen Kreditkartenbetrug, Identitätsdiebstahl und Kontoübernahmen nicht gefeit.

Tatsächlich sind diese Betrugsmuster im Web eher die Regel als die Ausnahme: In Deutschland waren 97 % der Onlineshops schon einmal Opfer von Betrug, in der Schweiz bereits 92 %. Dies zeigt die CRIFBÜRGELE-Umfrage „Betrug im Online-Handel“ vom Frühjahr 2020 unter 110 Online- und Versandhändlern aus beiden Ländern.

Und die Tendenz ist steigend: Laut einer aktuellen Studie von LexisNexis gab es weltweit im Zeitraum von Juni 2019 bis Juni 2020 bei den eCommerce-Transaktionen ganze 49 % Wachstum im Vergleich zum Vorjahr. Zugleich stieg allein im ersten Halbjahr 2020 die Zahl der Bot-Attacken auf Onlinehändler um 32 % im Vergleich zu den sechs Monaten zuvor. Betrüger nutzen Bots, um zum Beispiel gestohlene Anmelde- oder Kreditkartendaten zu prüfen oder Gutscheine einzulösen, wobei ihr Vorgehen immer raffinierter und damit schwerer zu erkennen wird.

Überdies konzentrieren sich Anbieter bei der Betrugsprävention vielfach nur auf Teilaspekte. Das Risiko eines Zahlungsausfalls kann zwar durch Überprüfung der Identität, Adressen und bestehender Zahlungserfahrungen ganz gut eingeschätzt werden. Kriminelle missbrauchen aber gerade gute und unauffällige Identitäten für ihre Zwecke: So ist, neben den Bot-Attacken, der sogenannte Account Takeover eine zunehmend häufigere Betrugsart. Hier versuchen Betrüger, sich mit gestohlenen Log-in-Daten oder durch den Einsatz von Schadsoftware Zugang zum Account des Opfers zu verschaffen. Ist das geschafft, nutzen sie die erbeuteten Informationen – wie etwa hinterlegte Zahlungsdaten – zum Beispiel, um im Namen des Opfers einzukaufen. Sie erhalten die Waren und nutzen die Dienste, die Rechnung aber bekommt das Opfer. So läuft das vielfach über einen längeren Zeitraum und bei verschiedenen Anbietern, die nicht misstrauisch werden, weil sie den Nutzer vermeintlich für einen gut bekannten und solventen Kunden halten. Wenn die Account-Übernahme bemerkt wird, ist der Schaden in der Regel längst entstanden.

Umfassende, intelligente Prävention wird also immer wichtiger, denn diese Betrugsmuster betreffen nicht nur Online-

shops, sondern auch Anbieter digitaler Dienste wie Banken, Telekommunikations- und Mobilitäts-Provider sowie Hosting- und Webservices, Streaming-, Dating- oder Gaming-Dienste und ähnliche Anbieter – überall, wo Betrüger Informationen missbrauchen können, um sich wirtschaftliche Vorteile zu verschaffen.

Schutz für Anbieter (und ihre Kunden) bietet die Kombination aus Standort- und Verhaltensdaten oder, anders ausgedrückt, physischer und digitaler Daten. Mit diesem Ansatz ist es möglich, in hoch dynamischen Geschäftsumfeldern erfolgreich zu sein, indem nicht nur vergangenheitsbezogene, klassische Identitäts- und Bonitätsdaten, sondern auch Realtime-Informationen für die Betrugsprävention mit einbezogen werden. Dabei kommt der verhaltensbasierten Biometrie als integrierte Lösung für Betrugsprävention und Risikobewertung besondere Bedeutung zu. Denn jeder Mensch hat eindeutige Merkmale, die ihn individuell kennzeichnen. Jeder Tastendruck, jedes Fingertippen und jede Wischgeste am Smartphone ist typisch für die jeweilige Person. So können die aus verschiedenen Sensoren stammenden Informationen analysiert und ein digitales Referenzmuster der Person gezeichnet werden, welches mit früheren und aktuellen Interaktionen verglichen wird.

Leistungsstarke künstliche Intelligenz erlaubt es, diese kaum sichtbaren biometrischen Kennzeichen zu nutzen. Die Machine-Learning-gestützte Prüfung von Kundenverhalten, Identitäts- und Gerätedaten erkennt Auffälligkeiten noch während eines Antrags- oder Bestellvorgangs und ermöglicht es den Fraud-Experten in die manuelle Klärfallbearbeitung einzusteigen. Die künstliche Intelligenz übernimmt Identitäts- und Betrugsprüfung, enttarnt Bot-Netzwerke und Betrug, warnt in Echtzeit und schützt so vor Missbrauch. Für bestmöglichen Schutz erfolgt die Prüfung parallel auf mehreren Ebenen, geprüft werden rund 900 verschiedene Faktoren:

- **Identity Proofing: Stimmt was nicht mit dem Nutzer?**  
Ist er real, schon einmal Kunde gewesen und wie steht es um seine Bonität?
- **Customer Order History: Stimmt was nicht mit dem Einkauf?**  
Entsprechen Frequenz und Warenwert dem typischen Verhalten, wird ungewöhnlich viel und teuer eingekauft oder anders bezahlt?
- **Device Intelligence: Stimmt was nicht mit dem Endgerät?**  
Gibt es Unregelmäßigkeiten bei IP-Adresse, Browser, Standort oder beim Tipp- und Klick-Verhalten?

- **Account Protection: Stimmt was nicht mit dem Kundenkonto?**

Passt das Verhalten zu den vorliegenden Daten oder wurden Stammdaten, zum Beispiel E-Mail- oder Heimatadresse, verändert?

- **Transaction Execution: Stimmt was nicht mit Abschluss und Lieferung?**

Stimmen Zahlungsdaten und Adresse mit früheren Käufen und anderen Quellen überein oder wird die Sendung womöglich umgeleitet?

Mittels Behavioural Biometrics und automatisierter Mustererkennung werden Betrüger ausgesiebt, bevor sie zum Zug kommen. Und dass bei reduziertem Aufwand für die manuelle Einzelbearbeitung: Machine Learning reduziert Klärfälle gegenüber herkömmlichen, regelbasierten Systemen um über 80 %. Überdies entwickelt sich das System stetig weiter. Jede neue Bestellung erweitert die Datenmenge und steigert die Qualität und Trennschärfe. Und nicht zuletzt: Die verhaltensbasierte Biometrie arbeitet im Hintergrund, ohne den Kunden in seinen Handlungsabläufen und in seiner Nutzererfahrung zu stören.

Im Idealfall wird der Bezahlvorgang für Kunden künftig genauso einfach wie das Verlassen einer Amazon-Go-Filiale ohne Kassiervorgang. Und auch für Händler wird vieles leichter: Sie erhalten eine erweiterte Entscheidungsgrundlage und müssen im Zweifel nicht von vornherein auf die beliebte Zahlung auf Rechnung verzichten. Stattdessen können sie sich auf echte Klärfälle konzentrieren, die Nutzererfahrung weiter verbessern sowie Zahlungsausfälle reduzieren bei gleichzeitiger Erhöhung der Conversion Rate.