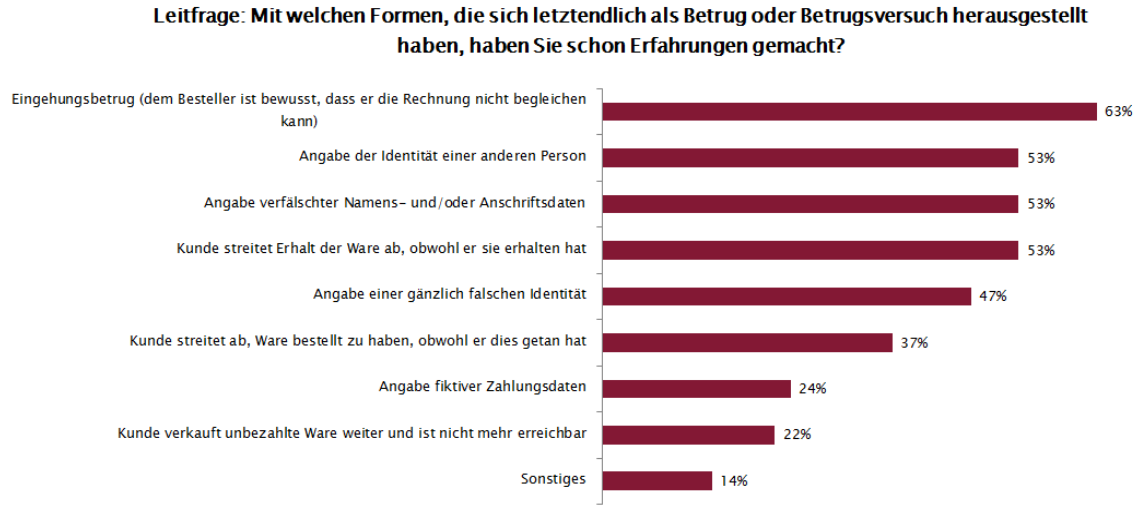
Online Betrugsprävention – Eine unternehmerische Gratwanderung

Von Christian Buttgereit

Das digitale Einkaufen ist ein wesentlicher Bestandteil unserer Gesellschaft geworden. Waren es vor einigen Jahren fast nur junge Leute, die sich auf ein Online-Shopping-Erlebnis eingelassen haben, so ist das Einkaufen über das Internet inzwischen ein generationsübergreifendes Thema. Alleine im letzten Jahr lag der eCommerce-Umsatz in Deutschland bei über 40 Mrd. Euro – Tendenz stark steigend. Leider gibt es aber auch eine Kehrseite. Nicht zuletzt aus den Medien erhält man fast täglich Berichte über die Risiken des Online-Shoppings: Datenklau der Konto- und Kreditkarteninformationen, Datenlecks oder scheinbar harmlose E-Mails, die einen freundlich auffordern, auf mysteriösen Seiten die persönlichen Daten inklusive Kontoverbindung zu aktualisieren oder doch einfach direkt eine Überweisung an ein dubioses Konto vorzunehmen.

Das Bundeskriminalamt weist einen Schaden durch Online-Kriminalität für private Endverbraucher von über 35 Mio. Euro aus (Stand 2015). Betrachtet man den volkswirtschaftlichen Schaden, inklusive Präventionsmaßnahmen, Ermittlungstätigkeiten, gehackte Kundendatenbanken, Schäden bei Privatpersonen und auch in Unternehmen etc., so belegt Deutschland den dritten Platz im weltweiten Ranking in Bezug auf die Kosten, die durch Online-Kriminalität verursacht werden: Über 50 Mrd. Euro werden schätzungsweise jährlich in Deutschland als solche Kosten verbucht, die der Online-Kriminalität zugerechnet werden. Die Dunkelziffer dürfte weitaus höher ausfallen.

Doch wie gestaltet sich das Bild aus Sicht der Unternehmen? Viele Unternehmen verfügen nicht über die entsprechenden Prüfprozesse und Reportinginstrumente, betrügerische Kunden bzw. Bestellungen zu identifizieren oder auch im Nachgang – nach Bestellung und Auslieferung – die Qualität der Kunden valide zu messen. Dreiviertel der deutschen Unternehmen mit Online-Shops wurden nach eigenen Angaben bereits Opfer von Online-Betrügern: Sei es durch Bestellungen, deren Rechnung im Nachgang nicht beglichen wurde, oder durch Verwendung gestohlener (und damit valider) Personen- und Kontodaten.

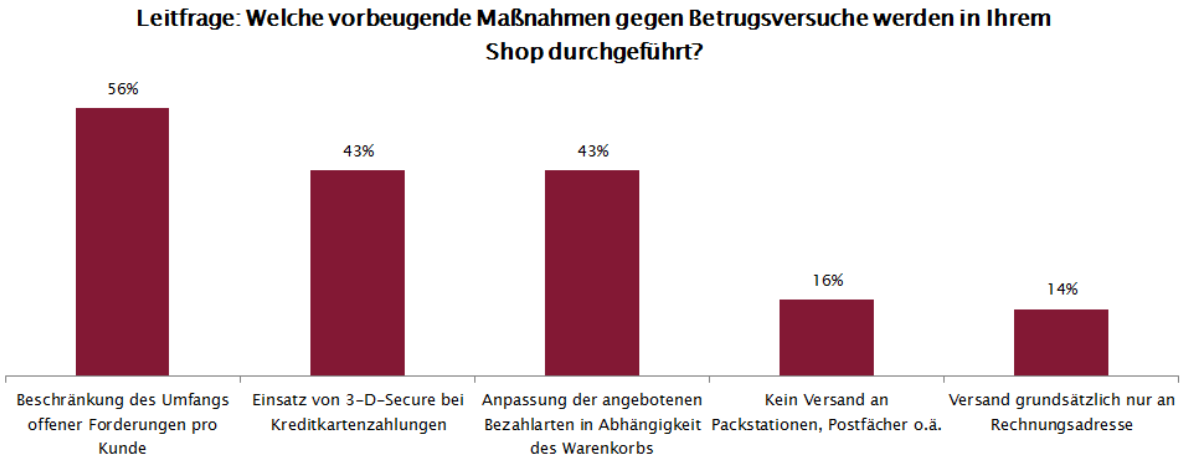


Quelle: ibi research 2015, n=163

Gerade das scheinbar anonyme Online-Geschäft lädt zu Betrugsversuchen ein. Nicht selten forcieren die Unternehmen jedoch selbst, in der Regel unbewusst, kriminelle Aktivitäten und verringern die Hemmschwelle für Betrugsversuche. Im Gegensatz zur „Offline-Welt“, dem Ladenlokal in der Fußgängerzone oder dem Warenhaus in der Innenstadt, können Kampagnen, Sonderangebote oder Aktionen verhältnismäßig kostengünstig im virtuellen Schaufenster präsentiert werden. Diese „Einfachheit“ verführt die Unternehmen zur schnellen Umsetzung ihrer digitalen Abverkaufsinitiativen und zieht womöglich Betrüger an. Was kann, auch mit einfachen Mitteln, unternommen werden?

- Verringerte Kaufhürden für Neukunden, bspw. durch minimale Datenabfrage bei Bestellungen als „Gast“.
- Aggressive Online-Werbung im Bereich Display oder Suchmaschinen-Marketing (SEM) bzw. falsche Auswahl der Affiliate-Partner.
- Rabatt- und Sonderaktionen für hochwertige Produkte.
- Abo-Modelle mit niedriger Erstzahlung oder Ratenzahlungen.
- Warenbestellungen auf Rechnung, auch für Neukunden/ Gastbestellungen.
- Keine Warenkorbbegrenzung bei hochwertiger Ware bei Neukundenbestellungen.

Die Praxis zeigt, dass einige Online-Shops einfache, vorbeugende Maßnahmen einsetzen, um die Kriminalität einzudämmen und gute von schlechten Bestellungen zu separieren.



Quelle: ibi research 2015, n=119

Eine besondere Herausforderung ergibt sich jedoch bei der Implementierung von detaillierten, integrierten und professionellen Prüfschritten zur Identifizierung von Online-Betrug. Betrachtet man Ende-zu-Ende den kompletten Kauf- und Bearbeitungsprozess von Internetbestellungen, so fängt dieser bereits im Suchmaschinen-Marketing und der Auswahl der Affiliate-Partner an, geht über die hausinterne Datenspeicherung und Qualitätsprüfung, und endet letztlich nicht beim Logistikdienstleister bzw. Paketlieferdiensten. Auch noch nach scheinbar erfolgreicher Abwicklung des Geschäfts und der damit verbundenen Zustellung beim Kunden – sei es physisch bei Paketbestellungen oder virtuell bei digitalem Content oder Krediten – können noch Szenarien für entgangenen Umsatz entstehen: Die Bankdaten für die Einzugsermächtigung sind falsch (ob unabsichtlich oder böswillig) oder Laufzeitverträge oder Finanzierungsmodelle werden nicht bedient und der Kunde ist, aufgrund falscher Angaben, nicht ausfindig zu machen. Doch wie können sich Unternehmen schützen? Hier gibt es unterschiedliche, kostengünstige wie auch kostenintensive, Ansätze:

- Integration von externen Dienstleistern, z. B. mittels Bonitätsprüfung, in den Online-Kaufprozess.
- Aufbau einer internen Betrugsdatenbank.
- Automatische Applikationen zur Real-Time-Überprüfung von Adress- und Bankdaten.
- Kommunikationsschnittstellen zur Rückmeldung von Auffälligkeiten durch Logistikdienstleister oder aus dem Mahnwesen.
- Professioneller Einsatz von Software zur Überprüfung bspw. von Gerätestandorten, über die die Bestellung getätigt wird, IP-Adressen, Browser- und Hardware-Einstellungen.

Für Unternehmen und Betreiber von Online-Shops gilt es, die Gratwanderung zwischen hinnehmbaren Umsatzeinbußen, z. B. durch attraktive Preismodelle, und Abwendung von Betrug zu

meistern. Eine wirtschaftliche Betrachtung ist zwingend notwendig, da ein durchgängiges Betrugspräventionsmanagement über alle beteiligten Abteilungen hinweg einen hohen Kosten-, Ressourcen- und Organisationsaufwand bedeuten kann. Online Marketing, Fulfillment, Logistik, Mahnwesen, Controlling, Risk Management usw. müssen eingebunden werden und es gilt mögliche Grabenkämpfe und Fürstentümer zwischen den Bereichen abzubauen. Während bspw. das Marketing mit Kampfpreisen möglichst viele Neukunden gewinnen will, möchte das Mahnwesen gerne nur Kunden mit „Qualität“ (=Liquidität) im Kundenstamm sehen. Hier zeigen sich oft unternehmensinterne Ziel- und Interessenskonflikte.

Die Implementierung eines Betrugspräventionsmanagements bietet viele Möglichkeiten, günstige und/oder kostenintensive Prüfschritte zu implementieren. Es gilt, unter Berücksichtigung der Wirtschaftlichkeit, eine angemessene Lösung für das Unternehmen zu finden, die zum Produkt- und Leistungsportfolio sowie zur Zielgruppe passt.

Haben Sie Fragen zur Implementierung von Systemen und Prozessen zur Betrugsprävention? Wir helfen Ihnen gerne weiter! Sie erreichen uns per Mail unter christian.buttgereit@anxo-consulting.com oder unter Telefon 06192 40 269 0.

ANXO. Wir verändern Ihre Welt.

Quellen:

Cybercrime – Bundeslagebild, Bundeskriminalamt 2015

Betrug und Betrugsprävention im Online-Handel, ibi research 2015