Online Betrugsprävention –

Eine unternehmerische Gratwanderung

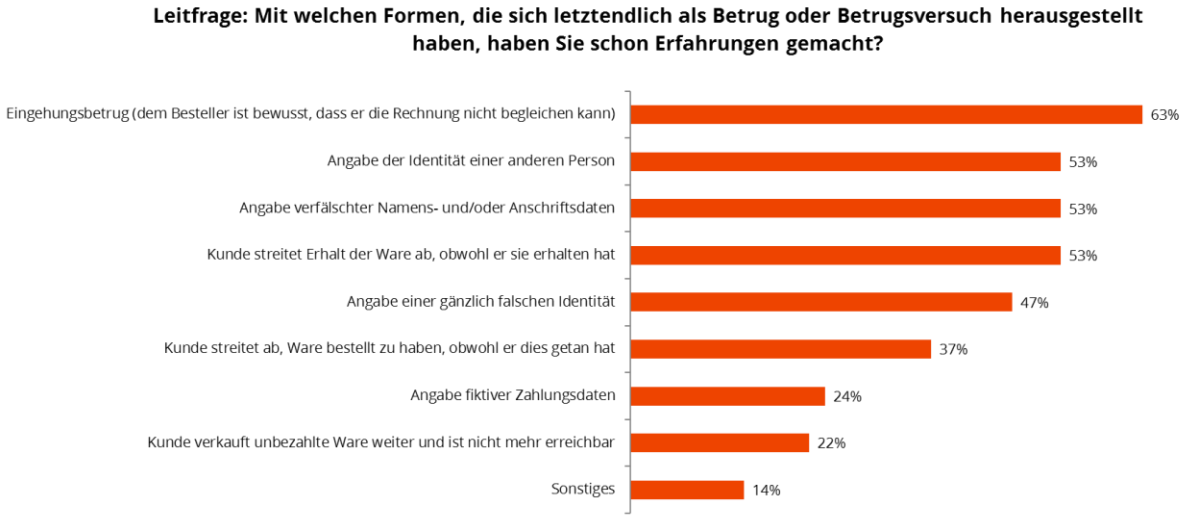
Von Christian Buttgereit

Hört man die Begriffe „Botnets“, „DDoS Attacken“ oder „Darknet“ so könnte man meinen, es handle sich um eine neue Star Wars-Episode, in der das Gute mal wieder gegen die dunkle Macht antritt. Ganz so weit hergeholt ist es allerdings nicht. Es handelt sich durchaus um Begriffe aus einem Kampf „Gut gegen Böse“. Die Guten sind in diesem Falle die Unternehmen. Die Bösen sind die Cyber-Kriminellen. Und wir befinden uns mitten drin im Krieg der digitalen Welten.

Das digitale Einkaufen ist schon längst nicht mehr der Generation Y (Geburtsjahre 1980 – 1999), den sogenannten Digital Natives vorbehalten. Durch alle Bevölkerungsschichten und Altersklassen zieht das Bestreben, digital einzukaufen. Online-Shopping kann allerdings mit gewissen Risiken verbunden sein: Datenklau der Konto- und Kreditkarteninformationen, Datenlecks oder Mails, die einen freundlich auffordern, auf mysteriösen Seiten die persönlichen Daten inkl. Kontoverbindung zu aktualisieren. Doch wie sieht das digitale Schlachtfeld aus Sicht der Unternehmen aus?

Deutschland belegt den dritten Platz im weltweiten Ranking im Bezug auf Schaden verursacht durch Online-Kriminalität. Über 60 Mrd. Euro werden jährlich in Deutschland als Schaden verbucht, der durch Online-Kriminalität verursacht wurde. Die Dunkelziffer dürfte weitaus größer ausfallen. Denn 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 richtig zu kategorisieren. Dreiviertel der deutschen Unternehmen mit Online-Shops wurden bereits Opfer von Online-Betrügern: Sei es durch Bestellungen, deren Rechnung im Nachgang nicht beglichen wurde, oder durch Bestellungen über geklaute – und damit valide – Personen- und Kontodaten.



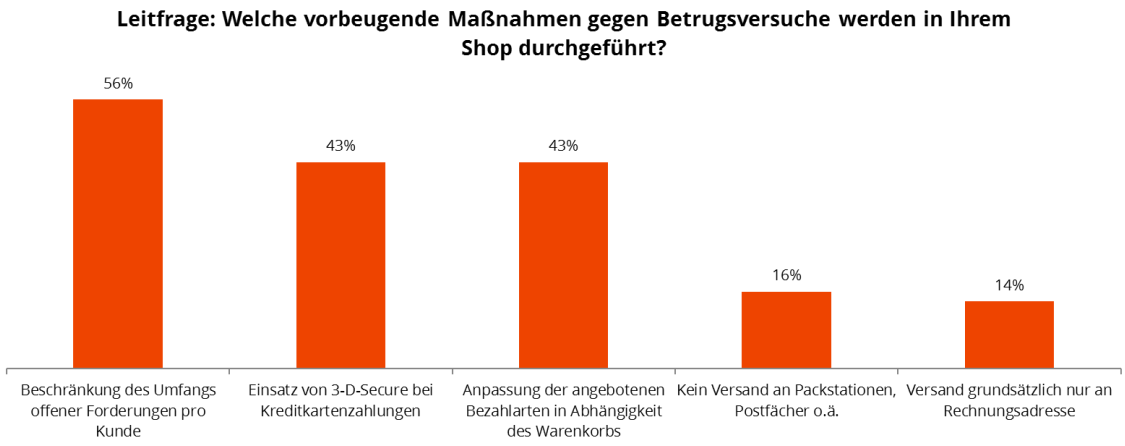
Quelle: ibi research 2015

Gerade das scheinbar anonyme Online-Geschäft lädt zu Betrugsversuchen ein. Nicht selten forcieren die Unternehmen jedoch selbst, in der Regel unbewusst, betrügerische Aktivitäten und verringern die Hemmschwelle für Betrugsversuche:

- Verringerte Kaufhürde für Neukunden, bspw. durch minimale Datenabfrage bei Bestellungen als „Gast“.

- Aggressive Online-Werbung im Bereich Display oder SEA bzw. falsche Auswahl der Affiliate-Partner.
- Rabatt- und Sonderaktionen für hochwertige Produkte.
- Abo-Modelle mit niedriger Erstzahlung oder mit Ratenzahlungen.
- Warenbestellungen auf Rechnung, auch für Neukunden/ Gastbestellungen.

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. Es müssen keine Flyer oder Plakate gedruckt werden, keine Plakatwände aufgestellt werden oder große Werbebanner innerhalb oder außerhalb der Einkaufsräume platziert werden. Diese „Einfachheit“ verführt die Unternehmen zu schnellen Umsetzungen ihrer Abverkaufsinitiativen und zieht womöglich Betrüger an. Allerdings sind auch viele Online-Shops vorbereitet und setzen bereits schon recht einfache Instrumente ein, um die Cyber-Kriminellen abzuwehren und gute von schlechten Bestellungen zu sortieren.



Quelle: ibi research 2015

Eine besondere Herausforderung ergibt sich jedoch bei der Implementierung von detaillierten 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 (SEM) und der Auswahl der Affiliate-Partner an, geht über die hausinterne Datenspeicherung und Qualitätsprüfung und endet letztlich nicht nur im engen Austausch mit dem Logistikdienstleister bzw. Paketlieferdient. 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. zur 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.

Eine besondere Herausforderung für Unternehmen und Betreiber von Online-Shops ist die Abwägung zwischen hinnehmbaren Umsatzeinbußen und Abwendung von Betrug. 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, Fulfilment, Logistik, Mahnwesen, Finance, Risk Management usw. müssen eingebunden werden und es gilt mögliche Grabenkämpfe und Fürstentümer 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 Betrugspräventationsmanagements bietet viele Möglichkeiten, günstige und/oder kostenintensiv Prüfschritte zu implementieren.

Es gilt unter Berücksichtigung der Wirtschaftlichkeit eine angemessene Lösung zu finden, die zum Produkt- und Leistungsportfolio sowie zur Zielgruppe passt.

Haben Sie Fragen zur Implementierung von Systemen und Prozessen zur Betrugspräventation? Melden Sie sich gerne gerne unter c.buttgereit@buttgereit-consulting.de oder unter 0211 93077305.

Quellen:

ibi research 2015

Über Buttgereit Consulting:

Buttgereit Consulting steht für innovative und ergebnisorientierte Beratung, Interim Management und Projektleitung in der digitalen Welt.

Durch die unterschiedlichen Beratungsprojekte und Erfahrungen im nationalen und internationalen Umfeld können Problemstellungen schnell erkannt und gemeinsam mit dem Mandanten Lösungen erarbeitet werden. Schwerpunkt bildet hierbei die Beratung im digitalen Themenumfeld für Handels-, Dienstleistungs- und Industrie-Unternehmen, die ihren digitalen Footprint auf- bzw. ausbauen möchten. Beratungsfokus ist im Wesentlichen: Digitale Transformation, Internet of Things (IoT), Industrie 4.0, Marketing, Strategieentwicklung, Prozessoptimierung, eCommerce, Online- und Mobile-Services sowie Cross Channel-/Omni Channel-Vertrieb im Privat- und Geschäftskundenbereich.