

## Presseclipping

---

Kunde: Computop

Publikation: ChannelPartner (IDG Expertennetzwerk)

Ausgabe: 06.12.2019

Seite: Online

Titel: „Biometrie im E-Commerce“

Auflage / Page Impressions pro Monat: 1.200.000 PIs

06.12.2019

Autor: Ralf Gladis (Experte)

Betrug minimieren, Sicherheit maximieren

## Biometrie im E-Commerce

**Geringe Betrugsraten steigern sowohl die Kundenzufriedenheit als auch den Umsatz. Neue Technologien ohne Passwörter schaffen die Voraussetzungen.**



Das Entsperren des Smartphones via Gesichtsscan kann im E-Commerce eingesetzt werden. Dann muss man sich keine Nutzerkennung-Passwort-Kombinationen mehr merken. Foto: Prostock-studio - shutterstock.com

Sicherheit ist ein menschliches Grundbedürfnis, dessen Befriedigung sich in ungeheurer Vielfalt in unserem Alltag manifestiert. Egal, ob wir unseren nächsten Autokauf vorbereiten, einen Partner wählen oder unsere

Altersvorsorge planen – wir sehnen uns stets nach einem gewissen Mindestmaß an Sicherheit und schätzen das Gefühl, sorglos auf jene Teilbereiche unseres Lebens blicken zu können, die sie uns bieten. Folgerichtig sollte es das Ziel eines jeden Unternehmens sein, dieses elementare Verlangen auch im Geschäftsmodell zu verankern.

Das gilt gerade im E-Commerce, bei dem Sicherheit nicht nur auf Kunden-, sondern auch auf Händlerseite einen enormen Stellenwert einnimmt. Kundendaten, insbesondere die Zahlungsdaten, sind heilig und sollten um jeden Preis geschützt werden. Wer ein Höchstmaß an Sicherheit mit außergewöhnlichem Komfort verbinden kann, minimiert Betrug, steigert die Konversion und pflegt nicht zuletzt seine Marke.

### **Mehr Sicherheit bedeutet mehr Umsatz**

Das mag zunächst verwundern, denn alljährlich lesen wir in den Nachrichten Statistiken, in denen wir erschreckende Einblicke erhalten, wie fahrlässig die Menschen im Internet mit ihrer Sicherheit umgehen. Inzwischen dürfte weithin bekannt sein, dass die übliche Kombination aus Passwort und Nutzernamen (oder E-Mail), die Online-Konten im Regelfall schützt, möglichst komplex sein sollte. Dennoch bedienen sich viele User ihrer Geburtsdaten, der Namen ihrer Lebenspartner und Haustiere oder anderen leicht zu erratenden Codes. Meist muss diese Kombination dann noch für alle Accounts gleichzeitig erhalten, von Amazon bis Zalando. Sicher geht anders.

Ist den Menschen Sicherheit also doch nicht so wichtig? Nein, im Gegenteil. Doch der Aufwand, sich etliche Passwörter und Nutzernamen zu merken, verhindert einen bewussteren Umgang mit der Thematik. Ebenso viele Menschen verspüren den Wunsch schlank und sportlich zu sein, bringen aber nicht die nötige Disziplin auf oder finden schlicht und ergreifend nicht die Zeit, um in Form zu kommen.

Das ist ein Grund, warum vermeintliche Schlankheitskuren und Diäten beständig riesige Umsätze generieren, obwohl sie in den seltensten Fällen funktionieren. Allein das Versprechen wirkt unglaublich verlockend. Was jedoch, wenn es im Bereich Online-Sicherheit wirklich ein Mittel gäbe, das zuverlässig und erwiesenermaßen wirkt? Könnte es sich ein Unternehmen leisten, darauf zu verzichten?

### **Argument für Kundenbindung**

In der Tat haben Firmen mächtige Argumente in der Hand, das Kundenvertrauen zu erhöhen und sich von der Konkurrenz abzuheben, sofern sie neueste Sicherheitsmechanismen anwenden. Die Zauberworte heißen Biometrie und starke Kundenauthentifizierung.

Mit der zunehmenden Verbreitung von biometrischen Logins gibt es Alternativen, die sowohl die Passworteingabe obsolet machen als auch höchstmögliche Sicherheit garantieren. Wer einfach seinen Daumen auf einen Fingerabdrucksensor legt, muss sich keine lästigen Passwort-Nutzername-Kombinationen mehr merken, geschweige denn ausdenken. So ist der Kunde komfortabel und zugleich sicherer im Netz unterwegs.

Bei einer guten Biometrielösung wird weder ein Passwort auf dem Server des Händlers abgelegt, noch verlässt ein rekonstruierbares Abbild des Fingerabdrucks, der Stimme oder des Gesichts das Gerät, mit dem es aufgezeichnet wurde. Folgerichtig kann selbst bei einem Datenleck des Händlers kein Schaden entstehen, denn modernste Lösungen, die mit dem FIDO-Standard arbeiten, funktionieren äußerst ausgeklügelt.

### **Verfügbar auf sämtlichen Geräten**

Wer über FIDO bereits alles weiß, kann gleich mit der nächsten Überschrift weitermachen. Doch es ist wichtig zu verstehen, was hinter dem Akronym steckt. Es steht für Fast Identity Online. Dabei handelt es sich um einen Branchenverband, der sich seit 2012 damit beschäftigt, die weltweit gängigen Standards zur auf Biometrie basierenden Identifizierung von Online-Usern zu definieren und damit die Abhängigkeit von Passwörtern zu reduzieren.

Dafür arbeiten führende Unternehmen der Szene zusammen, unter anderem Infineon, PayPal, Microsoft, Mastercard und Visa. Der Verband vergibt Zertifikate, die verbiefen, dass diese definierten Standards eingehalten werden. So können Nutzer und Anbieter von Online-Services gleichermaßen auf ein Höchstmaß an Sicherheit und Komfort vertrauen.

Und diese Standards, namentlich FIDO2/WebAuthn, haben es in sich. FIDO2 sorgt für die Authentifizierung im Internet und stellt eine fortschrittlichere und sicherere Alternative zu den klassischen Passwörtern dar. Es besteht aus zwei Komponenten: Einer API namens WebAuthn, die sicherstellt, dass FIDO auf allen Browsern und Web-Plattform-Infrastrukturen nutzbar ist und einem Protokoll namens CTAP, das dafür sorgt, dass die verschlüsselte und sichere Authentifizierung auf allen möglichen Geräten funktioniert. Das können spezielle USB-Sticks, NFC-Geräte, Bluetooth-Zubehör oder aber normale PCs, Laptops, Tablets und Smartphones sein.