Der letzte Welt-Passwort-Tag?

Von Volker Koppe – Der erste Donnerstag im Mai ist jedes Jahr der „World Password Day". Und dieses Jahr könnte seine letzte Stunde geschlagen haben – zumindest in Europa, denn hier wird die PSD2 mit den Anforderungen der Strong Customer Authentication (SCA) dazu beitragen, dass Passwörter für immer der Vergangenheit angehören werden, wenn es um die Authentifizierung von Zahlungen geht.

Eigentlich ist es überraschend, dass es so lange gedauert hat. Das Computer-Passwort wurde in den sechziger Jahren von Fernando Corbato erfunden und ist damit bereits über ein halbes Jahrhundert alt. Um sich ihre Passwörter besser merken zu können, schreiben viele sie auf. Manche benutzen dasselbe Passwort für verschiedene Accounts oder wählen einfach eines, das sich leicht erraten lässt. Laut der Security-Firma Splash Data sind die beiden meistverwendeten Passwörter „123456" und „password" – ein Traum für Hacker und Betrüger.

Zeit für etwas Neues

Das Zahlungsökosystem hat sich gewandelt – und daher muss sich auch die Art und Weise verändern, wie wir es sicher gestalten. Authentifizierung und Betrugserkennung sind mittlerweile so weit entwickelt, dass manche Banken und Händler heute schon Unterschrift und PIN als optional ansehen. Seit Oktober 2018 können Händler im Visa-Payment-Netzwerk auf Unterschriften verzichten, wenn sie die sicheren EMV-Chips nutzen. 3D Secure 2.0 kann heute zehn Mal mehr Daten auswerten und prüfen als je zuvor. So können Internettransaktionen im Hintergrund analysiert werden, ohne dass der Verbraucher aktiv werden muss. Darüber hinaus sorgt die Weiterentwicklung von Künstlicher Intelligenz für eine schnellere und genauere Betrugserkennung.

Vor dem Hintergrund dieser verbesserten Sicherheit passt das Konzept des Passworts nicht mehr. Dank der neuesten Technologien und der Ausnahmen von der starken Kundenauthentifizierung gibt es auch nach dem Inkrafttreten der PSD2 am 14. September 2019 eigentlich nur zwei Gründe, Verbrauchern zusätzliche Sicherheitsschritte aufzuerlegen: Entweder um die Identität des Karteninhabers sicherzustellen, oder weil einer der beteiligten Partner Auffälligkeiten bei der Zahlung entdeckt, die auf einen Betrugsversuch hindeuten könnten. Im ersten Fall sollte die zusätzliche Sicherheitsmethode Verbrauchern vermitteln, dass ihre Identität geschützt wird; im zweiten Fall sollte sie Betrüger zuverlässig abwehren. Ein Passwort kann weder das eine noch das andere erreichen.

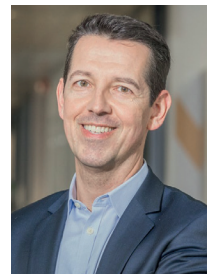
Flexible Authentifizierung

Die starke Kundenauthentifizierung ermöglicht einen neuen, moderneren Ansatz für den Verbraucher von heute. Die Frage ist also nicht, ob wir Kunden neue Authentifizierungsmöglichkeiten bieten sollten, sondern welche. Sicherheit ist immer dynamisch und anspruchsvoll – das muss sie auch sein, um Betrug zu verhindern. Aber das heißt nicht, dass wir auf einfache und kundenfreundliche Lösungen verzichten müssen. Visa arbeitet mit Kunden und Partnern eng daran, kreative Ideen zu entwickeln, damit verbesserte Sicherheit für Handel, Banken und Konsumenten nicht zu einer Belastung wird. Die zwei prominentesten Nachfolger für das Passwort sind dabei One-Time-Passcodes (OTPs) und Biometrie.

OTPs sind dabei für viele die nächstliegende Option. Die Sicherheit eines einzigartigen Codes übersteigt die eines Passworts – hinzu kommt die einfache Nutzung, denn der Code wird direkt an ein Mobilgerät geschickt, das auf einen spezifischen Karteninhaber zugelassen und mit großer Wahrscheinlichkeit in seiner Nähe ist. Nicht das Gerät ist in diesem Fall der Schlüssel, sondern der Code selbst. Somit kann der Code auch per E-Mail oder sogar per Festnetztelefon weitergegeben werden und damit verschiedenen Nutzerbedürfnissen gerecht werden. Das System ist vielen Nutzern bereits bekannt – wer sich in sein E-Mail-Konto oder sein Online-Banking einloggt, nutzt in vielen Fällen bereits heute OTPs. Ein Großteil der benötigten Infrastruktur steht also bereits zur Verfügung.

Die spannendere Option ist die biometrische Authentifizierung. War diese noch vor zehn Jahren nur ein Thema in Hollywood-Filmen, ist Biometrie heute längst alltäglich. Seit Fingerabdrucksensoren vor sechs Jahren zum ersten Mal serienmäßig in Smartphones verbaut wurden, haben sich Nutzer an sie gewöhnt und bringen der Technologie wachsendes Vertrauen entgegen. Eine US-amerikanische Visa-Studie zeigt, dass Verbraucher biometrische Authentifizierung für schneller, einfacher und sicherer als Passwörter halten. 83 Prozent der Verbraucher haben generell Interesse daran, durch Biometrie ihre Identität zu bestätigen oder Zahlungen zu verifizieren; 59 Prozent sind bereits mit Biometrie vertraut. Die biometrische Authentifizierung liefert die hohe Sicherheit der starken Kundenauthentifizierung ohne die Komplikationen, die von vielen befürchtet wurden.

Vielleicht liegt die Antwort darin, dem Kunden die Wahl zu lassen. Derselbe Verbraucher kann schließlich seine mobile Zahlung per Fingerabdruck authentifizieren, beim Kauf von Flugtickets am PC jedoch lieber ein Einmalpasswort/OTP per E-Mail nutzen. Und die Sicherheitsbedürfnisse verschiedener Konsumenten können sehr unterschiedlich sein. Unsere Infrastruktur bietet genau diese Flexibilität, damit der Handel und Banken auch in einer PSD2-Welt die Balance zwischen Sicherheit und Komfort sicherstellen können.



Volker Koppe, Head of Digital, Central Europe bei Visa, Frankfurt am Main