Starke Kundenauthentifizierung – noch viel zu tun

Von Swantje Benkelberg

Der große Aufschrei des Handels nach dem finalen Stichtag für die Umsetzung der starken Kundenauthentifzierung ist ausgeblieben. Das heißt aber nicht automatisch, dass alles zur Zufriedenheit aller Beteiligten gelaufen ist. Auswertungen von Computop zeigen vielmehr, dass die Erwartungen an 3D-Secure 2 sich bisher nicht erfüllt haben. Dabei zeigen sich zwar Unterschiede nach Handelsbranchen und Banken. Nachbesserungsbedarf gibt es jedoch offenbar noch reichlich. Red.

Vor allem in den Jahren 2019 und 2020 war die vollständige Umsetzung der PSD2 mit der Umstellung auf starke Kundenauthentifizierung eines der Hauptthemen, die die Paymentbranche umtrieb. Würden Banken, Acquirer und Händler es rechtzeitig schaffen, sich auf die neuen Vorgaben einzustellen? Würde zum Stichtag 31. Dezember 2020 – auch das schon eine Verlängerung gegenüber dem ursprünglichen Termin – im deutschen E-Commerce dank SCA nichts mehr gehen? So laut waren die Äußerungen der Bedenkenträger, dass die BaFin sich quasi im letzten Moment doch noch auf eine Umsetzung in Stufen einließ.

Fehlanzeige bei Vollzugsmeldungen

Seit Ende März ist nun endgültig Schluss mit der Verlängerung. Und was geschieht? Nichts. Nach all den Verlautbarungen darüber, mit welchen Problemen alle Beteiligten bei der Umsetzung der starken Kundenauthentifizierung zu kämpfen haben würden, hätte man doch zumindest ein Fazit dazu erwarten dürfen, wie denn der Übergang tatsächlich gelaufen ist. Stattdessen herrscht quasi ohrenbetäubendes Schweigen.

Das wiederum lässt sich auf verschiedene Weise interpretieren. Erstens wäre es natürlich denkbar, dass die Umstellung so gut gelaufen ist, dass die Kommunikatoren in den Unternehmen dies keiner Erwähnung für wert halten. „Alles bestens" ist nun einmal keine besonders aufregende Schlagzeile.

Hinzu kommt, dass man sich damit für zukünftige Fälle regulatorischer Änderungen bei der BaFin unglaubwürdig machen würde: Erst jahrelang zetern – und dann erweist sich, dass alles nur halb so schlimm war? Auf Nachsicht der Aufsicht und Gnadenfristen ohne Ende bräuchte man dann in Zukunft nicht mehr zu hoffen. Allerdings gilt das unabhängig davon, ob Erfolgsmeldungen verbreitet werden oder nicht. Schließlich hat die Aufsicht Einblick in den Sachverhalt und wird auch so merken, wenn all das Rufen nach Verlängerung und stufenweisem Hochlauf vielleicht doch übertrieben war.

Szenario Nummer zwei: Es kam alles genauso schlimm wie erwartet. Händler und ihre Kunden waren schlecht vorbereitet, die Erfolgsquoten der Authentifizierung sanken und mit ihnen die Konversionsraten der Händler. Warum dann aber kein öffentlicher Aufschrei des Handels oder der Payment-Dienstleister nach dem Motto: „Wir haben es ja vorausgesagt?"

Auch hier sind wieder zwei Möglichkeiten vorstellbar. Entweder sind die Einbrüche schlicht nicht so stark aufgefallen, weil sie auf einen E-Commerce-Markt trafen, der durch die Corona-Pandemie noch stärker wuchs als zuvor schon und in dem der Lockdown-Boom leicht übersehen ließ, dass die Geschäfte noch weitaus besser hätten laufen können, gäbe es die Probleme mit der starken Kundenauthentifizierung nicht. Oder die Probleme sind sehr wohl offenkundig geworden, die Payment-Dienstleister wollen damit jedoch nicht an die Öffentlichkeit gehen, um nicht vor der Branche schlecht dazustehen. Vermutlich ist es eine Mischung aus beidem.

Die Payment-Dienstleister geben sich zugeknöpft

Fest steht: Die Dienstleister tun sich extrem schwer damit, Informationen dazu herauszugeben, wie sich denn die Situation im E-Commerce seit April dieses Jahres unter PSD2 entwickelt hat, wie

Erfolgsquoten bei der Authentifizierung aussehen oder auch nur, ob sich der Zahlungsverkehrsmix seitdem wie erwartet verändert hat. Kommentare wie „sehr sensibles Thema" lassen jedoch nicht darauf schließen, dass alles zum Besten steht. Dass sich die Anbieter für ihre Erfolge selbst sehr gut loben können, ist schließlich bekannt.

Man wird also festhalten dürfen: Die Umsetzung der starken Kundenauthentizierung ist keineswegs hervorragend vollzogen worden und es gab oder gibt noch mancherlei nachzuarbeiten. Wo genau, dabei wollen sich die meisten Unternehmen nicht in die Karten schauen lassen. Einzig Computop hat auf einer virtuellen Veranstaltung Daten aus den eigenen Analysen veröffentlicht und die Auswertungen im Anschluss der Karten-Redaktion überlassen. Die Auswertungen basieren auf 25,5 Millionen Transaktionen von 2 590 Online-Händlern im Zeitraum Oktober 2020 bis Mai 2021.

3D-Secure 1.0.2 ist erfolgreicher als 3D-Secure 2.1

Aus diesem Datenmaterial geht folgendes hervor:

– Die Einführung von 3D-Secure 2 hat zumindest keine Katastrophen verursacht;

– 3D-Secure 2.1 und 1.0.2 sind beide parallel im Einsatz und nutzbar;

– Banken und Acquirer sind mit der Umstellung noch nicht fertig: Es fehlt noch an 3D-Secure 2.2 mit Ausnahmeregeln;

– Banken stufen viele 3DS-2-Transaktionen auf 3DS 1 herab (Downgrade);

– Viele Händler nutzen weiterhin 3D-Secure 1.0.2, weil es besser – sprich mit höheren Erfolgsquoten – funktioniert.

Aber: Sowohl im April als auch im Mai 2021 sind die Erfolgsquoten der Authentifizierung in den 27 EU-Ländern zurückgegangen – und zwar bei Visa- wie auch bei Mastercard-Transaktionen. Im Mittel der 27 Länder betrug die Erfolgsquote bei Visa im Mai 80 Prozent mit 3DS 2.1 – gegenüber 89 Prozent mit 3DS 1.0.2. Ganz ähnlich bei Mastercard: Hier lag die Erfolgsquote von 3DS 2.1 bei 80 Prozent – gegenüber 86 Prozent bei der Version 3DS 1.

Das Fazit lautet also: Bei Authentifizierungen ist 3D-Secure 1.02 besser als 3D-Secure 2.1. Das ist insofern ernüchternd, als die Branche sich doch gerade von 3D-Secure 2 nicht nur mehr Sicherheit, sondern auch ein verbessertes Handling versprochen hatte. Bisher zumindest kann 3D-Secure 2 diese Erwartungen offenbar nicht einlösen. Auch bei den Autorisierungen sieht es nicht besser aus. Auch hier ist 3DS 1 besser als 3DS 2. Im Mittel der 27 Länder liegt die Erfolgsquote bei der „alten" Version bei Visa mit 93 Prozent um einen Prozentpunkt höher als bei der „neuen". Bei Mastercard beträgt die Differenz sogar drei Prozentpunkte (93 Prozent bei 3DS 1 gegenüber 90 Prozent bei 3DS 2.1).

Modehandel hat die größten Probleme mit 3DS 2

Die Daten zeigen allerdings auch deutliche Unterschiede nach Branchen. Und hier gibt es – zumindest bei Mastercard – durchaus Bereiche, in denen 3DS 2.1 sich bei der Authentifizierung als erfolgreicher erweist als die Vorgängerversion 3DS 1, nämlich die Branchen Automotive, Consumer Electronics und Lebensmittel. Bei Visa liegen die Erfolgsquoten von 3DS 2.1 hingegen branchenübergreifend durchweg unter denen von 3DS 1.0.2.

Bei Transaktionen mit beiden Schemes scheint vor allem der Modehandel Probleme mit 3D-Secure 2 zu haben. Bei Visa-Transaktionen liegt hier die Erfolgsquote der Authentifizierung mit 82 Prozent um 12 Prozentpunkte niedriger als bei 3D-Secure 1. Bei Mastercard beträgt die Differenz sogar 14 Prozentpunkte (93 versus 79 Prozent).

Schwachstelle Kunde

Die Ursachen dafür, dass es noch nicht so gut läuft, lassen sich bei allen Beteiligten suchen:

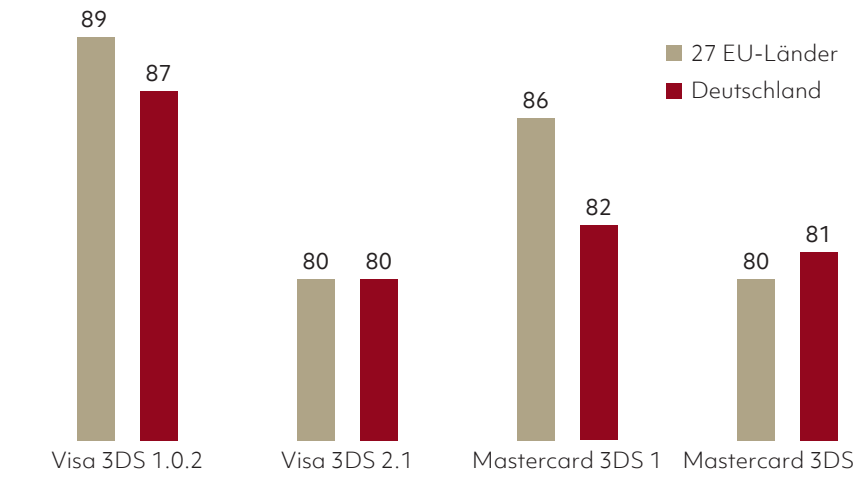
– den Kunden, die vielleicht nicht gut informiert sind und die Abläufe nicht verstehen,

– den Banken, die die neue Transaktions-Risikoanalyse noch nicht im Griff haben, Risiken überschätzen und die Kunden häufiger nach Authentifizierung fragen, als es tatsächlich erforderlich wäre, oder auch

– bei den Händlern, die nicht genug Daten übergeben, damit die Risikoanalyse der Bank funktioniert.

Ganz trivial zu lösen wird das Problem nicht sein. Die Kundeninformation scheint auf den ersten Blick am einfachsten zu sein. Wenn der Kunde weiß, wie es funktioniert, und alle Passwörter im Kopf hat, wäre der größte Teil der Schwierigkeiten behoben. So einfach

Abbildung 1: Bei 3D-Secure 2 holt Deutschland gegenüber dem Rest der EU auf



Erfolgsquote der Authentifizierung im Mai 2021, in Prozent

Quelle: Computop

sich das anhört, so sehr dürfte es pure Theorie bleiben.

Nur mit der Information allein ist es dazu allerdings nicht getan. Sondern Banken und Händler müssen es dem Kunden auch so einfach wie möglich machen. Wenn er etwa das 3D-Secure-Passwort seiner Kreditkarte vergessen hat, dann wäre es hilfreich, die Transaktion nicht einfach scheitern zu lassen, sondern dem Kunden eine andere Möglichkeit einzuräumen, sich zu authentifizieren, etwa indem man nach dem Namen der ersten besuchten Schule, des ersten Tanzpartners oder auch der Telefonnummer der besten Freundin fragt. All das lässt sich vorab hinterlegen, der Fantasie sind keine Grenzen gesetzt. Auch wenn es die Payment-Branche vermutlich nicht mehr hören kann: Hier lässt sich von Paypal einiges abschauen.

Nachbesserungsbedarf auf Emittentenseite

Die Merkbarkeit von Passwörtern ließe sich darüber hinaus erhöhen, wenn man sich auf einheitliche Anforderungen an dieselben einigen und beispielsweise alle Sonderzeichen akzeptieren würde, anstatt mal den Schrägstrich, mal das Ausrufezeichen und ein andermal das Fragezeichen auszuschließen. Denn wenn der Kunde seine Passwörter zusammenstellen kann, wie er möchte, dann fällt es ihm naturgemäß leichter, sie zu behalten. Aus eben diesem Grund wurde ja auch die Wunsch-PIN für Bankkarten eingeführt. Natürlich steigt mit mehr Einheitlichkeit bei den Anforderungen auch das Risiko, dass Kunden mit Karten verschiedener Anbieter immer das gleiche Passwort verwenden. Ganz ausschließen lassen wird sich das jedoch ohnehin nicht.

Nachbessern könnte die Emittentenseite auch beim Heranziehen der genutzten Hardware für die Authentifikation des Kunden. Warum sollte, was für ein Google-Konto funktioniert, nicht auch bei der Authentifikation für eine Payment-Transaktion beziehungsweise der Transaktionsrisikoanalyse helfen können? Und bei der Nutzung biometrischer Verfahren werden die Potenziale schon gar nicht sinnvoll genutzt.

N26 und VR-Banken performen am besten

Für den Handlungsbedarf aufseiten der Banken sprechen die Auswertungen nach Banken beziehungsweise Bankengruppen. Denn sie zeigen: Die Performance der Banken und mit ihr auch die Konversion ist höchst unterschiedlich. Gleiches gilt auch für die User Experience und den Support bei Payment-Problemen.

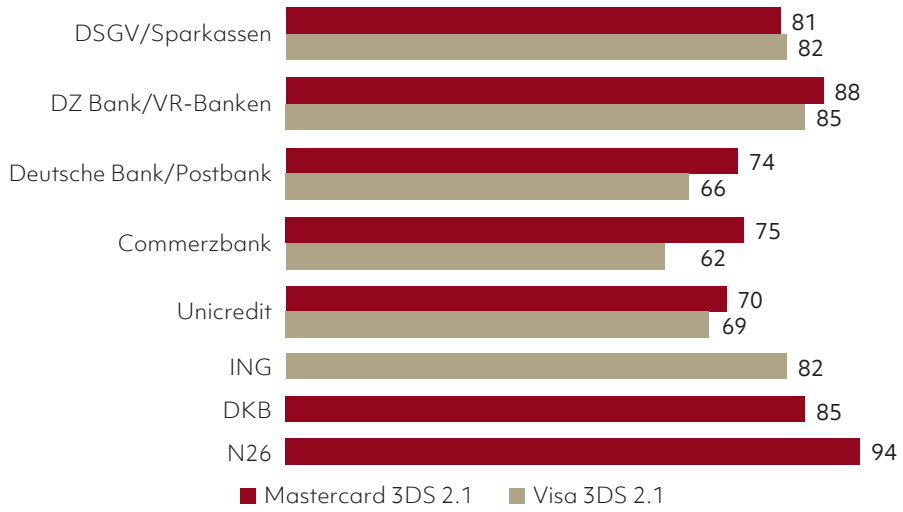
Am besten performt N26 mit 94 Prozent Erfolgsquote bei Mastercard 3DS 2.1 (Visa-Karten emittiert die Neobank nicht). Auf Platz zwei folgen die Genossenschaftsbanken mit einem Anteil von 88 (Mastercard) beziehungsweise 85 (Visa) Prozent erfolgreichen Authentifizierungen mit 3D-Secure 2.1. Auch die Sparkassen landen bei beiden Schemes bei Erfolgsquoten oberhalb von 80 Prozent. Ziemlich schlecht sieht es hingegen bei den Großbanken aus. Sowohl Commerzbank als auch Deutsche Bank und Postbank sowie Unicredit kommen bei Mastercard nicht über 75 Prozent hinaus, bei Visa-Transaktionen sieht es noch schlechter aus.

Delegated Authentification als „Bypass" für den Handel

Auf Händlerseite ist klar: Je mehr Daten der Händler übergibt, umso mehr verbessert sich die Transaktionsrisiko-Analyse der Banken und umso eher kann die Bank auf die Authentifizierung des Käufers verzichten. Auch das hört sich allerdings einfacher an, als es in vielen Fällen umzusetzen sein dürfte. Denn das Ausfüllen aller möglichen Datenfelder setzt eine Verknüpfung der verschiedenen Systeme voraus – immer unter strengster Beachtung des Datenschutzes. Wie lange ein Kunde bereits Kunde des Shops ist, wie seine Bestellhistorie aussieht oder welche Endgeräte und welchen Browser er für seine Bestellung nutzt – diese Daten liegen im Kassensystem der virtuellen Ladenkasse im Checkout-Prozess vielleicht gar nicht vor. Unter Umständen müssten dann erst verschiedene IT-Partner eingebunden werden, um all diese Daten liefern zu können.

Dem Handel bleibt allerdings die Option der Delegated Authentification mit Biometrie – sowohl beim Login ins Händlerkonto als auch für 3D-Secure. Noch wird das wenig genutzt. Wenn die Banken nicht nachbessern, könnte sich das allerdings bald ändern. Schließlich bietet sich dem Handel hier die Chance, die für hohe Konversionsraten so wichtige Nutzererfahrung bei hohem Sicherheitsniveau zu verbessern, ohne damit auf die Bankenseite warten zu müssen. Die Delegated Authentification könnte dann gewissermaßen zum „Bypass" werden. Aber auch Wallets wie Click to Pay mit Geräteerkennung können die Zahlungsabwicklung trotz PSD2 wieder komfortabler machen. ■

Abbildung 2: Direktbanken und die Verbünde haben ihre Hausaufgaben gemacht



Erfolgsquoten der Authentifizierung nach Banken(gruppen) im Mai 2021 für Mastercard 3DS 2.1 und Visa 3DS 2.1, in Prozent

Quelle: Computop