EU-Bankenaufsicht verliert den Verbraucher aus den Augen

Von Sebastian Schulz

Mit den technischen Regulierungsstandards, die die EBA zur Umsetzung der PSD2 entwickelt hat, werden Bezahlverfahren in unangemessener Weise verkompliziert, warnt Sebastian Schulz. Nicht nur seien die Regulatoren den Nachweis schuldig geblieben, dass überhaupt ein Regelungsbedarf besteht. Sondern die EBA konzentriere sich zudem in engstirniger Weise allein auf die starke Kundenorientierung und lasse Ausnahmen, die sich am Risikoniveau orientieren, außer Acht. Für den Versandhandel ist das fatal, so Schulz. Denn hier werden allzu aufwendige Checkout-Verfahren regelmäßig durch Kaufabbrüche bestraft – siehe 3-D-Secure. Vorzugswürdig sei deshalb ein risikobasierter Ansatz, in dessen Rahmen Handel und PSP auf Erfahrungswerte und Algorithmen gestützte Sicherheitsabwägungen treffen. Red.

Neben der Schaffung einer europaweit einheitlichen Rechtsgrundlage für Online-Zahlungen und der Gewähr des Zugangs für Zahlungsdienstleistungen Dritter soll die im Januar 2016 in Kraft getretene PSD2 vor allem für eines sorgen: Mehr Sicherheit im Online-Payment. Elektronisch angebotene Zahlungsdienste sollen sicher abgewickelt werden, „wobei Technologien einzusetzen sind, die eine sichere Authentifizierung des Nutzers gewährleisten und das Betrugsrisiko möglichst weitgehend einschränken können."

Jedenfalls bei den in der Praxis relevanten Vorgängen, etwa dem Zugriff auf ein Zahlungskonto oder der Auslösung eines elektronischen Zahlungsvorgangs, versteht der Richtliniengeber unter einer „sicheren" stets eine „starke" Kundenauthentifizierung" (Stichwort: „2 aus 3").

EBA-Entwurf: aus Angemessenheit wird Regelversessenheit

Technische Regulierungsstandards (RTS) zum Leitbild der starken Kundenauthentifizierung (SCA) sollen gemäß Artikel 98 der Richtlinie durch die Europäische Bankenaufsicht (EBA) erarbeitet werden. Im Rahmen dieses delegierten Rechtsaktes sind sowohl die „Erfordernisse des Verfahrens zur starken Kundenauthentifizierung" als auch „Ausnahmen von der Anwendung" festzulegen. Wohlgemerkt: Das Mandat der EBA erstreckt sich ausdrücklich auch auf die Definition solcher Szenarien, in denen abweichend vom Grundsatz eine starke Kundenauthentifizierung gerade nicht erforderlich ist.

Vor diesem Hintergrund kommt das durch die EBA im August 2016 vorgelegte Consultation Paper – vorsichtig ausgedrückt – etwas eingleisig daher. Anders als durch die PSD2 vorgegeben, finden sich darin ausschließlich Vorgaben zur Implementierung und Umsetzung einer starken Kundenauthentifizierung, nicht aber Ausführungen zu Ausnahmen vom Grundsatz (von der Ausnahme für Kleinstbeträge einmal abgesehen).

Würden die Vorschläge der Londoner Beamten am Ende tatsächlich Gesetz, bedeutete dies damit nichts anderes als eine Zäsur im Paymentsektor. Dynamische („targeted") Authentifizierungsverfahren, orientiert am tatsächlichen Transaktionsrisiko, gehörten der Vergangenheit an. Die Komplexität eines jeden Bezahlprozesses würde signifikant erhöht. Aus Angemessenheit würde Regelversessenheit.

Payment von hoher Relevanz für den Online-Handel

Um zu verstehen, welchen massiven Impact derartige Pläne auf den E-Commerce hätten, muss man sich nur die Relevanz

Zum Autor

Sebastian Schulz, Leiter Rechtspolitik und Datenschutz, Bundesverband E-Commerce und Versandhandel Deutschland e.V. (bevh), Berlin

des Themas „Payment" im Online-Handel im Allgemeinen vor Augen führen.

Die klassische Handelslehre unterscheidet zwischen drei „Strömen" im Handel: Dem Informationsstrom, dem Warenstrom und dem Strom der Nominalgüter – dem Geldfluss. „Kassieren" ist eine Kernkompetenz, wie man an der deutlichen Gewichtung in der Ausbildung der Verkäufer und Kaufleute im Einzelhandel erkennen kann. Auch im E-Commerce gibt es die „Kassenzone", den Checkout, als wichtigen Bestandteil im Kaufprozess.

Im Checkout bleiben viele Warenkörbe stecken. Warum? Der Kunde hat Bedenken. Bedenken über den Preis – denn den Gesamtpreis sieht er hier schon, bevor die imaginäre Kassiererin die einzelnen Produkte abgescannt hat. Bedenken wegen des Aufwands, eine Vielzahl von Informationen ein- und von sich preisgeben zu müssen. Und – es geht ums Geld! – freilich auch Bedenken wegen der (Daten-) Sicherheit.

Sicherheit ist nicht nur ein Bedürfnis auf Kundenseite

Sicherheit ist dabei aber längst nicht allein ein Bedürfnis auf Kundenseite. Das Anbieten sicherer Zahlungsmethoden ist eine von drei zentralen Herausforderungen, denen sich Online-Händler tagtäglich stellen müssen.

- Zum einen besteht die Aufgabe darin, die Zahlung so einfach wie möglich zu machen. Jeder Zwischenschritt an der virtuellen Kasse erhöht nachweislich die Wahrscheinlichkeit, dass der Kunde den Einkauf abbricht.

- Andererseits muss der Händler aus ureigenem Interesse heraus Zahlverfahren anbieten, die das Risiko des eigenen Zahlungsausfalls minimieren. Neue Dienstleister wie optile.net fungieren hier als intelligente Aggregatoren, die bei jedem einzelnen Kauf aufgrund des Kundenverhaltens und des Warenkorbes passende Zahlverfahren sogar von unterschiedlichen Payment-Dienstleistern vorschlagen.

- Das Thema Zahlungssicherheit ist Nummer Drei. Unternehmen, die wiederholt Datenklau, Betrug oder Identitätsmissbrauch Tür und Tor öffnen, sind weg vom Fenster.

All das unterstreicht: Beim Payment muss der Online-Händler akribisch arbeiten. Schon eine Umstellung der Reihenfolge von Abfragen im Checkout-Prozess kann zu einer Verbesserung der Konversionsrate oder umgekehrt zum Abschmelzen wertvoller Marktanteile führen.

Zeit ist Geld – gerade im E-Commerce

Studien belegen, was aus Einzelbeispielen lange bekannt ist: Der Kunde belohnt Händler, die ihm das Einkaufen auf jeglichem Kanal so einfach wie möglich machen. Das Modeunternehmen Engelhorn etwa hat in einem Test festgestellt, dass das Angebot nur eines weiteren digitalen Bezahlverfahrens die Zahl der Conversions im Checkout signifikant erhöht hat und in kürzester Zeit bei fast jedem dritten Kauf eingesetzt wurde.

Eine Analyse zeigte, dass der Checkout-Prozess sich für den Kunden von über zwei Minuten auf lediglich 30 Sekunden verkürzte. Zeit ist Geld, auch und gerade im E-Commerce.

Fast durchweg negative Erfahrungen mit 3-D-Secure

Umgekehrt haben die Händler mit dem 3-D-Secure-Verfahren faktisch ohne Ausnahme überaus negative Erfahrungen gemacht. Die Umleitung auf eine externe Seite mit separater Verifikation über ein weiteres Passwort erhöhte die Kaufabbrüche deutlich.

Seit der Einführung 2009 hat sich die negative Auswirkung zwar durch Verfahrensänderungen abmildern lassen. Dennoch haben in der gleichen Zeit die „einfachen sicheren" Zahlverfahren so deutlich zugelegt, dass im Jahr 2016 erstmals im E-Commerce die Online-Lastschrift sogar den Rechnungskauf überholte und mit 30 Prozent die am häufigsten genutzte Zahlweise war. Während im gleichen Zeitraum nach Erhebung des bevh der Kauf per Kreditkarte von 17 auf 15 Prozent zurückfiel, erhöhte sich der Anteil der digitalen Zahlverfahren von 19 auf 22 Prozent.

Nun mag man einwenden, die hier aufgezeigten wirtschaftlichen Implikationen müssten angesichts des übergeordneten Ziels eines Mehr an Rechtssicherheit zurückstehen. Und noch einmal: Die Bedeutung von größtmöglicher Sicherheit bei Zahlungsvorgängen steht außer Frage. Eine obligatorische starke Kundenauthentifizierung mag auch grundsätzlich als geeignet erscheinen, dieses Ziel zu erreichen.

Regelungsbedürfnis nicht nachgewiesen

Rechtliche Vorgaben müssen jedoch nicht nur geeignet, sondern vielmehr auch verhältnismäßig sein. Eine Übergewichtung des einen Ziels zulasten anderer, im Zweifel auch kollidierender Ziele, ist zu vermeiden.

An dieser Stelle bleiben sowohl EU-Kommission als auch EBA bereits den Nachweis schuldig, dass überhaupt ein vom geltenden Recht abweichendes Regelungsbedürfnis besteht. Freilich verwundert

Beilagenhinweis

Dieser Ausgabe liegt das **Sachregister 2016** von **cards Karten cartes** bei.

das am Ende nicht, bleibt doch die viel bemühte Fraud-Rate im Verhältnis zu den exponentiell anwachsenden Transaktionsvolumen im E-Commerce vergleichsweise gering.

Die Kriterien der durch die EBA (zwingend!) vorzunehmenden Verhältnismäßigkeitsprüfung werden durch die PSD2 übrigens sogar detailliert vorgegeben. So heißt es beispielsweise in den Absätzen 2 und 3 von Artikel 98, dass „benutzerfreundliche, allgemein zugängliche und innovative Zahlungsmittel" ermöglicht bleiben sollen. Ausnahmen vom Grundsatz einer SCA sollen sich an dem mit der Dienstleistung verbundenen Risikoniveau orientieren. Welcher Raum für Innovationen bleibt aber bei einer sakrosankten Fokussierung auf die starke Kundenauthentifizierung?

Bezahlverfahren werden in unangemessener Weise verkompliziert

Festzuhalten bleibt: Mit den bislang bekannt gewordenen Vorschlägen für Regulatory Technical Standards und der Abwesenheit von Ausnahmen vom Grundsatz der starken Kundenauthentifizierung verkompliziert die EBA Bezahlverfahren in einer für den E-Commerce inakzeptablen Weise. Mögen einzelne PSPs den gemachten Vorschlägen Positives abgewinnen, im Interesse der Verbraucher sind diese nicht.

Vorzugswürdig ist und bleibt ein risikobasierter Ansatz, im Rahmen dessen Handel und PSP auf Erfahrungswerte und Algorithmen gestützte Sicherheitsabwägungen treffen und so dem Kunden, das heißt uns allen, weiterhin ein gleichermaßen sicheres wie nutzerfreundliches Einkaufserlebnis ermöglichen können. Die EBA ist aufgerufen, im weiteren Verfahren ihre Engstirnigkeit zulasten der Verbraucher wie auch der europäischen E-Commerce-Wirtschaft aufzugeben.

Hinweis: Der überarbeitete Entwurf der EBA lag zum Redaktionsschluss noch nicht vor.