Stellungnahme

Berlin, 04. Januar 2017

Stellungnahme zum Gesetz zur Umsetzung der aufsichtsrechtlichen Vorschriften der Zweiten Zahlungsdiensterichtlinie (Zahlungsdiensteumsetzungsgesetz – ZDUG)

Berlin – Der Händlerbund e.V. kritisiert das Zahlungsdiensteumsetzungsgesetz (ZDUG) und die Payment Services Directive (PSD2) Richtlinie 2015/2366/EU, die zum jetzigen Zeitpunkt eine uneingeschränkte Einführung einer zwei-Faktor Authentifizierung (Starke Kundenauthentifizierung) für alle Online-Zahlungen ab 2018 vorsieht. Der Händlerbund e.V. unterstützt grundsätzlich die Pläne der EU-Kommission und des Bundesministeriums der Finanzen, Kunden bei Online-Zahlungen stärker schützen zu wollen, warnt jedoch vor den verheerenden Folgen auf die Wettbewerbsfähigkeit des deutschen Onlinehandels im Falle einer Einführung von starker Kundenauthentifizierung (SKA). Eine zwei-Faktor Authentifizierung ist ein starker Eingriff in den Onlinehandel, der sich oft negativ auf die Conversion-Rate der Händler auswirkt. Der Onlinehandelsverband fordert mehr Flexibilität im Checkout-Prozess. Weiterhin fordert er die Einführung dynamischer Authentifizierungsmaßnahmen, wie gezielte Kundenauthentifizierung und somit die Wahlfreiheit für die Onlinehändler, selbst zu entscheiden, wann SKA anzuwenden sei. Die Mandatierung eines statischen Authentifizierungs-Tools wie SKA bedroht die Existenz vieler KMU Onlinehändler, hemmt Innovation in der Payment Branche und trägt nicht effektiv zur Betrugsprävention bei.

1. Starke Kundenauthentifizierung bedroht den KMU Onlinehandel

Der Händlerbund e.V. unterstützt die Pläne der EU-Kommission, Kunden bei Online-Zahlungen stärker zu schützen und Betrug im Zahlungsverkehr zu bekämpfen. Nur eine sichere Zahlungslandschaft ermöglicht auch einen prosperierenden und grenzüberschreitenden Online-Handel in Deutschland und Europa.

Titel 6, § 56 des Zahlungsdiensteumsetzungsgesetz sieht eine Einführung einer zwei-Faktor Authentifizierung, auch Starke Authentifizierung (SKA) genannt, für alle Zahlungen im Internet, inklusive für die sogenannten Zahlungsauslösedienste und Kontoinformationsdienstleister ab dem 13. Januar 2018 vor. Die zwei-Faktor Authentifizierung erfordert mindestens zwei Elemente der Kategorie Wissen (Passwort, PIN), Besitz (e-Tokens, Kreditkarte, One-Time-Passwörter OTPs) und Inhärenz (Biometrische Merkmale). Zudem darf eines der oben genannten Elemente nicht wiederverwendbar sein. Eine starke Kundenauthentifizierung ist somit vor allem für den Onlinehandel ein drastischer Einschnitt im Checkout-Prozess, da Kunden

mehr Zeit verbringen müssen sich zu authentifizieren, was einen erhöhten Kaufabbruch zur Folge hat.

Der Händlerbund e.V. verweist in diesem Zusammenhang auf die gemeinsame Clever Advice Studie „Recommendations for improving European online payments regulation“[1] die beweist, dass die Abbruchrate von Kunden im Checkout-Prozess erheblich höher ist, wenn Kunden sich zweifach authentifizieren müssen. Nach Einführung des 3-D-Secure Verfahrens, ein zwei-Faktor Authentifizierungsverfahren für Kartentransaktionen, gab es einen Rückgang der Conversion-Rate von bis 23% im deutschen Onlinehandel. So hat in Deutschland fast jeder 3. Kunde einen Kauf aufgrund komplizierter Zahlungsverfahren abgebrochen. In einigen Ländern wie den USA oder Brasilien liegt die Steigerung der Kaufabbrüche im Onlinehandel sogar bei 65%. Durch die erhebliche Beeinträchtigung der Nutzerfreundlichkeit ist eine ähnliche Entwicklung bei einer uneingeschränkten Einführung der SKA im Onlinehandel zu erwarten. Gerade kleine und mittelständische Onlineshops, die einen besonders hohen Stellenwert auf die Customer-Journey bzw. eine nahtlose Kauferfahrung als Wettbewerbsvorteil legen, sind von dieser Entwicklung bedroht.

2. Keine verbesserte Sicherheit durch starke Kundenauthentifizierung

Ein einheitliches Authentifizierungsverfahren zu mandatieren, welches weder dynamisch agiert noch andere Faktoren wie das Einkaufsverhalten (Stammkunden vs. Neukunden, Adress- & Rechnungswechsel, Standort und Kunden-Endgeräte) einbezieht, garantiert keine verbesserte Sicherheit. Im Gegenteil – eine statische Authentifizierungsmethode bietet Betrügern im Zahlungsverkehr die Möglichkeit, mit Hilfe von Phising-Mails und Ähnlichem ihre Vorgehensweisen schneller anzupassen.

Starke Kundenauthentifizierung ist eine standardisierte und statische Einheitslösung die das dynamisches Problem des Zahlungsbetruges einschränken soll. Starke Kundenauthentifizierung verhindert jedoch nicht den Identitätsmissbrauch, falls Betrüger im Besitz beider Verifizierungselemente sind, selbst wenn diese unabhängig voneinander sind. Im Gegenzug bietet eine gezielte Kundenauthentifizierung ein real-time Monitoring des Kaufprozesses und somit einen kontinuierlichen Schutz vor Missbrauch im Zahlungsverkehr, da die Kunden in ständiger Interaktion mit dem Onlineshop sind. So kann zum Beispiel aufgrund stark abweichender Standorte oder Endgeräte der Kunden ein risiko-basierter Ansatz eine zweite, stärkere Authentifizierung im Checkout-Prozess veranlassen.

[1] Clever Advice. *Recommendations for improving European online payments regulation*. Supported by Ecommerce Europe. August 2016. Milan, Italy. https://www.ecommerce-europe.eu/app/uploads/2016/09/Suggestions-to-improve-European-Online-Payments-Regulation.pdf

Der Händlerbund e.V. verweist ausdrücklich auf die Studienergebnisse von Clever Advice und stellt klar, dass dynamische Authentifizierungsmaßnahmen, wie Risikomanagement und gezielte Authentifizierung (Targeted Authentication-TA), bessere, ausgewogenere und sicherere Alternativen zu einer starken Kundenauthentifizierung bieten. So ist laut Studie die Betrugsrate in England nach Einführung von TA-Maßnahmen nicht gestiegen, jedoch waren die Kaufabbrüche im Onlinehandel um bis zu 70% rückläufig. Durch die Reduzierung des Checkout-Prozesses von 50 auf 10 Sekunden und das transparente Kauferlebnis profitierten sowohl Verbraucher als auch die Onlinehändler.

Da das ZDUG sowie die EBA eine Einheitslösung zum Risikomanagement mit einem umständlichen Authentifizierungsprozess anstreben, besteht für die Händler jedoch kein Raum zur Risikobewertung von Onlinetransaktionen. Zahlungsdienstleister sollten deshalb die Möglichkeit haben, in Verbindung mit starke Authentifizierung auch alternative Authentifizierungs- und Verifizierungsverfahren anzubieten. Targeted Authentication bietet im selben Maß Betrugsprävention, wie starke Kundenauthentifizierung, ohne, dass die Nutzerfreundlichkeit beeinträchtigt wird.

3. Innovation in der Payment Branche wird gehemmt

Das wesentliche Ziel laut Gesetzesbegründung „Innovation im Zahlungsverkehr zu fördern,“[2] wird durch das mandatieren eines einheitlichen Authentifizierungsverfahren klar verfehlt. Eine uneingeschränkte Einführung eines einheitlichen und statischen Authentifizierungs-Tools hemmt das Innovationspotential der europäischen Payment Branche und ist im Hinblick auf die Gesetzgebung nicht technologie-neutral. Starke Kundenauthentifizierung ist eine standardisierte Einheitslösung und verhindert somit die Entwicklung neuer, dynamischer und risikobasierter Ansätze. Ein Level-Playing Field und ein innovationsfreundliches Klima ist nur möglich, wenn alle Marktakteure, sowohl Zahlungsdienstleister als auch Händler die Möglichkeit haben, neue Geschäftsmodelle zu entwickeln. Die voranschreitende Digitalisierung der Payment Branche bietet mit Hilfe von Data Analytics und Big-Data Anwendungen enormes Entwicklungspotential in Betrugsprävention, was nun durch das mandatieren von SKA verloren geht.

[2]Bundesministerium der Finanzen. *Entwurf eines Gesetzes zur Umsetzung der aufsichtsrechtlichen Vorschriften der Zweiten Zahlungsdiensterichtlinie.* 21.12.2016. Accessed on 03.01.2017. http://www.bundesfinanzministerium.de/Content/DE/Gesetzestexte/Referentenentwuerfe/2016-12-21-Zahlungsdiensteumsetzungsgesetz.html Seite 73.

Stellungnahme

Berlin, 04. Januar 2017

Kritisch zu betrachten ist auch die Übersicht zum Erfüllungsaufwand der Wirtschaft im Gesetzentwurf. Die Übersicht beziffert zwar die Kosten der Umsetzung und Wartung von Zahlungsdienstleistern sowie Kreditinstituten und Banken, lässt jedoch die Kosten der Onlinehändler für die Integration der neuen Dienste außen vor. Die Anpassung der Schnittstellen im Onlineshop sowie das Bereitstellen alternativer Zahlungsmöglichkeiten bei einer abgelehnten Authentifizierung werden nicht benannt. Da eine starke Kundenauthentifizierung einen drastischen Einschnitt im Checkout-Prozess des Onlinehandels darstellt, fehlt eine Kostenfolgenabschätzung der gesamten Branche. Es ist mit enormen Umsatzeinbußen durch hohe Abbruchraten zu rechnen.

Über den Händlerbund e.V.
Als größter Onlinehandelsverband Europas ist der Händlerbund Sprachrohr und Partner der E-Commerce-Branche. Der Verband fördert den Austausch zwischen Händlern und Dienstleistern, um den digitalen als auch stationären Handel nachhaltig zu unterstützen und zukunftsfähig auszurichten. Durch die europaweite Interessenvertretung und Bündelung verschiedener Dienstleistungen gestaltet der Händlerbund mit seinen Mitgliedern und Partnern aktiv die Branche.

Ihr Ansprechpartner:
Florian Seikel, Hauptgeschäftsführer florian.seikel@haendlerbund.de
Chris Berger, Referent Public Affairs chris.berger@haendlerbund.de

Händlerbund e.V.,
Potsdamer Straße 7 I Potsdamer Platz,
10785 Berlin