

HDE-Position zur starken Kundenauthentifizierung

Vorbemerkungen

Der HDE setzt sich grundsätzlich für Maßnahmen zur Steigerung des Verbraucherschutzes bei Online-Einkäufen und Einkäufen am Point of Sale ein. Das Vertrauen in die Sicherheit von Zahlungsverfahren ist dabei eine wesentliche Grundlage für den langfristigen Erfolg insbesondere im E-Commerce und Voraussetzung für den Einsatz moderner Zahlungsmittel am PoS.

Gleichzeitig ist jedoch eine praktikable Handhabung der Prozesse beim Onlinekauf ein wesentliches Kriterium für den Erfolg des E-Commerce. Ist der Einkauf zu kompliziert, erfolgen Kaufabbrüche. Dies gilt insbesondere für den Checkout-Prozess und für die Wahl der Zahlungsart. Am PoS ist ebenso eine praktikable Handhabung neuer, insbesondere mobiler Zahlungsverfahren essentiell für die Akzeptanz beim Kunden. Hier ist Convenience und vor allem Schnelligkeit gefragt. Prozesse müssen sich zunehmend in den Einkaufsprozess integrieren (Seamless Payment), um ein modernes und zeitgemäßes Einkaufen zu ermöglichen.

Die gebräuchlichsten Zahlungsarten im Internet sind neben der Kreditkarte der Kauf auf Rechnung, die Lastschrift sowie geschlossene Zahlungsplattformen. Wesentliches gemeinsames Kriterium dieser Zahlungsarten ist die bislang aus Kundensicht einfache Handhabung. Stark gesicherte Varianten der Systeme (z.B. Secure 3D bzw. Verified by Visa) werden kaum genutzt.

Am PoS dominiert Barzahlung, insbesondere bei Kleinbetragszahlungen. Bei Kartenzahlungen ist das deutsche Girocard-Verfahren das gebräuchlichste Zahlungsmittel, gefolgt von dem Lastschriftverfahren auf Basis der EC-Karte. Auch hier dominiert die aus Kundensicht einfache Handhabung die Entscheidung für die Systeme. Kontaktlose Zahlungsarten und Mobile Payment werden absehbar einen steigenden Anteil verzeichnen und kontaktbehafte Zahlungen ablösen. Dies kann nur dann geschehen, wenn die Handhabung mindestens genauso problemlos erfolgen kann.

Gesetzliche Vorgaben zur Sicherheit von Zahlungssystemen können sich direkt auf die Akzeptanz der entsprechenden Systeme auswirken, wenn für den Kunden zusätzliche Prozessschritte erforderlich werden bzw. die Handhabung komplexer wird. Dabei sind Marktverschiebungen zu bestimmten Zahlungsarten denkbar, wenn für diese vereinfachte Vorgaben gelten. Auch können Verbraucher vom Onlinekauf abgehalten werden und andere Einkaufskanäle nutzen, wenn die Anforderungen zu komplex erscheinen. Am PoS werden innovative Zahlungsarten keinen Erfolg haben, wenn die Anwendung durch regulatorische Vorgaben komplexer ist als bei den bestehenden Verfahren.

Aufgabe des Gesetzgebers ist daher, eine Ausgewogenheit zwischen Verbraucherschutz und Handhabbarkeit der Systeme herzustellen. Es müssen Rahmenbedingungen gefunden werden, die die Gestaltung effizienter Zahlungsarten nicht verhindert. Dabei müssen Kunden vor Zahlungsrisiken geschützt werden, ohne dass unnötige Hürden aufgebaut werden, die einen Einsatz der Zahlungsarten verhindern. Professionelle Marktakteure wie Kreditwirtschaft und Handel benötigen vor allem kalkulierbare Prozesse. Dabei ist ein gewisses Zahlungsausfallrisiko durchaus hinnehmbar, wie das durch den Handel entwickelte Lastschriftverfahren zeigt. Auch etablierte Kartenzahlungen der Kreditwirtschaft werden durch ein ausgefeiltes Risikomanagement praktikabel gehalten und liefern einen Beitrag im Zahlungsmix des Handels.

**Handelsverband
Deutschland (HDE) e.V.**
Am Weidendamm 1A
10117 Berlin

www.einzelhandel.de

Kontakt

Ulrich Binnebössel
T +49 30 726250-62
F +49 30 726251-88
binneboessel@hde.de

Betrachtung des Zahlungsrisikos

Aus Sicht der Verbraucher ist die Nutzung elektronischer Zahlungsmittel streng mit dem Risikoniveau verbunden. Zahlungsarten mit einem hohen Verlustrisiko würden nicht akzeptiert. Die Zahlungsdiensterichtlinie trägt diesem Umstand Rechnung und begrenzt das Haftungsrisiko des Zahlers für nicht autorisierte Zahlungen nach Artikel 74 auf künftig 50 Euro.

Aus Sicht der kontoführenden Institute ist die Kalkulierbarkeit der eigenen Haftung von entscheidender Bedeutung. Einerseits ist ein Herausgeber von Zahlungsinstrumenten an deren Einsatz interessiert. Im eigenen Interesse muss daher die Komplexität des Einsatzes des Instrumentes für den Zahler möglichst niedrig sein. Andererseits darf durch einen eventuellen Missbrauch das Verlustrisiko insgesamt nicht höher liegen als die erwarteten Gewinne aus dem Verfahren. Um einen Ausgleich zwischen der Praktikabilität des Zahlungsinstrumentes und dem Verlustrisiko herzustellen, bedienen sich die Institute verschiedenster Techniken. Dabei ist die Absicherung der Autorisierung einer Zahlung nur ein Mittel und wird ergänzt mit weiteren Maßnahmen zur Risikoeinschätzung und -vorsorge. Um das Ziel der Beaufsichtigung und Begrenzung von Risiken für Zahlungsdienstleister zu erreichen, können Regulierungen zur Analyse und Vermeidung von Risiken für Zahlungsdienstleister ausreichen, die sich nicht auf den Kunden auswirken. Die Vorgaben der SecurePay-Empfehlung und die deutsche Umsetzung im BaFin-Merkblatt liefern hier bereits gute Ansätze (Verantwortlichkeiten, Risikoanalyse, Berichtswesen). Auch Vorgaben zur Information von Kunden sind enthalten. Insgesamt ergibt sich bei heutigen Zahlungsinstrumenten bereits ohne starke Authentifizierung ein praktikabler Weg, um das Verlustrisiko auf Institutsseite zu begrenzen.

Aus Sicht des Handels ergibt sich eine ähnliche Betrachtung eines kalkulierbaren Risikos in Abwägung mit möglichst niedrigen Einsatzhürden. Ein zu 100 Prozent sicheres Zahlungsinstrument ist dann wertlos, wenn es in der Praxis am PoS oder im Onlineshop vom Zahler nicht eingesetzt wird. Ein extrem risikoreiches Zahlungsinstrument ist dann wertlos, wenn es vom Handel wegen Unkalkulierbarkeit nicht angeboten werden kann. Insbesondere im stationären Handel (PoS) hat sich gezeigt, dass die etablierten Prozesse der Risikokalkulation und der Autorisierungssysteme praktikabel sind und den Bedürfnissen der Beteiligten entsprechen. Das in Deutschland weit verbreitete Lastschriftverfahren dient hier als gutes Beispiel. Im E-Commerce müssen dagegen weitere Anstrengungen erfolgen, um ein für alle Akteure akzeptiertes und effizient einsetzbares Zahlungsinstrument zu entwickeln.

Aufgabe für eine Regulierung der technischen Standards ist es daher, einen Mittelweg aus Risikoprävention und Praktikabilität zu schaffen.

Forderung aus Handelssicht

Die EBA ist aufgerufen, die Vorgaben für eine starke Authentifizierung nach Artikel 97 der Zahlungsdiensterichtlinie 2 umzusetzen. Dabei ergeben sich nach Artikel 98 (1)b und 98 (3) Möglichkeiten der Definition von Ausnahmen aus dem Anwendungsbereich der starken Authentifizierung. Dabei ist u.E. insbesondere Artikel 98 (3) a von Bedeutung. Danach kann die EBA ein „mit der Dienstleistung verbundenes Risikoniveau“ berücksichtigen, um bestimmte elektronische Zahlungen von der Anwendung der starken Authentifizierung auszunehmen.

Der HDE setzt sich daher dafür ein, diese Option möglichst weitreichend zu nutzen. Elektronische Zahlungen am PoS sollten daher aufgrund des geringen Risikoniveaus generell ausgenommen werden. Es gibt etablierte Prozesse und Routinen, die das Risiko sowohl für Zahler und Zahlungsempfänger als auch für Zahlungsinstitute überschaubar und vor allem beherrschbar machen. Elektronische Zahlungen sollten hier den gleichen Anforderungen unterliegen wie etablierte Verfahren, um gleichberechtigte Chancen am Markt zu bekommen.

Für den Bereich des E-Commerce setzt sich der HDE dafür ein, entsprechende Standards zu schaffen, die sowohl vom Zahler akzeptiert werden, als auch dem Zahlungsempfänger eine kalkulierbare Grundlage schaffen. Zahlungsinstitute sollten in die Lage versetzt werden, die Haftungsrisiken möglichst auf der Grundlage von Vorgaben für das Risikomanagement abzuwägen. Dabei gilt auch hier, dass Transaktionen mit einem kalkulierbaren Risikoniveau aus der Betrachtung ausgenommen werden.

Es ist aus Handelssicht nicht zielführend, die starke Authentifizierung für Transaktionen im Konsumgüterhandel für alle elektronischen Zahlungen zum Standardfall zu erklären. Erst mit der Entwicklung und Marktdurchdringung einer von den Zahlern akzeptierten Lösung, die für den Handel kosteneffizient angeboten werden kann, ist eine derartige Entscheidung tragfähig. Bis dahin sieht der Gesetzgeber die Möglichkeit der Ausnahme derartiger risikoarmer Zahlungen vor.

Fazit

Zahlungsprozesse müssen auch in Zukunft einfach und praktikabel sein, um sich am Markt etablieren zu können. Zudem müssen sie den Anforderungen integrierter Einkaufsprozesse entsprechen. Dies muss auch für elektronische Zahlungen gelten, damit diese eine Chance auf Markterfolg haben. Die EBA sollte bei der Schaffung der regulatorischen technischen Standards diesen Umstand berücksichtigen und Freiräume für die Entwicklung praktischer Zahlungsinstrumente für den Einzelhandel lassen. Die Zahlungsdiensterichtlinie lässt diesen Freiraum und ermöglicht die Definition entsprechender Ausnahmen. Die starke Authentifizierung sollte dabei ausschließlich für Transaktionen mit unkalkulierbar hohem Risikoniveau vorgegeben werden. Alltägliche Transaktionen im Einzelhandel zählen aus Sicht des HDE nicht zu den vom Gesetzgeber gemeinten Fällen. Insbesondere am PoS sieht der HDE keine Notwendigkeit der starken Authentifizierung elektronischer Zahlungen, wenn andere Möglichkeiten der Risikobeherrschung genutzt werden können.

Berlin, Februar 2016

gez. Ulrich Binnebösel