HDE
Handelsverband
Deutschland

Stellungnahme zum Entwurf eines BaFin-Rundschreibens zu Mindestanforderungen an die Sicherheit von Internetzahlungen

19. März 2015

www.einzelhandel.de

I. Vorbemerkungen

Der Handelsverband Deutschland (HDE) bezieht sich in folgenden Ausführungen auf die Anforderungen des Merkblatts mit unmittelbarem Bezug auf den Onlinehandel und seine Kunden. Auf eine detaillierte Einschätzung wird in weiten Teilen verzichtet, da sich das Papier auf Zahlungsdienstleister bezieht.

Der HDE setzt sich grundsätzlich für Maßnahmen zur Steigerung des Verbraucherschutzes bei Online-Einkäufen ein. Das Vertrauen in die Sicherheit von Zahlungsverfahren ist dabei eine wesentliche Grundlage für den langfristigen Erfolg im E-Commerce.

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.

Die gebräuchlichsten Zahlungsarten im Internet sind neben der Kreditkarte der Kauf auf Rechnung, die Lastschrift sowie einige 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.

Gesetzliche Vorgaben zur Sicherheit von Zahlungssystemen können sich direkt auf die Akzeptanz der entsprechenden Systeme auswirken, wenn für den Kunden zusätzliche Prozessschritte erforderlich werden. Dabei sind Marktverschiebungen zu bestimmten Zahlungsarten denkbar, wenn diese vom Anwendungsbereich ausgenommen sind oder vereinfachte Vorgaben erhalten. Auch können Verbraucher vom Onlinekauf abgehalten werden und andere Einkaufskanäle nutzen, wenn die Anforderungen zu komplex erscheinen.

Aufgabe des Gesetzgebers ist daher, eine Ausgewogenheit zwischen Verbraucherschutz und Handhabbarkeit der Systeme herzustellen.

II. Bewertung des Merkblatts

Der HDE bewertet die vorgeschlagenen Maßnahmen des BaFin-Merkblattes als zu weitgehend und lehnt die Umsetzung des Papiers ab. Es sind weitreichende negative Auswirkungen auf den Onlinehandel zu befürchten, die bislang nicht ausreichend analysiert wurden. Eine Ausgewogenheit zwischen den Anforderungen und Auswirkungen der verschiedenen Marktakteure ist nicht erkennbar. Der HDE fordert daher eine umfangreiche Folgeabschätzung der Auswirkungen des Merkblattes auf den Markt bzw. den E-Commerce, bevor Maßnahmen getroffen werden.

Insbesondere die Anforderungen an eine starke Authentisierung können zu weitreichenden Auswirkungen auf den E-Commerce führen. Es können Marktverschiebungen zu Zahlungsarten erfolgen, die von der Anwendung ausgenommen sind oder vereinfachte Anforderungen erfüllen müssen. Damit werden die entsprechenden Zahlungsanbieter in ihrer Marktbedeutung gestärkt. Zudem könnten Kunden ganz von einem Einkauf im Internet absehen, wenn sich der Kaufprozess aufgrund der Vorgaben komplizierter gestaltet. Die Einbeziehung eines zweiten Kanals führt zwangsläufig zu einer komplexeren Gestaltung des Zahlungsprozesses. Der HDE ist daher der Ansicht, dass die Vorgaben zur starken Kundenauthentisierung (Punkt 3.2) gestrichen werden sollten.

Die Kosten der Auswirkungen auf den Onlinehandel lassen sich derzeit nicht seriös einschätzen. In jedem Falle aber sind weitaus höhere Kosten durch Marktverschiebungen oder Umsatzverluste zu erwarten, als sie die BaFin angibt (hier wird lediglich ein Erfüllungsaufwand von 20,3 Mio. Euro und geringe Bürokratiekosten berücksichtigt). Ebenfalls sind voraussichtlich wesentlich höhere Kosten für die Implementierung der Vorgaben auf Handelsseite notwendig als angegeben (z.B. Umgestaltung des Checkout-Prozesses, Kundenaufklärungs-/Informationskosten).

Grundsätzlich muss bezweifelt werden, ob eine Regulierung der technischen Kundenschnittstelle zu den Zahlungsarten überhaupt notwendig ist. 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. Das Merkblatt liefert hier gute Ansätze in Punkt 2 (Verantwortlichkeiten, Risikoanalyse, Berichtswesen). Auch Vorgaben zur Information von Kunden können sinnvoll sein (Punkt 4).

Das BaFin-Merkblatt enthält Mindestanforderungen an Zahlungssysteme im Internet, die auf Basis der Vorgaben der European Banking Authority (EBA) europaweit einheitlich gestaltet werden sollen. In der nationalen Ausprägung zeigen sich allerdings bereits wesentliche Unterschiede in den einzelnen Ländern. So werden Anforderungen teilweise ausgeweitet, oder unterschiedliche Umsetzungsfristen festgelegt. Einige Länder haben die Befassung vorerst ausgesetzt. Der HDE ist daher der Ansicht, dass die Arbeiten an dem Merkblatt vorerst ruhen sollten, bis sich eine europaweit einheitliche Umsetzung abzeichnet.

Das Merkblatt enthält an verschiedenen Stellen Vorgaben, die der Zahlungsdienstleister bei seinem Akzeptanzkunden durchsetzen und kontrollieren muss. Selbstverständlich hat der Dienstleister ein eigenes Interesse, Zahlungsausfall- und Betrugsrisiken zu minimieren und wird Maßnahmen treffen, um die Risiken zu begrenzen. Dabei steht ihm eine Vielzahl an Optionen zur Verfügung, die auch heute bereits eigenverantwortlich genutzt werden (etwa Ausschlussoptionen oder Rückstellungen). Das Merkblatt begrenzt diese Optionen zuungunsten des akzeptierenden Kunden. Die zusätzliche Sicherheit der Zahlungsmittel, die den Zahlungsdienstleistern zugutekommt, erfolgt also weitgehend auf Kosten des akzeptierenden Handels. Daher ist das Merkblatt als unausgewogen einzuschätzen und abzulehnen.

Bereits heute bestehen Industriestandards auf freiwilliger Basis, die von den Zahlungsdienstleistern umzusetzen sind und die Sicherheit von sensiblen Zahlungsdaten stärken sollen. Beispielhaft ist hier der Payment Card Industry-Data Security Standard (PCI-DSS) zu nennen. Eine gesetzliche Regulierung ist vor diesem Hintergrund zu hinterfragen, da sie die Möglichkeiten der Selbstregulierung erheblich einschränkt ohne dass ein unmittelbarer Sicherheitsgewinn für Verbraucher gegenüber den Industriestandards deutlich wird.

In vielen Fällen ist eine Klarstellung notwendig, wie bestimmte Anforderungen (insbesondere Tz 20-30) auszulegen sind, die von der Akzeptanzstelle umzusetzen sind. So können bei enger Auslegung z.B. der Tz 21 in Verbindung mit Tz 31alle IT-Systeme des Onlineshop-Betreibers von den Anforderungen betroffen sein, so auch diejenigen, die nicht in direkter Verbindung mit den Zahlungsdaten stehen. Der HDE fordert eine Konkretisierung der Anforderungen und eine Beschränkung auf Zahlungsdaten speichernde Systeme. Zudem muss klargestellt werden, dass das gebräuchliche Lastschriftverfahren im Internet (ohne Erteilung eines E-Mandats) vom Anwendungsbereich ausgenommen ist, auch wenn Dienstleister in die Prozessabwicklung eingebunden sind.

Grundsätzlich ist allerdings zu bezweifeln, dass die BaFin von Zahlungsdienstleistern die Einhaltung und Kontrolle von IT-Prozessen bei Akzeptanzstellen, die nicht in unmittelbaren Zusammenhang mit Transaktionsdaten stehen, überhaupt einfordern kann, da umfangreiche Regelungen zu Lasten Dritter geschaffen werden. Der HDE fordert daher eine Erläuterung der Zuständigkeit der BaFin in Bezug auf die unmittelbar den akzeptierenden Handel betreffenden Anforderungen.

III. Besondere Anmerkungen

Tz 2: Es sollte klargestellt werden, dass das in Deutschland übliche und im SEPA-Rat abgestimmte Lastschriftverfahren im Internet (ohne E-Mandat) nicht in den Anwendungsbereich fällt. Bei diesem Verfahren wird zwischen Zahler und Zahlungsempfänger über das Internet der Einzug einer Lastschrift vereinbart.

Zahlungsrisiken gehen innerhalb der SEPA-Fristen stets zu Lasten des Zahlungsempfängers. Eine Initiierung der Lastschrift findet erst bei Übertragung der Lastschriftdatei an die ausführende Händlerbank statt. Auch wenn die Hintergrundprozesse über einen Zahlungsdienstleister laufen, um z.B. eine Zahlungsgarantie zu prüfen, sieht der HDE keine Wirksamkeit des Merkblatts und bittet um entsprechende Klarstellung.

Tz 31: Das Merkblatt enthält umfangreiche Verpflichtungen der Zahlungsdienstleister zur Durchsetzung von bestimmten Anforderungen bei Akzeptanzstellen. So werden in den Tz 20-30 umfangreiche Vorgaben zur Gestaltung der IT-Landschaft des Dienstleisters beschrieben. Tz 31 sieht vor, dass auch die Online-Händler in gleicher Weise den Anforderungen genügen müssen. Der Dienstleister hat dies zu kontrollieren. Der HDE lehnt die Tz 31 daher als zu weitreichend ab und fordert die Streichung.

Tz 17 und Tz 18: Online-Händler sollen verpflichtet werden, „kritische IT-Vorfälle“ sowohl den Strafbehörden als auch den Zahlungsdienstleistern zu melden. Auch diese Anforderung ist zu weitreichend und umfangreich. Derart sensible Meldungen wären mit der Weitergabe an einen Dienstleister nicht mehr kontrollierbar. Der HDE fordert daher die Streichung dieser Anforderung.

Tz 42: Wie unter II. bereits dargestellt, hat die Forderung nach starker Kundenauthentisierung weitreichende Konsequenzen im E-Commerce. Online-Kunden werden tendenziell auf andere Zahlungsarten ausweichen, die weniger komplex zu handhaben sind. Eine Folgenabschätzung dieses Punktes liegt derzeit nicht vor und sollte zunächst erstellt werden. Ebenso ist zu hinterfragen, ob der unterstellte Kundenschutz nicht auch auf andere Art erreicht werden kann. Auch heute haben Verbraucher weitreichende Sicherheit bei vielen Zahlungsarten, selbst ohne starke Authentifizierung. Zahlungsdienstleister wiederum könnten auf andere Weise verpflichtet werden, die entstehenden Risiken in ihre Geschäftsmodelle zu integrieren. Der HDE sieht daher nach heutigem Stand keine Notwendigkeit zur Umsetzung einer starken Kundenauthentisierung und fordert die Streichung der Tz.

Tz 43: Sollte die starke Kundenauthentisierung verpflichtend werden, sollen Ausnahmen für bestimmte Fälle gestattet werden. Der HDE befürchtet hier eine Marktverschiebung zugunsten der Ausnahme-Tatbestände. Anbieter könnten dies ausnutzen und höhere Entgelte fordern. Insbesondere folgende Ausnahmen werden kritisch gesehen:

- Kunden können eine Liste sogenannter „vertrauenswürdiger Zahlungsempfänger“ anlegen, für die eine starke Authentisierung nicht erfolgen soll.
  Es ist zu erwarten, dass mit dieser Ausnahmeregelung führende Anbieter bevorteilt werden. Kunden werden tendenziell dort bevorzugt einkaufen, wo sie einen leichten Checkout-Prozess durchlaufen. Haben sie einmal einen Zahlungsempfänger vertrauenswürdig eingestuft, kann dieser ihnen einen leichten Zahlungsprozess ermöglichen. Kleine Anbieter und Händler, die nicht über Plattformen anbieten, sind hier voraussichtlich benachteiligt.
- Transaktionen zwischen zwei Konten desselben Zahlungsdienstleisters können ohne starke Authentisierung erfolgen, sofern eine Risikoanalyse des Dienstleisters dies rechtfertigt.
  Mit dieser Ausnahme werden Zahlungsplattformen bevorzugt, die im Internet bereits eine weitreichende Akzeptanz erreicht haben. Kunden können hier weiterhin mit den bereits erlernten (einfachen) Authentisierungsformen zahlen und werden diese Zahlart tendenziell noch stärker nachfragen. Für Onlinehändler wird dies einen zusätzlichen Druck aufbauen, solche Zahlungssysteme zu akzeptieren.

Die beschriebenen Ausnahmetatbestände sorgen nach Ansicht des HDE zu Marktverschiebungen. Einerseits werden große Onlineanbieter und Handelsplattformen begünstigt, für die der Kunde eine Whitelist anlegen kann. Dies wird er für kleine Onlinehändler eher nicht nutzen. Mittelständische Händler sind daher benachteiligt. Andererseits können Zahlungsplattformen ihre Marktbedeutung ausbauen, da sie weiterhin eine einfache Authentisierung ermöglichen können. Dies führt voraussichtlich zu weiteren Konzentrationsprozessen bei Online-Zahlungssystemen.

Tz 49: Mit dieser Anforderung wird die starke Authentisierung verpflichtend. Insgesamt wird der Punkt 3.2 „Starke Kundenauthentisierung“ Tz 42 bis 57 aus den genannten Gründen abgelehnt.

Tz 51 enthält keine Informationen dazu, wer durch die Vorgaben bei der Haftung profitieren soll. Hier sollte eine Klarstellung erfolgen. Bei bisherigen Vorgaben musste der Handel i. d. R. nötige Investitionen tätigen ohne dabei von Haftungsreduzierungen oder günstigeren Konditionen profitieren zu können.

Tz 66 +74: Die Anforderungen bezüglich der Beschränkung der Login-Versuche / Transaktionen ist restriktiv formuliert. Ein Limit muss aus Handelssicht unter Risikogesichtspunkten ausgewogen gesetzt sein, da sonst zu viele „echte“ Kunden im Kaufprozess unnötig eingeschränkt und somit Umsätze verhindert werden. Hier sollte eine ausgewogene Konkretisierung erfolgen.

Tz 77 bis 79: Grundsätzlich ist zu begrüßen, dass sensible Zahlungsdaten - sofern eine Speicherung notwendig ist – entsprechend geschützt werden sollten. Auch heute gibt es bereits umfangreiche Vorgaben der Zahlungssysteme, die Acquirer beim Onlinehändler durchsetzen müssen.
Der HDE ist der Ansicht, dass hier keine zusätzliche gesetzliche Verpflichtung notwendig ist und von den Systemanbietern im eigenen Interesse geschaffenen Vorgaben und Industriestandards ausreichend sind (siehe dazu auch II.).

TZ 88: Die Anforderung beschränkt oder verhindert die Dienstleistung einer sogenanten „Corporate Paypage“. Damit wäre es Onlinehändlern nicht mehr möglich, die Zahlungsseite innerhalb des Onlineshops zu integrieren. Sollten zudem die jeweiligen Zahlungsdienstleister wie z.B. Acquirer aufgeführt werden müssen, würde das die Verbraucher verunsichern, da diese Institute in der Öffentlichkeit und bei Verbrauchern nicht unbedingt bekannt sind. Mit dieser Regelung ist der Handel nicht einverstanden.

IV. Fazit

Der HDE bewertet das Merkblatt äußerst kritisch und unausgewogen. Die Umsetzung ist daher abzulehnen. Insbesondere die umfangreichen Anforderungen an die Systemlandschaft des Online-Handels, die von den Zahlungsdienstleistern durchzusetzen sind und kontrolliert werden müssen, sind zu weitreichend und unangemessen.

Die Umsetzung würde aus heutiger Sicht zu unüberschaubaren Marktverwerfungen führen. Zahlungsplattformen würden aufgrund von Ausnahmeregelungen bevorteilt und könnten ihre Marktbedeutung weiter ausbauen. Mittelständische Händler werden benachteiligt, da Kunden bevorzugt bei großen Händlern und Anbieterplattformen einkaufen, die sie in Whitelists eingetragen haben.

Insbesondere die gesetzliche Regelung der starken Authentisierung bewertet der HDE äußerst kritisch und lehnt die Umsetzung ab. Bereits am Markt bestehende Lösungen mit starker Authentisierung zeigen, dass sie von Kunden gemieden und stattdessen andere Systeme mit einer einfachen Handhabung genutzt werden. Die für den Erfolg im E-Commerce entscheidende Convenience wird mit der starken Authentisierung über zwei Wege komplexer und unpraktikabel. Zudem bestehen andere Möglichkeiten, um die Risiken für die Verbraucher zu minimieren. Zahlungsdienstleister haben ein Eigeninteresse für die Umsetzung entsprechender Strategien und nutzen diese bereits heute. Eine quasi gesetzliche Regulierung über die BaFin wird daher nicht unterstützt.

Ansprechpartner:
Ulrich Binnebößel
binneboessel@hde.de