DKB Deutsche Kreditbank AG

Bundesanstalt für
Finanzdienstleistungsaufsicht
Referat Bankenaufsicht BA 57
Herrn Martin

Per E-Mail: poststelle@bafin.de

Berlin, 19. März 2015

Konsultation 02/2015 – Rundschreiben zu den Mindestanforderungen an die Sicherheit von Internetzahlungen; Entwurf

Sehr geehrter Herr Martin,

wir möchten gerne die Möglichkeit der Konsultation nutzen, Sie auf einige Aspekte und Besonderheiten von kreditkartengestützten Zahlungstransaktionen im Internet hinzuweisen.

1. Die Mindestanforderungen sollten der gegenwärtigen organisatorisch-technischen Entwicklung bei den Kreditkarten Rechnung tragen

1.1 Gegenwärtig versuchen die Herausgeber von Kreditkarten die notwendige Sicherheit von kreditkartengestützten Internet-Zahlungen durch das sog. 3-D-Secure-Verfahren zu erreichen, welches auf einem (zusätzlichen) Passwort beruht, das vom Karteninhaber vor Durchführung der Zahlungstransaktion abgefragt wird (sog. statisches Passwort). Dieses Verfahren setzt voraus, dass der betreffende „Online-Händler" dieses 3-D-Secure-Verfahren seinerseits technisch unterstützt. Außerdem hängt es davon ab, dass dieser Händler aufgrund seiner eigenen Risikoabschätzung für die einzelne Transaktion die Entscheidung trifft, dieses Verfahren einzusetzen. Dies hat zur Folge, dass derzeit nur ein einstelliger Prozentsatz aller kartengestützten Internet-Aktionen über 3-D-Secure abgewickelt werden.

Leider hat sich in den letzten Jahren gezeigt, dass diese statischen Passwörter in zunehmendem Maße von Kriminellen im Wege des sog. Phishings abgefragt werden, so dass die Zahl der trotz des 3-D-Secure-Verfahrens autorisierten Transaktionen deutlich zugenommen hat. Aus diesem Grund sind die Herausgeber von Kreditkarten derzeit im Begriff, das statische Passwort durch eine individuelle Einmal-Transaktionsnummer (sog. dynamisches Passwort) zu ersetzen, die dem Karteninhaber für jede Transaktion gesondert übermittelt wird. Die Übermittlung erfolgt gegenwärtig in der Regel durch eine SMS als sog. SMS-Tan, soll jedoch zukünftig über eine App als sog. Push-Tan geschehen. Die SMS-Tan genügt jedoch den Anforderungen der Tz 42 nicht, da sie lediglich ein Element aus einer Kategorie („Besitz") aufweist. Die Push-Tan erfüllt zwar mit je einem Element aus zwei Kategorien („Besitz" und „Wissen") die Voraussetzung einer starken

Deutsche Kreditbank
Aktiengesellschaft
Sitz der Gesellschaft:
Berlin

Ein Unternehmen der
Bayerischen Landesbank

Postanschrift
Deutsche Kreditbank AG
10919 Berlin

Telefon
030 120 30 - 8000

Telefax
030 120 30 - 8011

E-Mail
Vorstandsstab@dkb.ag

E-Postbrief
info@dkb.epost.de

Internet
www.DKB.de

BLZ: 120 300 00
BIC: BYLADEM 1001

USt-ID-Nr.: DE137178746
Handelsregister
Berlin-Charlottenburg
(HRB 34165)

Authentisierung i.S. v. Tz 42, weil zum Öffnen der App eine zusätzliche PIN benötigt wird. Sie kann aber, da die Nutzung einer App erforderlich ist, nur von Karteninhabern genutzt werden, die ein Smartphone besitzen. Es ist jedoch zu erwarten, dass der Anteil der Karteninhaber, die ein Smartphone besitzen und mit der Nutzung von Apps vertraut sind, mittelfristig stark zunehmen wird, so dass in überschaubarer Zeit die Push-Tan der Regelfall sein wird.

Die Einführung des sog. dynamischen Passworts hat für die Herausgeber von Kreditkarten bereits erhebliche Kosten verursacht. Wenn dieser Weg jetzt abgebrochen werden müsste, würden weitere Kosten in signifikanter Größenordnung entstehen, die vermeidbar wären, wenn zumindest für eine mittelfristige Übergangszeit die SMS-Tan als ausreichende Kundenauthentisierung anerkannt würde.

1.2 Der Einsatz dieses 3-D-Secure-Verfahrens soll zukünftig nach einem risikogewichtenden Ansatz nur noch bei Transaktionen erfolgen, bei denen nach den Parametern, welche im Kreditkartengeschäft durch die zahlreichen Verfahren zur Missbrauchsprävention gewonnen werden, ein entsprechend hohes Missbrauchsrisiko ermittelt worden ist. Dies trifft auf ca. 20 bis 30 % der Transaktionen zu. Die übrigen Transaktionen (70 bis 80 %) sollen nach gegenwärtigem Planungsstand nur die genannten Präventionsverfahren durchlaufen, ohne dass ein zusätzliches Authentisierungsverfahren zum Einsatz kommt.

Ein zusätzliches Authentisierungsverfahren ist auch nicht erforderlich, da bei der Durchführung kreditkartengestützter Zahlungstransaktionen im Rahmen der Autorisierung die Transaktion durch in der Regel mehrere, parallel eingesetzte Verfahren zur Missbrauchsprävention umfassend geprüft wird. Hinzukommt, dass der Umfang, in dem das 3-D-Secure-Verfahren eingesetzt wird, nicht festgeschrieben ist, sondern flexibel erfolgt. Bei zunehmender Zahl an Missbrauchsfällen stellen die Kartenherausgeber oder deren Dienstleister die Präventionsregeln schärfer ein - im eigenen Interesse, denn sie tragen ja den Missbrauchsschaden. Dies führt zwangsläufig zu einem Anstieg der 3-D-Secure-Authentisierungen.

2. Die Mindestanforderungen sollten gleiche Anforderungen für Issuer und Acquirer vorsehen

Die Sicherheit kreditkartengestützter Zahlungstransaktionen im Internet ist nur im Wege eines Zusammenwirkens zwischen dem Herausgeber der Kreditkarte und den Vertragsunternehmen, welche Kreditkarten akzeptieren („Akzeptanten") möglich. Dies zeigt sich beispielsweise an den gegenwärtigen 3-D-Secure-Verfahren: Hier wird eine Registrierung des Karteninhabers für dieses Verfahren nur dann wirksam, wenn es auch von der Akzeptanten- bzw. Händlerseite technisch unterstützt und im konkreten Fall auch eingesetzt wird, vgl. oben Ziffer 1.1.

Vor diesem Hintergrund ist es nicht ausreichend, wenn in den Tz 48 und 49 lediglich verlangt wird, dass die Acquirer Technologien für starke Authentisierung zu unterstützen und insbesondere „von ihrem Online-Händlern zu fordern" haben, ihrerseits solche Technologien zu unterstützen. Um eine ausreichende

Wirksamkeit der aufzustellenden Mindestanforderungen an die Sicherheit von Internet-Zahlungen zu gewährleisten ist es erforderlich, dass die Acquirer „ihren Online-Händlern" vertraglich vorzugeben haben, starke Authentisierungsverfahren zu unterstützen. Die Worte „zu fordern" in Tz 49 sind also durch die Worte „sicherzustellen" zu ersetzen.

3. Die Mindestanforderungen sollten auch für Intermediäre gelten

Dem Vernehmen nach soll die zukünftigen Mindestanforderungen nicht gelten, wenn ein Intermediär wie z.B. PayPal in die Transaktionskette eingeschaltet wird – vgl. Tz 43 dritter Gliederungspunkt. Die dort genannte Voraussetzung, dass es sich um Transaktionen „innerhalb desselben Zahlungsdienstleisters" handelt, trifft nämlich nicht zu. Die zur Abwicklung eines Geschäftsvorfalls erforderlichen Transaktionen finden nur zum Teil innerhalb des Intermediärs statt, zu einem erheblichen Teil aber auch außerhalb. Diese Beurteilung wird durch die praktische Erfahrung bestätigt: Auch bei der Abwicklung von Geschäften über PayPal entstehen Schäden durch den Missbrauch der bei PayPal hinterlegten Kreditkartendaten. Dies ist auch nicht überraschend, da der Kreditkarteninhaber sich gegenüber PayPal lediglich durch einen User-Namen und ein statisches Passwort authentifiziert.

Wir halten es deshalb für erforderlich, dass die zukünftigen Mindestanforderungen auch gegenüber einem Intermediär gelten.

Für Fragen stehen wir gern zur Verfügung.

Mit freundlichen Grüßen

Deutsche Kreditbank AG

Tilo Hacker
Mitglied des Vorstands

Christian Breitbach
stellv. Bereichsleiter Privatkunden