Wirtschaftskammer Österreich

Bundessparte Bank und Versicherung
Herrn Geschäftsführer Dr. Franz Rudorfer

Fachverband Finanzdienstleister
Herrn Mag. Philipp Bohrn

Wiedner Hauptstraße 63
1045 Wien

BEREICH Bankenaufsicht
GZ FMA-SG23 9590/0085-CSA/2014
(bitte immer anführen!)

EXPERT Mag. Bettina Kapfer
PHONE (+43-1) 249 59 - 1123
FAX (+43-1) 249 59 -1199
E-MAIL bettina.kapfer @fma.gv.at

WIEN, AM 4. Mai 2015

Veröffentlichung der EBA- Leitlinien zur Sicherheit von Internetzahlungen

Sehr geehrter Herr Dr. Rudorfer,
sehr geehrter Herr Mag. Bohrn!

Wir dürfen Sie darüber informieren, dass die Europäische Bankenaufsichtsbehörde (EBA) mit 19. Dezember 2014 Leitlinien zur Sicherheit von Internetzahlungen (EBA/GL/2014/12) publiziert hat. Die FMA begrüßt diese Leitlinien, weil diese europaweit einheitliche Mindeststandards für Internetzahlungen einführen. Die EBA hat dabei die Inhalte der Recommendations for the Security of Internet Payments des European Forum on Retail Payments („SecuRe Pay“) übernommen, in denen die vorliegenden Mindestanforderungen für Zahlungsdienstleister und auch Zahlungssysteme bereits Anfang 2013 veröffentlicht wurden (jedoch in für Zahlungsdienstleister nicht rechtsverbindlicher Form).

Sicherheitsstandards als Qualitätsmerkmal

Ziel von EBA ist es, einheitliche Sicherheitsvorschriften für sämtliche Zahlungsdienstleister in der EU festzulegen, damit im Ergebnis die Zahlungsdienstnutzer von der künftig wesentlich erhöhten Sicherheit von Internetzahlungen profitieren. Gleichzeitig soll damit auch das Vertrauen der Kunden in die Sicherheit von Internetzahlungen gestärkt werden.

Aus den genannten Gründen der erhöhten Sicherheit und Qualität von Internetzahlungen begrüßt auch die FMA die EBA Leitlinien, deren Einhaltung wir uns nicht nur erwarten, sondern darüber hinaus auch als Qualitätsmerkmal der Dienstleistungen von beaufsichtigten Unternehmen sehen.

Die FMA hat an die EBA daher eine positive Compliance-Erklärung gemäß Art. 16 Abs. 3 EBA-VO erstattet.

Zum Inhalt der Leitlinien zur Sicherheit von Internetzahlungen

Anwendungsbereich

Diese Leitlinien gelten, wie schon der Titel impliziert, für die Erbringung von über das Internet angebotenen Zahlungsdiensten durch Zahlungsdienstleister gem. Art. 1 der Richtlinie 2007/64/EG über Zahlungsdienste im Binnenmarkt („PSD"), sofern diese Internetzahlungen browserbasiert durchgeführt werden.

Vom **Anwendungsbereich erfasst** sind demnach folgende **browserbasierte Internetzahlungen**, unabhängig vom verwendeten Zugangsgerät:

- die Ausführung von Kartenzahlungen,
- die Durchführung von Überweisungen im Internet,
- die Erteilung und Änderung von elektronischen Einzugsermächtigungen,
- die Übertragung von elektronischem Geld;

Die Formulierung „unabhängig vom verwendeten Zugangsgerät" soll klarstellen, dass u.a. auch browserbasierte Internetzahlungen, die z.B. über ein Mobiltelefon oder Tablet ausgeführt werden, jedenfalls vom Anwendungsbereich der Leitlinien erfasst sind. Ausdrücklich vom Anwendungsbereich ausgeschlossen sind jedoch alle nicht browserbasierten mobilen Zahlungen, z.B. Zahlungen die ausschließlich in der Umgebung einer nativen Applikation abgewickelt werden.

Sofern Applikationen jedoch unter Einbindung eines Browsers agieren, muss geprüft werden, ob diese Einbindung dazu führt, dass eine browserbasierte Internetzahlung vorliegt und damit die gegenständlichen Leitlinien Anwendung finden. Die Anwendbarkeit der Leitlinien auf solche „gemischten Lösungen" muss daher im Einzelfall beurteilt werden.

Begriff der „sensiblen Zahlungsdaten"

Zentrales Element der Leitlinien ist die starke Kundenauthentifizierung, die die Auslösung von (browserbasierten) Internetzahlungen und den Zugang zu **sensiblen Zahlungsdaten** ebenso wie deren Änderung schützen soll. Die Leitlinien verwenden den Begriff der sensiblen Zahlungsdaten zwar an mehreren Stellen, lassen aber eine ausdrückliche Definition vermissen.

Aus einer Zusammenschau der Punkte 7. und 11. der Leitlinien kann abgeleitet werden, dass der Begriff der sensiblen Zahlungsdaten jedenfalls Folgendes umfasst:

- alle zur Identifizierung und Authentifizierung von Kunden verwendeten Daten,
- Erstellung/Änderung von so genannten „weißen Listen" (und damit implizit auch „schwarze Listen"),
- Daten, die einfach zu Betrugszwecken missbraucht werden können;

Auch die SecuRe Pay Recommendations on the Security of Internet Payments, auf denen die

vorliegenden EBA-Leitlinien beruhen, sehen gleichlautende Regelungen zum Schutz von sensiblen Zahlungsdaten vor, ohne diesen Begriff zu definieren. Hilfsweise kann damit auf den von SecuRe Pay veröffentlichten Assessment Guide (https://www.ecb.europa.eu/pub/pdf/other/assessmentguidesecurityinternetpayments201402en.pdf) zurückgegriffen werden, der **sensible Zahlungsdaten** als solche Daten definiert, die dazu **verwendet werden könnten, um Betrug zu begehen**. Als sensible Zahlungsdaten genannt werden hier ebenfalls **Daten, die zur Initiierung eines Zahlungsauftrages verwendet werden** (z.B. IBAN, nicht aber BIC, oder Kartendaten) und jene **Daten, die zur Authentifizierung verwendet werden**, wie z.B. Kundenidentifikatoren (z.B. Kundennummer, Log-In-Name), Passwörter, Codes, PINs, Geheimfragen für die Zurücksetzung von Passwörtern oder Telefonnummern. Gleichermaßen sollten auch jene Daten geschützt sein, die **zur Bestellung von Zahlungsinstrumenten oder Authentifizierungstools verwendet werden können** (sofern dem Kunden diese Funktionalität online zur Verfügung steht), wie z.B. Postadresse, Telefonnummer oder E-Mailadresse.

Damit hat jeder Zahlungsdienstleister anhand seiner jeweiligen technischen Lösung zu beurteilen, welche Daten konkret als sensible Zahlungsdaten einzustufen sind und damit durch starke Kundenauthentifizierung geschützt werden müssen.

Ad-hoc Anzeigeverpflichtung von schwerwiegenden Zahlungssicherheitsvorfällen

Ein „schwerwiegender Zahlungssicherheitsvorfall“ wird in den Leitlinien definiert als ein Vorfall, der wesentliche Auswirkungen auf die Sicherheit, Integrität oder Kontinuität der Zahlungssysteme des Zahlungsdienstleisters und/oder die Sicherheit sensibler Zahlungsdaten oder -mittel hat oder haben könnte. Bei der Beurteilung der Wesentlichkeit sollte die Anzahl der potenziell betroffenen Kunden, der Risikobetrag und die Folgen für andere Zahlungsdienstleister oder sonstige Zahlungsinfrastrukturen berücksichtigt werden.

Aufgrund der breiten Definition verbleibt für den einzelnen Zahlungsdienstleister ein großer Beurteilungsspielraum, was im konkreten Fall für den jeweiligen Zahlungsdienstleister, sein Geschäftsmodell und seine technischen Lösungen ein solcher schwerwiegender Sicherheitsvorfall ist. Im Rahmen der Erstellung der Sicherheitsrichtlinien nach Punkt 1., der Risikobewertung nach Punkt 2. und aufgrund der Verpflichtung in Punkt 3., Verfahren für Sicherheitsvorfälle festzulegen, ist von jedem Zahlungsdienstleister in seinen Sicherheitsrichtlinien individuell festzulegen, wann ein schwerwiegender Sicherheitsvorfall gegeben ist. Der Zahlungsdienstleister sollte demgemäß jedenfalls festlegen, ab welcher Anzahl potentiell betroffener Kunden, ab welchem Risikobetrag und angesichts welcher potentiellen Folgen für andere Dienstleister ein schwerwiegender Zahlungssicherheitsvorfall vorliegt, der gegebenenfalls auch gemäß Punkt 3.2. sofort den zuständigen Aufsichtsbehörden anzuzeigen ist („Ad-hoc-Anzeige“).

Damit diese Ad-hoc-Anzeige von allen Zahlungsdienstleistern (Verpflichtung gegenüber der FMA aufgrund der EBA-Leitlinien) aber auch von Zahlungssystemen (Verpflichtung gegenüber

der OeNB aufgrund der SecuRe Pay Recommendations) einheitlich erfolgt, haben OeNB und FMA gemeinsam ein Formular erstellt, das wir im Anhang anschließen. Dieses Formular ist für die Ad-hoc-Anzeige zu verwenden, d.h. im Fall eines schwerwiegenden Zahlungssicherheitsvorfalls an die jeweils zuständige Behörde zu übermitteln. Details zur Übermittlung finden Sie auf Seite 2 des Formulars.

Wir hoffen, Ihnen mit diesen Ausführungen zu den EBA Leitlinien zur Sicherheit von Internetzahlungen gedient zu haben und würden Sie ersuchen, die Zahlungsdienstleister über dieses Schreiben in Kenntnis zu setzen.

Mit freundlichen Grüßen,

Finanzmarktaufsichtsbehörde
Für den Vorstand

Dr. Michael Hysek
Bereichsleiter

Dr. Dagmar Urbanek
Stellvertretende Abteilungsleiterin

elektronisch gefertigt

Signaturwert	dOBQJZTQJcz5RNxxZHMUHJym48Ak7cVXXYRp0LWi18ktWpihkyedrohBu4gNhi4bkfyT/+eDyyUzkoj4tR33c8qAkfl17YsVWfFfKuBZ7Asvj5Athm/zN6Amq4XweVWqOlHJ7d5OrF31vtzPv3LG23kx1mr+C/Kx9QB71s7BsHG8pXeCoseyEvZ9p4QVcXe5kyzPS/FZn751T/Yt2Wx2/SsoFpvtl8V1kO+xnLi1rRM5gDM4xpIuENb1RhmfEIAH6TOKugwmXA6mMRSFkF40GcCXE+x6msTVfZWVgV81E6vbxDKr3+rRJyD3smp0lTKDzlLqrbr++URbXd4Fq3TRaQ==	
	Unterzeichner	Österreichische Finanzmarktaufsichtsbehörde
	Datum/Zeit-UTC	2015-05-05T06:53:55Z
	Aussteller-Zertifikat	CN=a-sign-corporate-light-02,OU=a-sign-corporate-light-02,O=A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH,C=AT
	Serien-Nr.	524262
	Methode	urn:pdfsigfilter:bka.gv.at:binaer:v1.1.0
Prüfinformation	Informationen zur Prüfung der elektronischen Signatur finden Sie unter: http://www.signaturpruefung.gv.at	
Hinweis	Dieses Dokument wurde amtssigniert. Auch ein Ausdruck dieses Dokuments hat gemäß § 20 E-Government-Gesetz die Beweiskraft einer öffentlichen Urkunde.	