

Open banking, Token, Contactless & Co.: Mit 14. September 2019 greift die PSD2-Richtlinie

Fri, 09/13/2019 - 10:46

Die Tipps für VerbraucherInnen der VZS

Die Bank hat mitgeteilt, dass es Änderungen bei der Nutzung von Bankomat- oder Kreditkarte geben wird, oder dass der Zugang zum Homebanking nunmehr anders zu erfolgen hat? Für die Nutzung der Bank-App muss die Geolokalisierung erlaubt werden, auch im Urlaub? Oder hat ein großer Onlinehändler um die Erlaubnis angefragt, Informationen über Ihr Bankkonto einholen zu dürfen? All dies hängt mit der sogenannten PSD2-Richtlinie zusammen, die ab 14. September voll durchgreift. Die „Payment Services Directive 2“, kurz PSD2, ist eine europäische Richtlinie, welche u.a. den Binnenmarkt der Zahlungen effizienter gestalten und die Zahlungen sicherer machen soll.

Freier Zugang für Drittanbieter

Eine große Neuheit betrifft das genannte open banking: ab 14.09.2019 können BankkundInnen Dritte dazu ermächtigen, ihre Konten einzusehen, und die Banken müssen diesen Drittanbietern Zugang gewähren. VerbraucherInnen können den Drittanbietern auch erlauben, Zahlungsbewegungen durchzuführen. Den KundInnen steht es dabei natürlich frei, die Ermächtigung an die Drittanbieter jederzeit zu widerrufen.

Sicherheit: die „starke“ Authentifizierung

Was die sogenannte „starke Kunden-Authentifizierung“ bei Online-Bank-Bewegungen oder Karten-Zahlungen mit Zugang über PC, Smartphone, usw. betrifft, hat die Banca d'Italia den Banken eine weitere Übergangsfrist eingeräumt, um die notwendigen technischen Umstellungen vorzunehmen, da einige Banken anscheinend noch hinterherhinken. Ein genaues Enddatum für diese Zusatzfrist hat die

Notenbank bis heute nicht bekannt gegeben.

Wie werden BankkundInnen identifiziert?

Die Identität der KundInnen muss festgestellt werden, indem 2 von 3 möglichen Faktoren abgefragt werden:

1. etwas, das nur der Kunde kennt, z.B. Pin-Nummer oder Passwort;
2. etwas, das nur die Kundin hat, z.B. Smartphone oder anderer Token;
3. etwas, das nur der Kunde ist, z.B. Fingerabdruck oder andere biometrische Erkennungsart.

Was ändert sich für VerbraucherInnen?

Innerhalb Europas reicht es nicht mehr, bei Zahlungen per Kreditkarte nur deren Nummer und den Sicherheitscode (CVV) auf der Rückseite der Karte zu kennen, und auch die von den verschiedenen „Token“ generierten Passwörter der Vergangenheit reichen nicht mehr aus, um den Zugriff aufs Konto zu gewähren. Auch die TAN-Nummern-Listen in Papierversion dürfen nicht mehr verwendet werden. Alle Zugänge und Zahlungen (mit nur wenigen Ausnahmen wie z.B. die contactless-Zahlung per Karte bei Beträgen unter 50 Euro) müssen der starken Kunden-Authentifizierung gerecht werden.

Nicht genehmigte Abbuchungen vom Konto

Diese können grundsätzlich beanstandet werden, und zwar sowohl bei Ungereimtheiten in einer an sich legitimen Belastung als auch gänzlich nicht genehmigten Belastungen (die Details finden sich hier).

Fazit

„In der Summe soll die PSD2-Richtlinie mehr Sicherheit für BankkundInnen bringen, da die starke Authentifizierung kriminelle Zugriffe auf Konten und Karten unterbindet; dies bringt jedoch komplexere Login-Prozeduren mit sich. VerbraucherInnen müssen auch noch besser darauf achten, was zur Unterschrift vorgelegt wird, da per Ermächtigung jedem Drittanbieter Einblick und Zugriff auf die Karten und Konten gewährt werden kann“ fasst VZS-Geschäftsführer Walther Andreas zusammen.

PSD2 – Ein (sehr) kurzes Glossar

Instant payment	Sofort-Zahlung Schnellüberweisung über gesonderten Kanal
Mobile payment	Mobile Zahlung Zahlung, die per Smartphone, Smartwatch, usw. veranlasst wird
Open banking	zum Unterschied zur traditionellen, „geschlossenen“ Beziehung (Bank-Kunde) werden durch die PSD2 „offene“ Beziehungen möglich (Bank – Kunde – Drittanbieter – Preisvergleichswebsite ... usw.)
OTP - one time password	Einmal-Passwort, meist numerisch, das in diesem Kontext normalerweise im Moment generiert wird und eine sehr begrenzte Dauer (z.B. 60 Sekunden) hat
SCA – strong customer authentication	Starke Kunden-Authentifizierung die Authentifizierung muss über 2 Faktoren erfolgen, allein die Eingabe von Username und Passwort ist nicht mehr ausreichend
TAN–Liste: Liste mit Transaktions-Authentifizierungs-Nummern	Bis dato von einigen Banken verwendetes Verfahren: die Bank übergab eine Liste von Transaktionsnummern; bei jedem Buchungsvorgang – der Transaktion – musste eine beliebige TAN der aktiven Liste eingegeben werden. Dieses Verfahren darf mit PSD2 nicht mehr verwendet werden, die TAN müssen anderweitig erzeugt werden (z.B. photoTAN und QR-TAN)
Token	hier: Physisches Hilfsmittel zur Identifizierung und Authentifizierung
TPP - Third Party Providers	Drittanbieter, die mit Ermächtigung auf Konten oder Karten zugreifen können