Sicherheit

Zwei-Faktor-Authentifizierung bei Amazon

Rund ein Jahr nach dem Start in den USA hat Amazon im Dezember 2016 auch in Deutschland die Zwei-Faktor-Authentifzierung eingeführt (die bei dem Online-Händler „Zwei-Schritt-Verifizierung" genannt wird). PSD2-konform ist der Online-Riese aber vermutlich noch lange nicht, allein schon deshalb, weil der Kunde die zusätzliche Sicherheitsstufe für Endgeräte, die er häufig zum Online-Kauf nutzt, abschalten kann.

Wer sich unter den „erweiterten Sicherheitseinstellungen" für die Zwei-Schritt-Verifizierung anmeldet, muss zum Abschließen einer Bestellung neben dem Namen und Passwort ein weiteres Merkmal zum Login in Form eines Zahlencodes angeben. Dieser Code kann entweder per SMS oder Sprachanruf zugestellt oder per App erzeugt werden. Im ersten Schritt der Einrichtung kann hierzu entweder eine entsprechende Mobilfunknummer angegeben oder die Nutzung per App gewählt werden. Im letztgenannten Fall soll im App-Store des Handys nach „Authentifizierungs-App" gesucht werden. Möglich ist beispielsweise die Nutzung von Google Authenticator und Microsoft Authenticator. Die Anmeldung in der App kann dann wiederum über das Scannen eines QR-Codes erfolgen. Zu guter Letzt fordert Amazon die Nutzer auf, eine Back-Up-Methode anzugeben, falls die gewählte Authentifizierungs-Methode nicht funktioniert.

Gestartet ist das Verfahren offenbar mit Kinderkrankheiten, die sich wohl werden ausmerzen lassen. Eine Reihe von Kunden musste sich selbst nach Rücksprache mit dem Kundendienst wieder von der Zwei-Schritt-Verifizierung abmelden, weil das System die SMS mit dem Transaktionscode in ihrem Fall offenbar gar nicht erst generierte.

Die eigentliche Tücke liegt allerdings wohl an anderer Stelle: Solange für Einkauf und Code-Abfrage unterschiedliche Geräte verwendet werden, ist das Verfahren plausibel. Immer dann aber, wenn der Kunde für den Einkauf das gleiche Smartphone nutzt, an das auch der Code zur Transaktionsfreigabe geschickt wird beziehungsweise auf dem sich die App befindet, bietet sich ein potenzieller Angriffspunkt für Cyberkriminelle, wenn das Smartphone erst einmal von einem Trojaner befallen ist.

Für das Mobile Banking ist die SMS-TAN aus diesem Grund nicht erlaubt. Mithin dürfte ein vergleichbares Verfahren auch gemäß PSD2 beziehungsweise den technischen Regulierungsstandards der EBA vermutlich keinen Bestand haben.

Damit steht Amazon aber nicht allein. Wie sich die geforderte Unabhängigkeit der beiden Faktoren beim Mobile Banking oder eben auch dem Mobile Shopping lösen lässt, scheint derzeit noch nicht ausgemacht. Nicht wenige Marktteilnehmer haben sich schließlich schon dahingehend geäußert, dass derartige Nutzungen künftig nur noch mit zwei getrennten Geräten möglich sein könnten. Mobile Shopping ginge dann wohl nur noch mit dem Notebook oder dem Zweithandy. So sieht es offenbar auch der S-ID-Check vor, den die Pluscard als neues Sicherheitsverfahren für Sparkassen-Kreditkarten entwickelt hat (siehe dazu Beitrag auf Seite 24). Im Erklärfilm zu S-ID wird für den Einkauf ein Tablet genutzt, während die Transaktionsfreigabe auf dem Smartphone erfolgt. **Red.**