PSD2 und Banking

Seit dem 14. September 2019 schreibt die PSD2 beim Online-Banking eine Zwei-Faktor-Authentifizierung vor, die zwei Elemente aus zwei der drei Bereiche Wissen, Besitz und Inhärenz (Biometrie) verlangt. c't beantwortet die wichtigsten Fragen rund um deren Umsetzung.

Von Markus Montz

Home- und Multibanking

Ich kann mit meiner Homebanking-Software/Multibanking-App keine Kontodaten von Kreditinstitut XY mehr abrufen, geschweige denn Überweisungen tätigen. Was ist das Problem?

Wir wissen, dass Nutzer von Home- und Multibanking-Anwendungen insbesondere in den ersten Wochen nach der Umstellung auf die Starke Kundenauthentifizierung mit größeren Problemen kämpften, als es zunächst den Anschein hatte. Bei einigen Banken waren die Schnittstellen überhaupt nicht erreichbar, anderswo traten Probleme bei der Authentifizierung auf oder die Durchführung gestaltete sich sehr umständlich.

Die Probleme kommen wenig überraschend: Bereits für die Entwickler einer Banking-Anwendung gestaltet es sich schwierig, die Schnittstellen hunderter Kreditinstitute unter den neuen Regeln auf Anhieb reibungsfrei anzubinden. c't geht deshalb davon aus, dass es sich um Umstellungsprobleme handelt, die die Hersteller und Banken erst allmählich in den Griff bekommen. Auch c't kann Fehler und ihre Ursachen nur selten eindeutig identifizieren: Zum einen können wir nicht tausende Kombinationen von Anwendungen und Banken permanent beobachten, zum anderen technische Fehler häufig nicht zweifelsfrei einer Partei zuordnen – so gerne wir Ihnen als Leser auch weiterhelfen würden.

Neben technischen Schmerzen hat an vielen Stellen zudem der Komfort gelitten. Die Kreditinstitute handhaben die Ausnahmen unterschiedlich, die die Europäische Bankenaufsicht in den „technischen Regulierungsstandards für eine starke Kundenauthentifizierung und für sichere offene Standards für die Kommunikation", kurz RTS, festgelegt hat (sie bilden eine Art Durchführungsbestimmung für die Sicherheitsanforderungen der PSD2). Daher kann ein Kontenrundruf bei mehreren Banken auch zu mehreren TAN-Abfragen führen – eine Bank lässt die 90-Tage-Ausnahme beim Login zu, die andere nicht. Hier bleibt nur zu hoffen, dass die Banken den Kunden auf Dauer entgegenkommen, etwa durch individuelle Konfigurationsmöglichkeiten.

Android-Smartphones unsicher?

Ich habe gelesen, dass vor allem Android-Smartphones keine gute Wahl für eine TAN-App sind, weil sie nach relativ kurzer Zeit keine Betriebssystem-Updates mehr erhalten. PSD2 scheint aber dazu zu führen, dass die Kreditinstitute ihre Kunden zur Nutzung solcher Apps drängen. Wie seht Ihr das bei c't?

Zunächst einmal haben Sie meist die Wahl zwischen TAN-Generator und Smartphone – was wir gut finden. Für sich genommen stellt aber auch ein Smartphone mit veraltetem Android noch kein Problem dar. Die Bank bindet eine TAN-App bei der Einrichtung an das jeweilige Handy oder Tablet – und sie kontrolliert, dass das Gerät dem rechtmäßigen Kontoinhaber tatsächlich gehört. Die TAN-App prüft das Smartphone beim Start auf (auch unbemerktes) Rooting und andere Unregelmäßigkeiten. Im Normalfall muss der Nutzer die App außerdem per Passwort oder Fingerabdruck/Gesichtserkennung aufsperren. Die TAN selbst wird verschlüsselt übermittelt. Geht trotzdem etwas schief, darf eine Bank ihre Kunden bei einfacher Fahrlässigkeit nur bis maximal 50 Euro für Schäden haftbar machen. Das zwingt sie dazu, ihre Apps auch für ältere Android-Handys so sicher wie möglich zu halten.

Direkte Angriffe auf Smartphones, etwa durch eine Sicherheitslücke im Browser („Drive-by"), sind zwar möglich, geschehen aber relativ selten. Betrüger setzen vor allem auf indirekte, einfachere Wege, um sich Zugriff auf das Onlinebanking Dritter zu verschaffen: Trojaner in Mailanhängen, Textnachrichten oder Werbebannern, Schadcode auf Websites, die Lücken im Browser ausnutzen. Infizierte PCs mit persönlichen Daten des Nutzers liefern ebenfalls Angriffsmöglichkeiten. Unter anderem erleichtern sie eine gezielte Verhaltensmanipulation des Nutzers („Social Engineering"). Zu letzterer gehören Phishing-Mails oder auch gefälschte Rechnungen oder Mahnungen, gegen die keine Zwei-Faktor-Authentifizierung hilft. Eine weitere Gefahrenquelle sind Apps aus nicht vertrauenswürdigen Quellen.

Sichere TAN-Verfahren

Was ist das sicherste TAN-Verfahren? Warum soll die SMS-TAN ein unsicheres Verfahren sein? Und warum darf ich mein gerootetes Smartphone nicht nutzen, ich kenne mich doch aus?

Bei den technisch gesehen sichersten Verfahren holen Sie die TAN über einen dedizierten TAN-Generator mit eingesteckter Bankkarte ohne Verbindung zum Internet ab. Dazu zählen chipTAN, photoTAN und QR-TAN. Um diese Verfahren auszutricksen, müsste man Ihnen einen manipulierten Kartenleser unterjubeln, uns ist aber kein solcher Fall bekannt. Verfahren, die mit schreib- und kopiergeschützten HBCI-Schlüsseldateien oder Lesegerät-Chipkarten-Kombinationen arbeiten, gelten als vergleichbar sicher.

Smartphones mit speziellen TAN-Apps sind nach derzeitigem Stand fast genauso sicher, solange man das Gerät vor unbefugtem Zugriff schützt (siehe dazu auch die nächste Frage). Wichtig ist hier wie bei allen TAN-Verfahren, dass man die Überweisungsdaten vor der Bestätigung abgleicht. Am besten geschieht dies mit den Daten auf der Rechnung, da sich Bildschirmanzeigen manipulieren lassen.

© Copyright by Heise Medien
Persönliches PDF für alle Leser der c't aus 30625 Hannover

Die SMS-TAN ist ein Streitfall. Die Europäische Bankenaufsicht hat sie in einer Stellungnahme als zulässiges Authentifikations-Verfahren bezeichnet. Gegen die SMS-TAN spricht, dass sie unverschlüsselt verschickt wird – von einem per Trojaner gekaperten Smartphone lässt sie sich mühelos auslesen. Wenn Kriminelle an persönliche Daten eines Onlinebanking-Nutzers gelangt sind, können sie sich beim Mobilfunkprovider unter Umständen auch eine Zweit- oder Ersatz-SIM-Karte verschaffen und so an die TANs gelangen.

Beim Rooting sind die Banken aus guten Gründen strikt. Auf gerooteten (oder bei Apple gejailbreakten) Smartphones sind wichtige Schutzfunktionen deaktiviert. Angreifer können leicht schädliche Apps installieren oder Code ausführen. Wir raten deshalb vom Rooting ab und kennen auch keine Bank, die vertraglich und technisch ein Onlinebanking, geschweige denn die Aktivierung von TAN-Apps auf gerooteten Handys zulässt.

Ausnahmen ja oder nein?

Konterkariert die 90-Tage-Ausnahme nicht das Sicherheitsversprechen der PSD2? Mein Kreditinstitut fordert nicht einmal dann erneut eine TAN an, wenn ich mich von einem neuen Gerät anmelde!

Grundsätzlich erhöht jede Zwei-Faktor-Authentifizierung auch die Sicherheit. Insofern stellen die Vorschriften der PSD2 verglichen mit der zuvor üblichen Praxis „Nutzerkennung plus PIN/Passwort“ auch mit Ausnahmen bereits einen Fortschritt dar. Saldo- und Umsatzdaten werden etwas besser geschützt, zumal ja Abfragen jenseits der vorangegangenen 90 Tage trotzdem eine TAN erfordern. Eine TAN-Abfrage bei einem Login von neuen Geräten halten wir zur Verbesserung der Sicherheit ebenfalls für geboten, um Betrügern selbst den lesenden Zugang zu fremden Konten zu erschweren – die PSD2 und ihre technischen Regulierungsstandards schreiben solch ein Vorgehen allerdings nicht vor.

Das gilt auch für den umgekehrten Fall. Entscheidet sich ein Kreditinstitut, bei jedem Login obligatorisch eine TAN-Abfrage durchzuführen, handelt es juristisch korrekt. Ein Zwang zur Implementierung der Ausnahmen besteht nicht. Die damit einhergehenden Probleme für die Benutzerfreundlichkeit insbesondere von Home- und Multibankinganwendungen kennen wir ebenfalls; die technischen Regulierungsstandards lassen den Banken und Sparkassen aber die Wahl.

Wünschenswert wäre vor diesem Hintergrund aus unserer Sicht, dass die Banken und Sparkassen ihren Kunden in Zukunft möglichst weitreichende Autonomie geben, anstatt ihnen statische Vorgaben zu machen. Die Voreinstellungen sollten maximale Sicherheit liefern, Kunden in den Einstellungsoptionen ihres Kontos aber die Wahl zwischen einer Zwei-Faktor-Authentifizierung bei jedem Login und Ausnahmen haben. Zu den Ausnahmen zählen neben der 90-Tage-Regel beispielsweise auch eine vom Kunden gepflegte Liste vertrauenswürdiger Empfänger sowie die Kleinbetragsregelung, nach der Überweisungen bis 30 Euro TAN-frei sein dürfen.

Auf mittlere Sicht erreicht die PSD2 aber vielleicht eines der Ziele ihrer Schöpfer: Banken, die Sicherheit und Komfort am besten verknüpfen, werden im Wettbewerb einen Vorteil genießen.

Verlorenes Smartphone

Auf Empfehlung meiner Bank habe ich im Zuge der PSD2-Umstellung auf ein TAN-App-Verfahren gewechselt. Nun frage ich mich natürlich, was passiert, wenn ich das Smartphone verliere, es mir gestohlen wird oder es den Geist aufgibt. Wie komme ich in solch einem Fall schnell wieder in vollem Umfang an mein Bankkonto?

Wenn Sie auf Nummer sicher gehen wollen oder müssen, aktivieren Sie als Backup ein zweites Gerät. Die meisten Kreditinstitute erlauben parallel eingerichtete TAN-Verfahren. Beispielsweise können Sie bei der Postbank sowie vielen Genossenschaftsbanken und Sparkassen zusätzlich zur TAN-App auf dem Smartphone ein chipTAN-Verfahren mit dem sogenannten Flickercode freischalten. Entsprechende Geräte sind untereinander kompatibel und für unter 10 Euro zu haben. Die proprietären photo- und QR-TAN-Generatoren anderer Banken erfüllen den gleichen Zweck, sind aber zum Teil deutlich teurer. Ebenso ist ein billiges Handy für SMS-TANs denkbar; hier müssen Sie allerdings darauf achten, dass die SIM-Karte aktiviert bleibt. Für die SMS können Gebühren anfallen.

Da die Bank die TAN-App fix an das nicht mehr verfügbare Smartphone gebunden hat, können Sie Ihren Onlinebanking-Zugang je nach Bank ansonsten nicht oder nur lesend nutzen, bis Ihnen die Bank die neu installierte App auf einem neuen Smartphone freigeschaltet hat. Bei einigen Kreditinstituten hat ein Backup jedoch den Vorteil, dass Sie mit dem Backup-Gerät eine neu installierte TAN-App direkt aktivieren dürfen. Damit vermeiden Sie etwaiges Warten auf Freischaltcodes per Briefpost.

Bei mutmaßlichem Diebstahl oder Missbrauch des Gerätes müssen Sie außerdem den Zugang zu Ihrem Onlinebanking sperren, etwa über die Notfallnummer 116 116. In solchen Fällen werden Sie zusätzlich zur App auch um den Aufwand einer erneuten Freischaltung des Bankings nicht herumkommen. *(mon@ct.de)*

Hat Ihre Bank Ihnen ein erstes Endgerät für die TAN-Übermittlung freigeschaltet, können Sie in der TAN-Verwaltung oft weitere Endgeräte aktivieren – natürlich mit vorheriger Bestätigung per TAN. Bei Bedarf lassen sich Geräte einzeln deaktivieren oder sperren. Bei der TAN-Eingabeaufforderung während des Bankings wählen Sie das Ihnen gerade genehme Zielgerät aus.

© Copyright by Heise Medien
Persönliches PDF für alle Leser der c't aus 30625 Hannover