Regulierung

Die EBA irrt – Screen Scraping darf nicht verboten werden

Von Ralf Ohlhausen ▬ Mit der zweiten Zahlungsdiensterichtlinie wollte die EU eigentlich die Position von Fintech-Unternehmen stärken. Ein technisches Detail zielt jetzt aber genau auf das Gegenteil ab und benachteiligt die neuen Player der Finanzbranche.

Da wird der Bock zum Gärtner gemacht: Die zweite, erweiterte Zahlungsdiensterichtlinie der EU (Payment Service Directive 2, PSD2) geht im Januar 2018 an den Start. Sie wirft jedoch schon länger ihre Schatten voraus. In diesem Schatten stehen jetzt ausgerechnet Fintech-Unternehmen, die durch die PSD2 eigentlich gestärkt und ins rechte Licht gerückt werden sollten.

Zentrales Streitthema ist ein Detail, das von der Europäischen Bankenaufsicht (European Banking Authority, EBA) in einem Begleitdokument zur PSD2 aufgeführt wird. In einem der Regulatory Technical Standards (RTS) geht es um die Kundenauthentifizierung und die sichere Kommunikation zwischen Banken und Fintech-Unternehmen. Darin möchte die EBA eine Technik namens Screen Scraping untersagen, die bisher von Fintech-Unternehmen auf breiter Front eingesetzt wird, um auf Daten von Bankkunden – in deren Auftrag und mit deren Erlaubnis natürlich – zuzugreifen. Ein solches Verbot würde eindeutig Banken bevorzugen und Fintech-Unternehmen unnötige Steine in den Weg legen.

Umweg statt direkter Zugriff

Screen Scraping hört sich vielleicht besorgniserregend an, ist aber nichts anderes als ein automatisiertes „Internet Browsing", das heißt das gleiche, was man sonst manuell macht, nur schneller. Mehr und mehr seriöse Fintech-Unternehmen – und übrigens auch viele Banken – setzen dieses automatisierte Navigieren und Auslesen von Webseiten in vielen ihrer Produkte ein. Technisch gesehen handelt es sich dabei also einfach um einen erlaubten, direkten Datenzugriff auf das Kunden-Interface einer Bank. „Erlaubt" deshalb, weil der Fintech-Kunde natürlich erst explizit zustimmen muss, wenn zum Beispiel eine App oder ein Dienst auf seine Bankdaten zugreifen will, etwa, weil er seinen Kontostand abrufen oder andere Finanzdienstleistungen in Anspruch nehmen möchte.

Im vorliegenden Papier der EBA steht nun, dass Banken diesen direkten Zugriff auf die Kundendaten nicht gewähren müssen, wenn Sie stattdessen einen anderen, indirekten Zugriff ermöglichen, das heißt eine eigens für Drittanbieter eingerichtete Programmierschnittstelle (Application Programming Interface, API) schaffen. Frei nach dem Motto: Warum einfach, wenn es auch kompliziert geht.

Banken kontrollieren Fintechs

Aber warum reicht den Fintechs ein solcher indirekter Zugriff auf die Kundendaten nicht aus? Und warum wollen sich die Banken diese zusätzliche Mühe machen? Um das zu verstehen, muss man sich die aktuelle Situation in der Finanzbranche ansehen. Der Erfolg von Fintech-Unternehmen steht auf zwei Beinen: Innovation und Nutzererlebnis. Fintechs haben den Banken in den letzten Jahren gezeigt, wie sich ein Markt durch technische Innovationen revolutionieren lässt, sei es mit Apps, die direktes Bezahlen von Smartphone zu Smartphone erlauben, oder mit Webdiensten, welche die monatlichen Ausgaben auf einen Blick übersichtlich darstellen oder in Bruchteilen von Sekunden den günstigsten Kredit für den Nutzer finden. Wichtig ist dabei das Stichwort „Nutzer", denn die technischen Fortschritte bieten Fintechs in kinderleicht zu bedienende Apps und über Zahlungsdienste. Coole Innovationen und das perfekte Benutzererlebnis sind jedoch akut gefährdet, wenn der direkte Zugriff auf die Kundendaten wegfällt.

Wenn die Banken stattdessen nur eine API bereitstellen müssen, können sie zukünftig wieder alles selbst kontrollieren – insbesondere die Innovationen der Fintechs. Denn was die Schnittstellen für Drittanbieter genau können müssen, ist nirgends festgelegt. Neue Funktionen könnten möglicherweise erst einmal nur die Bankkunden auf direktem Weg nutzen, in der API landen sie erst später oder gar nicht. Das wirkt sich natürlich auch auf das Nutzungserlebnis der Kunden aus. Fintechs verlieren durch die Neuregelung also beide Standbeine und Banken behalten die Hoheit über die Daten der Nutzer.

Falsch verstandene Sicherheit

EBA und Banken schwingen als Argument gegen Screen Scraping die Sicherheitskeule – zu Unrecht. Natürlich muss man Kunden vor Datendiebstahl schützen, etwa vor Phishing-Angriffen, aber genau dafür gibt es ja die neuen, zusätzlichen Sicherheitselemente der PSD2, die für Banken und Fintechs gleichermaßen gelten werden. Zudem ist es dafür nicht relevant, ob man vorne das Online-Banking direkt nutzt oder

durch die Hintertür über eine API auf den Kundenstamm zugreift.

Dass sich regulierte Finanzdienstleister den Zugang zu Kundendaten teilen, sollte nicht nur selbstverständlich möglich sein, es ist dank PSD2 auch sehr gut abgesichert. Finanzunternehmen müssen sich regelmäßigen Audits unterziehen sowie technische und rechtliche Schritte unternehmen, um Kundendaten zu schützen. Das umfasst natürlich die Zugangsdaten, aber auch die tatsächlichen Finanzdaten. Sollten hier Fehler passieren, drohen massive Strafen.

Kontrolle durch die Kunden

Dabei sollte es in der aktuellen Diskussion gar nicht um die Frage gehen, ob Banken oder Fintechs die Kontrolle über Kundendaten haben. Diese wird nämlich gerade ganz woanders beantwortet: Die neue EU-Datenschutz-Grundverordnung legt weitreichend fest, dass die Kontrolle über Daten beim Kunden selbst liegen muss, also weder bei den Banken, noch bei den Fintechs. Und übrigens gilt das auch für alle anderen Unternehmen, die Kundendaten (nur) verwalten, wie beispielsweise Versicherungen, Telekommunikationsunternehmen oder Social-Media-Anbieter.

Kunden müssen auf ihre Daten zugreifen, sie anpassen und auch teilen können, wenn sie das wollen, um innovative neue Services zu nutzen. Der automatisierte, direkte Zugriff über die Kunden-Schnittstelle ist dabei der verlässlichste und oft auch einzige Weg, der dafür offen stehen bleiben muss.

Ralf Ohlhausen, Business Development Director, PPRO Group, London