Die EU öffnet den Markt für neue Zahlungsdienstleister

Innovationen von Nichtbanken revolutionieren den Zahlungsverkehr. Doch die traditionellen Banken wehren sich gegen eine regulierte Marktöffnung. Anders als die Schweiz hat die EU darauf reagiert: Sie öffnet den Markt für Drittanbieter, fordert aber gleichzeitig höhere Sicherheitsstandards. *Susan Emmenegger*

Abstract **Die Digitalisierung führt auf dem Markt für Zahlungsdienste zu neuen Produkten und neuen Anbietern aus dem Nichtbankensektor. Das verschärft nicht nur den Wettbewerb, sondern erhöht auch das Risiko von unbefugten Zugriffen auf die Konten von Bankkunden. Wie sollen die Banken mit diesen neuen Akteuren umgehen? Und wie kann man die Kontosicherheit erhöhen? Die EU hat mit der zweiten Zahlungsdiensterichtlinie (PSD2) klare Entscheidungen getroffen. Sie forciert die Öffnung der Banken gegenüber neuen Anbietern (Fintechs) und erhöht die Sicherheitsanforderungen bei elektronischen Zahlungsvorgängen. In der Schweiz besteht seitens der Banken Widerstand gegen einen entsprechenden Regulierungsansatz. Mittelfristig lassen sich allerdings gewisse regulatorische Eckpunkte für die neuen Anbieter nicht vermeiden; spätestens dann wird sich aber die Frage einer forcierten Marktöffnung für Zahlungsdienste aus dem Nichtbankensektor erneut stellen.**

Die technologiegetriebenen Innovationen im Zahlungsverkehr haben eine Vielzahl von neuen Produkten und Anbietern hervorgebracht. Spontan denkt man an Bitcoin, Ethereum oder Ripple oder an eine weitere der rund 1500 Kryptowährungen. Diese dienen allerdings heute nur selten als Zahlungsmittel; sie werden primär als Anlageinstrumente eingesetzt. Doch auch im eigentlichen Zahlungsverkehr gibt es Innovationsschübe, die unübersehbar sind, wie etwa die Near-Field-Technologie, die von Apple Pay oder der Schweizer Bezahl-App Twint verwendet wird. Die neuen Technologien sind in den letzten Jahren zur Gewohnheit geworden und haben die Abwicklung von Zahlungsvorgängen stark verändert und beschleunigt.

Getrieben werden die Entwicklungen nicht zuletzt durch die sogenannten Finanztechnologieunternehmen (Fintechs). Sie brechen die traditionelle Wertschöpfungskette der Banken auf, nutzen aber vielfach deren Infrastruktur für die eigene Dienstleistung. Ein Zahlungsverkehr ganz ohne Banken, wie ihn die Blockchain-Technologie verspricht, ist momentan noch Wunschdenken.

Das «Surfen auf der Bankinfrastruktur» verschärft die Problematik der Datensicherheit und des Datenschutzes, die beim elektronischen Zahlungsverkehr ohnehin schon bestehen. Eng damit verbunden ist die Gefahr von unbefugten Zugriffen auf die Konten von Bankkunden, namentlich durch Hackerangriffe.

Die EU hat bereits darauf reagiert. Das Auftreten von Anbietern ohne Banklizenz und die erhöhte Gefahr von Hackerangriffen wurden mit der Revision der ersten Zahlungsdiensterichtlinie aus dem Jahr 2009 angegangen. Die zweite Zahlungsdiensterichtlinie (Second Payments Services Directive, PSD2) gilt seit Anfang 2018.

Zahlungsdienste ohne Banklizenz

Mit der neuen EU-Richtlinie PSD2 werden drei Kategorien von sogenannten Dritten Zahlungdienstleistern auf dem Markt für Zahlungsdienste zugelassen: Kontoinformationsdienste, Zahlungsauslösedienste und Drittemittenten von Zahlungskarten. Letztere gibt es auf dem Markt noch nicht, weshalb sich die gegenwärtige Diskussion auf die ersten beiden konzentriert.

Kontoinformationsdienste wie etwa Qontis ziehen sämtliche Kontoinformationen eines Bankkunden bei den verschiedenen Banken zusammen und erlauben einen benutzerfreundlichen Überblick über dessen gesamte Finanzlage. Sie werden meist mit anderen Diensten, wie Liquiditätstools oder Budgetierungstools, kombiniert. Bei den Zahlungsauslösediensten wie zum Beispiel Klarna (früher Sofort GmbH) handelt es sich um eine Softwarebrücke zwischen den E-Commerce-Händlern und den Webportalen der Bank, die einen einfachen Zahlungsvorgang ermöglicht. Bei beiden Diensten gewährt die Kundin den Zahlungsdienstleistern einen direkten Onlinezugriff auf ihr Bankkonto, indem sie ihre persönliche PIN oder Transaktionsnummer auf dem Webportal der externen Zahlungsdienstleister eingibt. Dieser Vorgang, den man «screen scraping» nennt, ist anfällig für Hackerangriffe (sogenannte Man-in-the-Middle-Attacken).

Auch in der Schweiz haben sich Kontoinformationsdienste und Zahlungsauslösedienste etabliert. Wer diese Dienste nutzt, trägt zurzeit aber die gesamte Verantwortung für Störvorgänge, insbesondere auch für Hackerangriffe auf das Bankkonto. Denn die Schweizer Banken untersagen in ihren Allgemeinen Geschäftsbedingungen (AGB) den Kunden, ihre PIN und Transaktionsnummer an Externe weiterzugeben.

EU verbessert Kundenschutz

Ganz andere Wege geht die EU mit der PSD2. Die Banken werden darin ausdrücklich verpflichtet, den Dritten Zahlungsdienstleistern den Zugang zu den Konten zu gewähren, falls die Kunden dies wünschen. Allerdings muss das über eine separate Schnittstelle geschehen, denn das Screen Scraping wird in der EU nach einer Übergangsfrist verboten. Zudem werden die Banken allgemein zur Kooperation mit den neuen Zahlungsdienstleistern verpflichtet: So müssen Überweisungen, die per Zahlungsauslösedienste angestossen werden, gleich schnell und zu denselben Kosten ausgeführt werden, wie wenn sie von der Bank selbst vorgenommen werden. Gemäss Richtlinie muss die Bank auch dann mit dem Zahlungsauslösedienst kooperieren, wenn kein Vertrag zwischen den beiden besteht. Das bedeutet, dass die Banken diesen Zugang unentgeltlich zur Verfügung stellen müssen. Das Trittbrettfahren von Dritten Zahlungsdienstleistern wird also bewusst gefördert.

KEYSTONE

Wer in der Schweiz Zahlungsdienstleistungen von Nichtbanken nutzt, trägt die Verantwortung bei Hackerangriffen selber.

Die EU erhofft sich davon einen verstärkten Wettbewerb auf dem Markt der Zahlungsdienste. Für die Dritten Zahlungsdienstleister ist die forcierte Marktöffnung allerdings mit dem Preis einer Regulierung verbunden: Sie benötigen eine Lizenz, und es gilt für sie ein umfangreiches Pflichtenheft bezüglich Datenschutz und Datensicherheit.

In der Schweiz werden die Drittanbieter hingegen nicht reguliert. Konkret bedeutet das, dass diese Dienstleister nach wie vor das Screen Scraping betreiben dürfen und die Kunden das volle Risiko für Fehlvorgänge tragen.

Unbefugter Zugriff auf Bankkonten

Auch beim heute wohl grössten Risiko im elektronischen Massenzahlungsverkehr, den Hackerangriffen, geht die EU andere Wege als die Schweiz. So verpflichtet die PSD2 die Banken im Zusammenhang mit elektronischen Zahlungsvorgängen regulatorisch zu einer sogenannten starken Kundenauthentifizierung. Das bedeutet, dass die persönlichen Legitimationsmittel aus mindestens zwei unabhängigen Authentifizierungselementen bestehen müssen und der Zahlungsvorgang dynamisch mit der Überweisungssumme und dem Zahlungsempfänger verknüpft sein muss. Die Freigabe eines Online-Zahlungsvorgangs, der beispielsweise per PIN und Transaktionsnummer am Computer ausgelöst wird, kann nur erfolgen, wenn die Kundin zusätzlich einen weiteren Code auf einem unabhängigen Gerät, etwa einem Smartphone, erhält und mit diesem Code gleichzeitig mitgeteilt wird, an wen die Zahlung geht und welche Summe überwiesen werden soll. So werden typische Man-in-the-Middle-Attacken erkennbar.

Zudem werden die hohen Sicherheitsstandards in der EU nicht nur regulatorisch, sondern auch über die Haftungsverteilung durchgesetzt. Verlangt die Bank für die elektronische Zahlungsauslösung keine starke Kundenauthentifizierung, muss sie den unbefugt abgezogenen Betrag auch dann ersetzen, wenn die Kundin sich im Umgang mit ihren persönlichen Legitimationsmitteln grob fahrlässig verhalten hat. Nur gerade bei betrügerischer Absicht kann die Bank also das Risiko einer unautorisierten Transaktion auf die Kundin abwälzen. Darüber hinaus begrenzt die EU das Risiko der Kunden selbst bei einem starken Kundenauthentifizierungsverfahren auf 50 Euro, wenn diese leicht fahrlässig gehandelt haben. Allerdings sollten solche Konstellationen nach Einführung der starken Kundenauthentifizierung nicht mehr vorkommen. Denn: Wer trotz Angabe des Zahlungsempfängers und des Überweisungsbetrags eine unbefugte Zahlung freigibt, muss sich grobe Fahrlässigkeit vorhalten lassen.

Anders in der Schweiz: Zwar hat sich auch hier die 2-Faktoren-Authentifizierung mit PIN und Transaktionsnummer etabliert, aber die wenigsten Finanzinstitute bieten eine starke Kundenauthentifizierung nach dem EU-Muster an. Zudem sehen die AGB der Schweizer Banken vor, dass eine Zahlung immer dann als autorisiert gilt, wenn sie unter Verwendung der personalisierten Legitimationsmittel erfolgt. Das Risiko für Hackerangriffe trägt also uneingeschränkt die Kundin. Ob eine solche vertragliche Ausgestaltung der Risikoverteilung privatrechtlich zulässig ist, ist fraglich. Aber sie ist in den AGB so geregelt, und die betrogenen Kunden müssten ihre Rechte erst durch alle Instanzen klagen. Zwar mögen die Banken sich – gerade im Fall von breit angelegten Hackerangriffen – kulant zeigen. Kulanz ist aber aus Kundensicht kein nachhaltiges Lösungsmodell.

Schweizer Banken gegen Regulierung

Die EU hat auf die Innovationen und die erhöhten Risiken im Zahlungsverkehr reagiert und mit der PSD2 klare Entscheidungen getroffen. Sie öffnet den Markt für ausgewählte neue Zahlungsdienstleister und fördert durch den zunehmenden Wettbewerb, dass die Wertschöpfung im Zahlungsverkehr auch Drittanbietern offensteht. Gleichzeitig verlangt sie hohe Sicherheitsstandards und erweitert den Kundenschutz.

In der Schweiz hat sich die Bankiervereinigung in einem Positionspapier vom September 2017 gegen eine entsprechende schweizerische Regulierung ausgesprochen. Die Kritik richtet sich insbesondere gegen den regulatorischen Zwang zur Marktöffnung für die Konkurrenz aus dem Nichtbankensektor. Gemäss der Bankiervereinigung stellt dieser einen unnötigen Eingriff in einen funktionierenden Markt dar. Zudem sei die Öffnung aus Sicherheitsgründen bedenklich, und die Kunden müssten die damit verbundenen Kosten tragen.

Die PSD2 ist keine leicht verdauliche Regulierungskost. Sie hat aber den Vorteil, dass die neuen Anbieter von Zahlungsdiensten in die Regulierung eingebunden sind. Das schafft für die Nutzer von Zahlungsdiensten mehr Sicherheit. Mittelfristig ist es unvermeidbar, dass man für diesen Sektor regulatorische Eckpunkte setzt. Dann wird man allerdings auch die Frage eines regulatorisch vorgegebenen Open Banking erneut diskutieren müssen, bei dem auch Drittanbieter Zugang zum Markt für Zahlungsdienstleister haben.

Susan Emmenegger
Professorin für Privat- und Bankrecht und Direktorin des Instituts für Bankrecht, Universität Bern