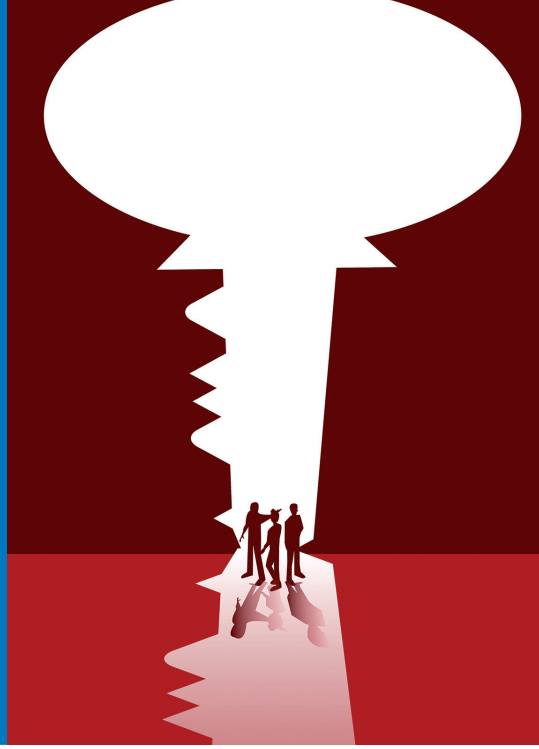
Keine neuen **Risiken** durch die **PSD2**



Von Thomas Büttner und Stefan Roßbach

Die Frage, ob durch die Schnittstellen zu Zahlungskonten ihrer Kunden, die Banken gemäß der PSD2 für Drittanbieter schaffen müssen, neue Risiken für Datenschutz und Datensicherheit entstehen, beantworten Thomas Büttner und Stefan Roßbach mit nein. Denn erstmals müssen dann auch Drittanbieter Angaben zu ihrer Sicherheitsstrategie machen und bestimmte Vorschriften erfüllen. Für Banken ist es nach Einschätzung der Autoren deshalb jetzt an der Zeit, die PSD2 als Chance zu sehen und die vorhandenen Daten für neue Dienste und Services zu nutzen. Red.

Die Umsetzung der Anforderungen, die aus der novellierten Zahlungsdiensterichtlinie PSD2[1)] folgen, beschäftigt derzeit die gesamte europäische Finanzbranche. Mit Umsetzung dieser Richtlinie, die für Januar 2018 geplant ist, werden Drittanbieter Zugang zu online geführten Zahlungskonten von Bankkunden haben. Die kontoführenden Institute können sich dem nicht verwehren und müssen zudem auch noch die hierfür erforderliche Schnittstelle entwickeln und bereitstellen. Mehr Wettbewerb soll sich innovationsfördernd auf die Digitalisierung des Finanzmarktes auswirken. Doch zwangsläufig stellt sich auch die Frage, ob dadurch neue Risiken in Sachen Datenschutz und Datensicherheit entstehen.

Die vertragliche Beziehung zwischen Online-Banking-Kunden und ihrer Bank sieht bisher keine Einbeziehung Dritter vor. Banken regeln über ihre Online-Banking-Bedingungen, denen die Kunden zustimmen müssen, genau, wie sich die Kontoinhaber bei Nutzung des Online-Bankings authentifizieren und Zahlungen autorisieren. Der Zugriff muss immer direkt über die durch die Bank bereitgestellten Online-Banking-Systeme und Mobile-Banking-Apps beziehungsweise bei Einsatz einer Banking-Software über die FinTS (HBCI) Schnittstelle erfolgen. Nur so kann sichergestellt werden, dass kein Dritter unberechtigt in den Besitz der Zugangsdaten kommt und somit Zahlungskonten ausspähen und Transaktionen ohne Erlaubnis des Kunden durchführen könnte.

Neue Risiken durch Fintechs

In den vergangenen Jahren wurden jedoch immer mehr Drittanbieter beziehungsweise Fintechs gegründet, deren Geschäftsmodelle im Wesentlichen darauf basieren, Banking für die Kunden einfacher, schneller und attraktiver zu gestalten[2)]. Sie führen beispielsweise E-Commerce-Zahlungen im Auftrag der Kunden aus, rufen Salden und Umsätze von Konten unterschiedlicher Banken ab, um diese in modernen Multibanking Apps für ein Haushaltsbuch („Personal Finance Manager") zusammenzuführen, oder erleichtern den digitalen Kontowechsel.

Zur möglichst einfachen Nutzung dieser Services ist es jedoch zwangsläufig notwendig, die Online-Banking-Zugangsdaten und teilweise auch Authentifizierungsinstrumente (TANs) auf Eingabemasken der Drittanbieter einzugeben, die diese im Hintergrund an die Bank übermitteln, um die Aufträge auszuführen.

Dies führte plötzlich zu ungeahnten Risiken. Es schaltet sich – wie eigentlich bislang nur beim Online-Betrug mittels „Man-in-the-Middle"- Angriff bekannt – ein vom Kunden offiziell beauftragtes System dazwischen und greift auf Konto und Kontoinformationen zu. Bei der Weitergabe ihrer Zugangsdaten besteht so die Gefahr, dass Kunden zu fahrlässig agieren. Sie sind sich häufig nicht der möglichen Folgen und Risiken bewusst.

Zu den Autoren

Thomas Büttner, Senior Consultant, **Stefan Roßbach**, Managing Director, beide TME AG, Frankfurt am Main

Drittanbieter bislang nicht kontrolliert

Während Banken die Sicherheit ihrer bereitgestellten Online-Banking-Systeme und -Prozesse auf Basis regulatorischer Vorgaben zur Sicherheit von Internetzahlungen

(MaSi[3]) gewährleisten müssen und von der BaFin kontrolliert werden, gibt es für Drittanbieter bislang keine Gesetzgebung über den notwendigen Schutz und die Sicherheit ihrer Infrastruktur. Zwar werben diese Anbieter wie Banken damit, dass die marktüblichen Datenschutzstandards eingehalten werden, sowie teilweise auch mit der Abnahme und Zertifizierung durch bekannte Prüfgesellschaften – aber staatlich kontrolliert wird das bislang nicht. Der Kunde muss bis heute bei jedem einzelnen Anbieter überlegen, ob er diesem genügend vertraut oder nicht. Da er selbstverständlich nicht jedes Unternehmen kennt, schreckt so mancher sicher davor zurück, auf Dienste von Drittanbietern zurückzugreifen.

Neue Kontodienstleistungen für Kunden ab 2018 [4]

Um hier endlich Klarheit zu schaffen, hat sich schlussendlich die europäische Gesetzgebung mit den Veränderungen am Markt befasst und mit der PSD2 die Grundlage für einen sicheren Wettbewerb bei Finanzdienstleistungen in der Zukunft geschaffen.

Die novellierte Zahlungsdiensterichtlinie PSD2 sieht vor, dass kontoführende Finanzinstitute den sogenannten dritten Zahlungsdienstleistern aus der gesamten europäischen Union zukünftig den Zugang zu Bankdienstleistungen ermöglichen müssen. In Artikel 98 der PSD2 wird angekündigt, dass hierzu entsprechende technische Standards für eine sichere Authentifizierung und Kommunikation entwickelt werden sollen. Die EBA selbst stellt hier jedoch nur die Anforderungen. Die technische Spezifikation des Standards obliegt im Anschluss dem Markt.

Die EBA unterscheidet grundsätzlich zwischen drei verschiedenen Diensten für die sich ein Dritter zertifizieren lassen kann:

- Kontoinformationsdienst – zum Beispiel zum Abruf von Umsätzen des Zahlungskontos über eine Kontostands-App, Push Notifications bei Zahlungseingängen, Multibanking-Aggregation oder digitales Haushaltsbuch.

- Zahlungsauslösedienst – zum Beispiel zum Einreichen einer Zahlung beim E-Commerce Shopping.

- Deckungsabfragedienst – zum Beispiel beim Einsatz einer Karte eines Drittemittenten am Point of Sale (PoS).

Der Zugang zu all diesen Diensten muss grundsätzlich unentgeltlich zur Verfügung gestellt werden. Die zugehörige Schnittstelle hierfür ist durch das kontoführende Kreditinstitut bereitzustellen, das somit auch die Kosten für die Entwicklung trägt. Drittanbieter müssen sich lediglich zertifizieren lassen. Die PSD2 gilt dabei für alle Marktteilnehmer, also auch für solche Zahlungsauslöse- und Kontoinformationsdienste, die sich bereits am Markt etabliert haben. Sie müssen sich ebenfalls der neuen Regulierung unterwerfen, um weiterhin Zugriff auf die Kundenkonten zu erhalten.

Sicherheitsrelevante Anforderungen des Gesetzgebers[5]

Um als Drittanbieter am Markt aktiv werden zu können, braucht das interessierte Unternehmen eine erweiterte Erlaubnis durch die nationale Aufsichtsbehörde. In Erweiterung zum bisherigen Zulassungsantrag werden nun erstmalig auch wesentliche Unterlagen zur Sicherheitsstrategie des Anbieters gefordert. Die Dienstleister müssen unter anderem darlegen und angeben, wie sie

- mit Sicherheitsvorfällen und sicherheitsbezogenen Kundenbeschwerden umgehen,

- sensible Zahlungsdaten handhaben,

- die Geschäftsfortführung im Krisenfall sicherstellen und

- bestimmte statistische Daten erheben, etwa über Geschäftsvorgänge.

Je nach Ausgestaltung ihres Geschäftsmodells haben die Drittdienstleister besondere Vorschriften zu beachten, die den Zugang zum Zahlungskonto und zu den Kontoinformationen sowie deren Nutzung regeln. So müssen sie beispielsweise sicherstellen, dass die personalisierten Sicherheitsmerkmale, wie die Online-Banking-Zugangsdaten und TANs des Zahlungsdienstnutzers, also des Kunden, keiner anderen Partei als dem Nutzer und dem Herausgeber der personalisierten Sicherheitsmerkmale zugänglich sind. Die Übermittlung dieser Merkmale darf nur über sichere und effiziente Kanäle des Zahlungsauslöse- beziehungsweise Kontoinformationsdienstleisters erfolgen.

Zentraler Ansprechpartner im Missbrauchsfall bleibt die Bank

Die Banken unterrichten die Kunden zudem zukünftig über jeden erfolgten Zugriff und geben ihm die Möglichkeit, den Zugriff der Dienste über Blacklist und Whitelist genau zu regeln.

Die aktuell noch in der Entwurfsfassung vorliegenden Leitlinien zur Meldung von Zwischenfällen („Guidelines on major incidents reporting under the Payment Services Directive 2“) sehen vor, dass beteiligte Zahlungsdienstleister eine Meldepflicht haben. Sollte es trotz diverser Vorkehrungsmaßnahmen zu einem Datenmissbrauch kommen und wird dieser durch eine der beteiligten Parteien entdeckt, ist die zuständige Aufsichtsbehörde unverzüglich darüber in Kenntnis zu setzen sowie während der gesamten Aufarbeitung des Falls immer wieder darüber zu informieren.

Entstehen dem Kunden finanzielle Schäden aus dem Missbrauch seiner Daten, sind die Drittanbieter über eine Versicherung, die als notwendiger Bestandteil zur Zertifizierung gefordert wird, abgesichert. Der Vorteil für den Kunden hierbei ist, dass der zentrale Ansprechpartner in allen Fällen seine Bank ist.

Auf der einen Seite stehen also die Fintechs. Haben sie sich mit ihren Geschäftsmodellen bislang teilweise in einer Grauzone bewegt, bekommen sie durch die PSD2 nun die rechtlich saubere Basis für ihre Kontodienstleistungen. Auf der anderen Seite profitieren Banken von der neuen Regelung. Um die sich bietenden Chancen zu nutzen, sollten sie schnell und konsequent handeln, da sonst die Gefahr besteht, immer mehr nur Datenlieferant zu sein, statt selbst Geschäft mit den Kunden zu machen.

PSD2 als Chance sehen

Banken haben mit Inkrafttreten von PSD2 die Option, die Umsatzdaten von Fremdbankkonten ihrer Kunden in die eigenen Prozesse und Dienste zu integrieren. Das erleichtert es ihnen, etwa vor einer Kreditvergabe die Bonität des potenziellen Empfängers zu prüfen. Auch eröffnen sich dank aussagefähigerer Daten neue Möglichkeiten, die Kunden bei ihrer Finanzplanung besser zu unterstützen. All das wird selbstverständlich nur mit dem Einverständnis des Kunden umsetzbar sein, doch dieses Einverständnis brauchen auch die Drittanbieter, wollen sie ihre Leistungen an den Mann beziehungsweise die Frau bringen.

Banken können zudem künftig genau unterscheiden, ob der Kunde direkt oder über Dritte auf sein Konto zugreift. Falls der Zugriff über Dritte erfolgt, sind diese dann den einheitlichen Regulierungen zu Datenschutz und Datensicherheit unterworfen. Das bedeutet für die Drittanbieter zwar Aufwand, aber erhöht auch ihre Vertrauenswürdigkeit. Es dürfte sich also positiv auf die Bindung bestehender und vor allem die Akquise neuer Kunden auswirken.

Zu guter Letzt profitieren natürlich auch die Online-Banking-Kunden selbst von der neuen Richtlinie. Erstmalig können sie sich tatsächlich sicher sein, dass von ihnen beauftragte Drittanbieter einer staatlichen Kontrolle unterzogen wurden und nur exakt die Information über die Schnittstelle bekommen, die sie zur Auftragsausführung benötigen. Man darf also gespannt sein, welche neuen Geschäftsmodelle und Services künftig noch auf den Markt kommen werden.

Die EBA erhofft sich durch die zukünftige Regelung mehr Transparenz und Wettbewerb im digitalen Finanzmarkt, was mit der PSD2 durchaus gelingen kann. Dort, wo Geschäftsmodelle heute auf wackeligen Füßen standen, kommt mit der PSD2 ein stabiles Fundament für die Zukunft. Es wird für Dritte nun möglich sein, noch mehr Vertrauen beim Kunden zu erwecken. Die Hoheit über sein Konto und über seine Daten besitzt jedoch weiterhin der Kunde. Er wird auch künftig derjenige sein, der entscheidet, wann und wie auf sein Online-Zahlungskonto zugegriffen wird.

Mehr Sicherheit für alle Beteiligten

Neben der im Januar 2016 in Kraft getretenen PSD2 gibt es noch mehrere Zusatzdokumente, sogenannte Regulatory Technical Standards (kurz RTS), mit deren Erstellung sich der Gesetzgeber derzeit noch befasst und in einer Konsultationsphase Feedback vom Markt einholt. Über 260 Vertreter von Banken, Fintechs, Zahlungsdienstleistern, Verbänden und anderer Marktteilnehmer haben sich zum Beispiel zum Entwurf der „Regulatory Technical Standards on strong customer authentication and secure communication" geäußert.

Parallel zur Diskussion der RTS entwirft das Bundesministerium für Finanzen aktuell ein deutsches Umsetzungsgesetz, das die nationale Realisierung der PSD2 regelt. Was auf den ersten Blick nach viel Regulatorik aussieht, verfolgt letztendlich nur einen Zweck: mehr Wettbewerb bei gleichzeitiger Gewährleistung eines Höchstmaßes an Datenschutz und Datensicherheit.

Fußnoten

1) Payment Service Directive 2
2) Vgl. erschienene TME Publikationen „Innovative Geschäftsmodelle im Banking" und „Innovative Geschäftsmodelle im Digital Wealth Management" (https://www.tme-ag.de/publikationen/tme-factbooks/)
3) Mindestanforderungen an die Sicherheit von Internetzahlungen (MaSI) Veröffentlicht mit BaFin-Rundschreiben Nr. 4/2015 vom 5. Mai 2015
4) Auszug aus dem TME Whitepaper „Mehr digitaler Wettbewerb bei Banken und Finanzdienstleistern durch PSD2 – Wichtige Details zur Kontoschnittstelle lassen noch auf sich warten", vom 22. Dezember 2016
5) Vgl.: BaFin Journal: Zweite Zahlungsdiensterichtlinie: Neue europäische Vorschriften für Zahlungsdienstleister, 15. März 2016