FÜR MEHR SICHERHEIT UND VERLÄSSLICHKEIT IM ZAHLUNGSVERKEHR

vzbv fordert in der EU-Konsultation zur Zweiten Zahlungsdiensterichtlinie besseren Verbraucherschutz

20. Juli 2022

1. Einleitung

Die Zweite Zahlungsdiensterichtlinie (Revised Payment Services Directive 2 = PSD2) setzt wichtige Regeln für den elektronischen Zahlungsverkehr. Ihre Umsetzung haben Verbraucher:innen am deutlichsten an den neuen Sicherheitsverfahren, der sogenannten Starken Kundenauthentifizierung (Strong Customer Authentication = SCA) gespürt, die seit Herbst 2019 im Online-Banking und für digitale Bezahldienste sowie, mit etwas Verzögerung, auch für Kreditkarten gelten. Die Starke Kundenauthentifizierung hat damit insbesondere die alten Papier-TAN-Listen abgelöst.

Daneben reguliert die PSD2 neuartige Zahlungsdienste, wie Zahlungsauslöse- und Kontoinformationsdienste und macht Vorgaben zur europaweiten Aufsicht über Zahlungsdienstleister.

Derzeit evaluiert die Europäische Kommission den Rechtsakt und hat dazu eine Experten-Konsultation durchgeführt. Es wird erwartet, dass die Europäische Kommission im kommenden Jahr auf Grundlage der Evaluierung einen Vorschlag für eine überarbeitete Zahlungsdiensterichtlinie vorlegen wird.

> Der vzbv sieht Verbesserungsbedarf und fordert:
> 1.) Konten und Zugänge müssen besser geschützt werden.
> 2.) Die Privatsphäre der Verbraucher:innen muss sichergestellt werden.
> 3.) Verbraucher:innen, die kein Smartphone für Bankgeschäfte verwenden wollen oder können, dürfen nicht vom Zahlungsverkehr ausgeschlossen werden.
> 4.) Aufsichtsbehörden müssen besser aufgestellt werden und sowohl grenzüberschreitend als auch behördenübergreifend eng zusammenarbeiten, um Missstände am Markt zu beseitigen.

2. Haftung

Die PSD2 sieht vor, dass Zahlungsdienstleister (Banken, Sparkassen, Kreditkartenanbieter, E-Payment-Anbieter, usw.) für Schäden aufkommen müssen, wenn Kundengelder zum Beispiel durch Kartendiebstahl oder Phishing-Attacken gestohlen werden. In der Praxis gelingt es Anbietern in bestimmten Fällen jedoch, dies zu

umgehen. Verbraucher:innen bleiben auf dem Schaden sitzen, weil ihr Verhalten häufig als grob fährlässig eingestuft wird. Gerichte legen hier unterschiedliche, teils sehr strenge Maßstäbe an. Und dies trotz der Tatsache, dass auch größte Vorsicht inzwischen nicht mehr vollständig vor Phishing-Angriffen schützt und auch die Institute durch geeignete Maßnahmen fähig und verpflichtet sind, solche Angriffe zu vermeiden, sodass ein erfolgter Angriff selten ausschließlich auf das Versagen von Verbraucher:innen zurückzuführen ist. Die gesetzlich vorgeschriebene Pflicht, den entstandenen Schaden schnellstmöglich zu erstatten, wird von den Instituten häufig umgangen, indem sie grobe Fahrlässigkeit unterstellen. Die Banken behaupten damit, sie hätten einen Anspruch gegen die Kund:innen, weil diese selbst für Schäden aufkommen müssten, die auf einer solchen groben Fahrlässigkeit beruhen. Diesen Anspruch stellen sie dem Anspruch der Verbraucher:innen gegenüber und verweigern die Erstattung des Betrags, da die Verbraucher:innen dem Institut zum Ausgleich verpflichtet seien. Obwohl die grobe Fahrlässigkeit also nur von der Bank oder Sparkasse behauptet wird, jedoch nicht gerichtlich geklärt ist, erhalten Verbraucher:innen dennoch keine Entschädigung. So lassen es Kreditinstitute immer wieder darauf ankommen, ob Verbraucher:innen den potenziell langwierigen und kostspieligen Weg gehen, ihren Anspruch auf Erstattung einklagen zu müssen, statt den Betrag innerhalb der gesetzlich vorgesehenen Frist gutgeschrieben zu bekommen

> Eine Revision der Zahlungsdiensterichtlinie sollte sicherstellen, dass Verbraucher:innen darauf vertrauen können, dass sie nicht haften, wenn ihr Geld gestohlen wird. Dazu muss geklärt werden, dass nur offenkundig grob fahrlässiges Verhalten zur Mithaftung führen kann und dass Zahlungsdienstleister Kundengelder zunächst sofort erstatten müssen. Eine Aufrechnung von behaupteten Gegenansprüchen darf nicht eingesetzt werden, um die unmittelbare Kompensation zu umgehen.

3. Starke Kundenauthentifizierung und finanzielle Inklusion

Die mit der PSD2 eingeführte Starke Kundenauthentifizierung (Strong Customer Authentication = SCA) hat den elektronischen Zahlungsverkehr sicherer gemacht. Insbesondere bedeutete sie das Ende der betrugsanfälligen Papier-TAN-Listen.

Allerdings haben die neuen Vorgaben auch Nachteile. Einerseits erfordert die SCA die Einrichtung neuer Sicherheitsverfahren. Im Zuge der Einführung kontaktierten Zahlungsdienstleister Verbraucher:innen mithilfe von Briefen, Mails und Browser-Benachrichtigungen. Erprobte Faustregeln zur Sicherheit im Online-Banking, nach denen sich die Hausbank beispielsweise niemals per Mail meldet, galten nicht länger. Wer eine Mail wegen Phishing-Verdachts nicht öffnete, konnte im schlimmsten Fall kurzfristig den Kontozugang verlieren. Andere wurden ohne Faustregeln und angesichts der unübersichtlichen Lage Opfer von Phishing-Angriffen durch Kriminelle, die sich die Umstellung mit fingierten Mails zur SCA-Einführung zu Nutze machten.

Zudem nimmt mit der Starken Kundenauthentifizierung die Komplexität zu. Da die Vorgaben technologieoffen angelegt sind, nutzen Zahlungsdienstleister unter-

schiedliche Methoden. Jedes Konto erfordert ein eigenes Authentisierungsverfahren und die SCA-Methode kann sich für jedes Bankkonto unterscheiden. Dies erschwert gerade das Multibanking, also das Verwalten mehrerer Konten über eine App, das die PSD2 eigentlich befördern wollte.
Im Ergebnis machte die Starke Kundenauthentifizierung das Verwalten der eigenen Finanzen aufwändiger.

Manche Verbraucher:innen drohen durch die PSD2 den Zugang zum elektronischen Zahlungsverkehr gänzlich zu verlieren. Kreditinstitute setzen zunehmend auf App-Lösungen. Wer kein aktuelles Smartphone besitzt oder dieses nicht fürs Online-Banking einsetzen kann oder dies zum Beispiel aus Sicherheitsgründen nicht will, kann das Online-Banking entweder nicht nutzen oder ist auf eigens zu bezahlende Geräte wie TAN-Generatoren angewiesen.
Der mögliche Einwand „Wer Online-Banking nutzt, hat auch ein Smartphone“ geht dabei an der Lebensrealität vieler Verbraucher:innen vorbei, die teilweise seit Jahrzehnten Online-Banking am PC betreiben, die ihre Bankgeschäfte jedoch nicht übers Smartphone tätigen wollen oder können.

> Verbraucher:innen sollten grundsätzlich das Recht haben, eine nicht-Smartphone-basierte Methode zur starken Kundenauthentifizierung verwenden zu können.

4. Kontoinformationsdienste und Datenschutz

Durch die PSD2 wurde es Drittanbietern erleichtert, Zugang zu Zahlungskonten zu erhalten. Dies sollte mehr Wettbewerb ermöglichen. Neben den Zahlungsauslösediensten, die in Deutschland auch vor der PSD2 bekannt waren, wurden Kontoinformationsdienste reguliert, die den Zugriff auf Kontoumsätze ermöglichen. Diese ermöglichen Einblicke in die Privatsphäre, wie die Parteizugehörigkeit, Gewerkschaftsmitgliedschaft oder die sexuelle Orientierung. Hierbei mangelt es jedoch an konkreten Vorgaben, die sicherstellen, dass Abruf und Verarbeitung der Daten im Einklang mit der Datenschutzgrundverordnung erfolgen. Der vzbv hat in einer jüngsten Untersuchung Defizite bei Kontoinformationsdiensten festgestellt[1].

> Die künftige Regulierung von Kontoinformationsdiensten und anderen datenbasierten Finanzdienstleistungen sollte sich an den Leitlinien des Europäischen Datenschutzausschusses[2] orientieren. Insbesondere sollten nur die für eine Dienstleistung erforderlichen Datenkategorien abgerufen werden, um dem Datensparsamkeitsprinzip, das in der DSGVO verankert ist, gerecht zu werden.

[1] Verbraucherzentrale Bundesverband: Mängel bei Kontoinformationsdiensten beheben, 2022, https://www.vzbv.de/pressemitteilungen/maengel-bei-kontoinformationsdiensten-beheben, 18.07.2022
[2] Europäischer Datenschutzausschuss: Leitlinien 06/2020 zum Zusammenspiel zwischen der zweiten Zahlungsdiensterichtlinie und der DSGVO, 2020, https://edpb.europa.eu/system/files/2021-06/edpb_guidelines_202006_psd2_afterpublicconsultation_de.pdf, 18.07.2022

5. Aufsicht

Die Aufsicht muss besser aufgestellt sein und sowohl grenzüberschreitend als auch behördenübergreifend eng zusammenarbeiten. Doch an beidem hapert es.

Dass es für Zahlungsdienstleister möglich ist, mit nur einer Lizenz aus einem Mitgliedsstaat im gesamten Gebiet der Europäischen Union Zahlungsdienste anzubieten, darf für Verbraucher:innen keinen Nachteil darstellen. Dazu muss insbesondere die grenzüberschreitende Zusammenarbeit der Aufsichtsbehörden verschiedener Mitgliedsstaaten gut funktionieren. Verbraucher:innen müssen in der Lage sein, ohne lange Nachforschungen zum Unternehmenssitz, unkompliziert und in ihrer Landessprache Beschwerde gegen einen Zahlungsdienstleister zu erheben. Die Ermittlung der für Untersuchungen und Sanktionen zuständigen Aufsichtsbehörde und Weiterleitung der Beschwerde an diese muss durch die Aufsichtsbehörden untereinander erfolgen.

Auch eine Zusammenarbeit zwischen Finanz- und Datenschutzaufsicht ist aus Verbraucherperspektive unerlässlich. Die Datenschutzaufsicht hat neben der Expertise auf diesem Gebiet auch allein die Kompetenz zum Verhängen von Bußgeldern nach der Datenschutzgrundverordnung, während die Finanzaufsicht durch ihre Befugnis zur laufenden Kontrolle von Finanzinstituten die tiefsten Einblicke erhält und außerdem bei der Lizenzierung auch Datenschutzprozesse untersucht. Diese Kompetenzen stehen nicht in Abgrenzung zueinander, sondern in gegenseitiger Ergänzung. Eine enge Zusammenarbeit der Aufsichtsbehörden ist unerlässlich für starken Datenschutz im Finanzbereich.

> Verbraucher:innen müssen darauf vertrauen können, dass Zahlungsdienstleister in allen Mitgliedsstaaten und in allen Tätigkeitsbereichen wirksam und streng beaufsichtigt werden. Dazu bedarf es eines Behördennetzwerks, das sowohl staatenübergreifend als auch mit Aufsichtsbehörden anderer Sachgebiete eng verzahnt zusammenarbeitet.

Kontakt

Verbraucherzentrale
Bundesverband e.V.

Team
Finanzmarkt

Rudi-Dutschke-Straße 17
10969 Berlin

finanzen@vzbv.de

Der Verbraucherzentrale Bundesverband e.V.
ist im Deutschen Lobbyregister registriert.
Sie erreichen den entsprechenden Eintrag hier.