SICHER DIGITAL BEZAHLEN – OHNE KONTROLLVERLUST?

Rede von Klaus Müller, Vorstand des Verbraucherzentrale Bundesverbands (vzbv), am 29.01.2019 im Rahmen des Safer Internet Day 2019 in Berlin

[Es gilt das gesprochene Wort]

Sehr geehrte Damen und Herren,

ich habe jetzt die ehrenvolle Aufgabe, Sie aus Ihrem Mittagstief zu holen. Wir haben heute Vormittag schon viel über digitale Bezahlmöglichkeiten gehört. Ich möchte Ihnen nun in den nächsten Minuten die Chancen aufzeigen, die digitale Bezahlmöglichkeiten für Verbraucherinnen und Verbraucher bieten. Ich wäre aber nicht der Vorstand des Verbraucherzentrale Bundesverbandes, wenn ich nicht auch auf die Risiken aufmerksam mache. Dabei denke ich vor allem an die Folgen, die es haben kann, wenn man sich von einzelnen Technologien abhängig macht. Und ich frage mich – haben wir bei digitalen Bezahlmöglichkeiten die Chance die Kontrolle über unsere Daten zu behalten?

Meine Damen und Herren,

ich gehe noch einmal kurz zurück – worüber reden wir hier heute eigentlich?

Die Deutschen lieben ihr Bargeld. Nach wie vor werden 74 Prozent aller Zahlungsvorgänge in Geschäften in bar getätigt.[1] Und wenn die Verbraucherinnen und Verbraucher nicht bar bezahlen, dann zücken sie ihre Karte. Die Möglichkeit, mit dem Handy etwas im Geschäft zu bezahlen, kennen bereits fast 2/3 der Verbraucher, genutzt haben es aber nur 2 Prozent.[2] Wenn man mit dem Smartphone zahlen möchte, dann wollen die Mehrheit der Verbraucherinnen und Verbraucher das zur Zahlung von Fahrkarten (17 Prozent) - aber 44 Prozent der Befragten bleibt dabei: sie möchten *NIE* mit dem Smartphone zahlen.[3] Bei Apps zum Empfangen und Versenden von Geld sieht es ähnlich aus. Das kannten 2017 nur knapp etwas mehr als die Hälfte der Verbraucher, genutzt haben es 5 Prozent.[4] Gleichwohl steigen aber E-Geldzahlungen in der Gunst der Verbraucherinnen und Verbraucher. Geht es um Zahlungen im Internet ist hier PayPal ganz vorne.[5] Wir reden hier also insgesamt immer noch von einem Nischenthema – zumindest in Deutschland.

---

[1] https://www.bundesbank.de/de/zahlungsverhalten

[2] https://www.bundesbank.de/de/zahlungsverhalten

[3] Befragung November/Dezember 2017 durch Statista (Global Consumer Survey)

[4] https://www.bundesbank.de/de/zahlungsverhalten

[5] https://www.bundesbank.de/resource/blob/634056/8e22ddcd69de76ff40078b31119704db/mL/zahlungsverhalten-in-deutschland-2017-data.pdf

Vielleicht ändert sich das bald. Apple ist Ende letzten Jahres mit seinem Bezahldienst Apple Pay in Deutschland gestartet und hat auf Anhieb zehntausende Kunden gefunden, die mit ihrem Smartphone oder ihrer Smartwatch jetzt im Supermarkt bezahlen.[6]

Dass die Karte bis heute am meisten zur unbaren Zahlung eingesetzt wird, kann ich gut nachvollziehen. Anders als ein Smartphone geht sie nicht gleich kaputt, wenn sie mal runterfällt. Und Karten hat heute auch immer jeder in seinem Portemonnaie dabei. Zudem behaupte ich mal, dass Karten auch weniger störanfällig sind. Sie sind in der Regel ein verlässlicher Begleiter mit festem Platz im Portemonnaie. Bei virtuellen Zahlungskarten in Banking-Apps ist das noch ganz anders. Eine Bekannte hat sich im letzten Schweden-Urlaub allein auf ihre Banking-App als Zahlungsmittel verlassen, Nach einem Software-Update ging in der App nur leider gar nichts mehr[7] und so stand sie quasi ohne Geld da. Das ist mehr als nur ärgerlich – sie wird diesen Urlaub wohl so schnell nicht vergessen.

Wie wir heute Vormittag gehört haben, sind bereits einige Angebote um digital zu Bezahlen auf dem Markt – die Verbraucherinnen und Verbraucher bevorzugen aber weiterhin bereits vorhandene Zahlungsmittel wir Geldscheine oder Karten.

Meine Damen und Herren, ich frage mich: Woran liegt das? Woher rührt die Skepsis der Verbraucherinnen und Verbraucher?

Meine Kolleginnen und Kollegen vom Marktwächter Digitale Welt haben 2017 elektronische Bezahlverfahren einmal unter die Lupe genommen.[8] Die Untersuchung zeigt im Kern das, was wir in ähnlicher Form auch in anderen Märkten sehen: Die Verbraucherinnen und Verbraucher sorgen sich um den Schutz und die Sicherheit ihrer persönlichen Daten.

Diejenigen, die digitale Zahlverfahren gar nicht nutzen, gaben an, die Verfahren seien ihnen zu unsicher oder sie wollen keine persönlichen Daten offenlegen.

Auch diejenigen, die sie nutzen haben Vorbehalte. Ein Drittel würde die elektronischen Bezahldienstleister nicht mehr nutzen, wenn die Daten für individualisierte Preise und Werbung weitergegeben werden würde. 30 Prozent würden die Dienste nicht mehr nutzen, wenn mit den Daten ein Einkaufsprofil erzeugt würde.

Die Untersuchung einzelner elektronischer Bezahlverfahren hat auch gezeigt, dass sich die Verbraucherinnen und Verbraucher zu Recht Sorgen machen.

Erstens: Es werden mehr Daten erhoben als für den Dienst notwendig: Die Anbieter agieren überwiegend nicht „datensparsam“. Sie erheben zusätzliche Daten, die zur Abwicklung des reinen Online-Kaufes oder zur Einhaltung von Sicherheitsaspekten nicht notwendig sind.

---

[6] https://www.sueddeutsche.de/digital/apple-pay-deutschland-1.4285581

[7] Betraf 2018 einige Anwendungen wie Postbank Finanzassistenten nach Android 8 Update, längere Zeit keine Funktionalität der hinterlegten Karte mehr möglich. Kann man auch in den Bewertungen der Apps nachlesen. Antwort der Postbank: „Es tut uns leid, dass wir das Mobile Bezahlen aktuell unter Android 8 nicht gewährleisten können. Wir arbeiten aktuell an einer Lösung des Problems und werden uns an dieser Stelle wieder melden, sobald es etwas Neues gibt!“

[8] https://www.marktwaechter.de/sites/default/files/downloads/17-11-14_untersuchungsbericht_e-payment.pdf

Zweitens: Nutzer können mit Hilfe bestehender Datenschutzerklärungen nicht erkennen, was mit ihren Daten geschieht. Im Fall von PayPal benötigt man beispielsweise ca. 24 Minuten zum Lesen der Datenschutzerklärung. Dabei noch nicht berücksichtigt: die 48-seitige Aufzählung Dritter, an die Daten weitergeleitet werden.

Drittens: Verbraucher wünschen sich etwas anderes, als die Realität widerspiegelt: Verbraucher wollen kurze, einseitige Datenschutzerklärungen, die innerhalb von fünf Minuten lesbar sind, und ein Format mit aktiver Wahl bzw. Abwahl von Einzeldaten durch die Nutzer. Hinsichtlich der Datenpreisgabe besteht der Wunsch, so wenig wie möglich Daten preiszugeben bzw. nur solche, die tatsächlich für die Ausführung des Dienstes notwendig sind.

Viertens: Das Sicherheitsniveau der untersuchten elektronischen Bezahldienstleister ist gemessen an allgemeinen Web-Anwendungen hoch. Bei Phishing-Attacken gibt es jedoch keinen durchgängig wirksamen Schutz.

Wenn ich jetzt auch noch ein paar Wochen zurück blicke: Da werden tausende persönliche Daten von Politikern und Prominenten gehackt und ins Netz gestellt. Letzte Woche wird dann ein weiterer riesiger Datendiebstahl aufgedeckt: 773 Millionen E-Mail-Adressen, 87 Gigabyte an Daten und 21 Millionen im Klartext lesbare Passwörter.

Das verunsichert Verbraucherinnen und Verbraucher nicht nur – das hält sie schlicht davon ab digitale Anwendungen zu nutzen. Geht es dann noch um ihr Geld, muss das Vertrauen in die digitalen Anwendungen erst recht hoch sein.

Meine Damen und Herren: Es muss dringend was passieren, damit das verloren gegangene Vertrauen der Verbraucherinnen und Verbraucher zurückgewonnen wird.

Die Schlüsselwörter sind Datenschutz und Datensicherheit! Das Datenschutz und Datensicherheit von Teilen der Politik in der Vergangenheit oftmals als sicherheitspolitische und wirtschaftliche Hindernisse diskreditiert wurden, muss endlich ein Ende haben.

Datenschutzbedenken lassen sich nur auflösen, wenn Verbraucherinnen und Verbraucher Gewissheit haben, dass sie mit einem Zahlungsmittel nicht gleichzeitig auch ihre Daten für weitere Verwendungen freigeben. Sie wollen nicht für alles was sie zahlen dann auch die passende Werbung immer und überall bekommen. Zudem sagen Zahlungsdaten wirklich viel über Verbraucher aus und können besonders gut zur individuellen Preisbildung verwendet werden. Das würde den Wettbewerb durch Preisvergleich für alle Verbraucherinnen und Verbraucher stark beeinträchtigen. Zahlungsdaten sind keine Daten mit denen man zahlt. Personenbezogene Daten gehören immer zur Person auf die sie sich beziehen, sie sind nicht selbst das Zahlungsmittel und dürfen es auch nicht werden.

Diese Forderung nach einem Kopplungsverbot ist nicht neu, sondern sogar gesetzlich in der Datenschutz-Grundverordnung verankert. So enthält die Datenschutzgrundverordnung (DSGVO) auch Regelungen zur IT-Sicherheit sowie zum Datenschutz durch Technikgestaltung („privacy by design“) und zu datenschutzfreundlichen Voreinstellungen („privacy by default“).

Die Bundesregierung muss aus meiner Sicht die Datenschutzaufsichtsbehörden und die Rechtsdurchsetzungsstrukturen stärken, damit die bereits bestehenden Datenschutzregelungen konsequent angewendet und durchgesetzt werden können. Nur so können das Risiko und das Ausmaß von Datenskandalen verringert werden. Und nur so kann das Vertrauen in digitale Anwendungen wie Mobile Payment wieder wachsen.

Verunsicherung gibt es auch wegen der Vielzahl der beteiligten Anbieter beim digitalen Bezahlen. Verbraucher erkennen nicht immer automatisch den richtigen Ansprechpartner. Wen spricht man an, wenn etwas nicht stimmt mit einem Zahlvorgang? Die Bank, den App-Anbieter, den Anbieter des Betriebssystems Google oder Apple oder gar den Mobilfunkanbieter?

Ich habe letztens selbst eine unzulässige Buchung bei PayPal festgestellt. Was würden Sie machen? PayPal kontaktieren? Lastschriftabbuchung von PayPal widersprechen? Nicht ganz einfach, oder? Ich kann ihnen nur sagen: Bei solchen unzulässigen Abbuchungen wenden sie sich an PayPal und nicht an ihr Kontoinstitut. Ansonsten haben sie schnell Ärger mit gesperrtem Paypal-Konto und Inkassoforderungen.
Egal um welchen Dienst es geht: Verbraucher müssen die Zuständigkeiten der einzelnen Beteiligten am Zahlverfahren klar erkennen können. Das ist auch eine Frage der Sicherheit. Hier muss im Zweifel auch gelten, ist ein Anbieter unzuständig, muss für eine rasche Aufklärung und Weiterleitung an den Zuständigen gesorgt werden.

Ich sage es gefühlt bei jedem Safer Internet Day und ich werde es so lange sagen bis ein Umdenken einsetzt: Datenschutz ist eine Chance und es lohnt sich, sich dafür einzusetzen, die Privatsphäre der Verbraucherinnen und Verbraucher nachhaltig zu sichern. Die Bundesregierung sollte endlich anpacken und dafür sorgen, dass die guten Regeln aus der Datenschutz-Grundverordnung konsequent angewandt werden. Und wir müssen weiterdenken: Die Bundesregierung muss auf eine Verbesserung des allgemeinen IT-Sicherheitsniveaus hinarbeiten, beispielsweise durch verpflichtende IT-Sicherheitsstandards für Unternehmen und ein digitales Produkthaftungsrecht.

Meine Damen und Herren, ich habe hiermit meine Hausaufgaben an die Bundesregierung verteilt. Ich hoffe, dass ich im nächsten Jahr Positives zu berichten habe. Ich wünsche Ihnen eine weitere spannende Diskussion.

Herzlichen Dank!