ÜBERSICHT ZUR ERHEBUNG BEI KONTOINFORMATIONSDIENSTEN

31. Mai 2022

TESTAUFBAU

Im Zuge der europäischen Zahlungsdiensterichtlinie 2 (PSD2) traten Dienste in den Markt ein, die für bestimmte Servicedienstleistungen auf Daten der Girokonten von Verbrauchern zugreifen können (Kontoinformationsdienste, KID). Sie nutzen diese Daten allerdings auch, um weitere Angebote unterbreiten zu können. So werben sie beispielsweise damit, dass sie automatisch Versicherungslücken erkennen, maßgeschneiderte Kreditfinanzierungslösungen anbieten können oder die notwendige Anpassung einer Berufsunfähigkeitsversicherung.[1] Auf die Kontodaten greifen die Anbieter hierzu über eine eigens geschaffene Schnittstelle zu. Als KID können sich klassische Zahlungsverkehrsanbieter wie Banken registrieren lassen oder aber auch neuartige Dienste, die keinen Bezug zum Zahlungsverkehr haben. Die Aufsicht über diese Dienste ist beschränkt. Bei der BaFin müssen diese nur registriert werden. Einige KID greifen nicht selbstständig auf die Kontodaten zu, sondern nutzen Schnittstellenanbieter, die diese Arbeit für sie übernehmen.

Zwecke angebotener Servicedienstleistungen können z. B. sein, die eigene Identität bei einem Händler zu verifizieren, die Ausgabenstruktur eines Kontos zu analysieren oder eine gesonderte Bonitätsprüfung durchzuführen. Selbst wenn ein KID lediglich begrenztes Interesse an den Kontodaten hat, weil beispielsweise nur die Identität bestätigt werden soll, wird ihm über die Schnittstelle aktuell ein Komplettzugriff auf das Konto gewährt. Es gibt Dienste, die angeben, welche Informationen sie bei einem Zugriff abfragen, bei anderen bleibt aber weitgehend im Dunkeln, was und wie oft etwas abgefragt wird und was mit den Daten konkret geschieht.[2] Vereinzelte Beschwerden im Frühwarnnetzwerk der Verbraucherzentralen[3] zeigen, dass Verbraucher:innen von Anbietern nach einer legitimierten Abfrage auch in den folgenden Wochen noch mehrfach Kontoabfragen monierten, obwohl aus Nutzersicht kein legitimer Grund dafür mehr bestand. Es steht zu befürchten, dass gläserne Verbraucher:innen entstehen, deren Daten an verschiedenste Stellen abfließen, über die sie keine Kontrolle mehr haben.

---

[1] Siehe beispielsweise https://banksapi.de/analytics/, 21.4.2022.

[2] Wurde der Zugriff auf das Konto einmal durch den Kontoinhaber freigegeben, besteht für den Kontoinformationsdienst bislang die Möglichkeit, ohne weitere Prüfung weitere 90 Tage auf das Konto zuzugreifen. Im April 2022 schlug die Europäische Bankenaufsicht eine Verlängerung dieser Frist auf 180 Tage und unter bestimmten Voraussetzungen für Kontoinformationsdienste sogar die gänzliche Aufhebung einer Freigabe durch den Kunden vor (https://www.eba.europa.eu/eba-publishes-final-report-amendment-its-technical-standards-exemption-strong-customer, 5.4.2022).

[3] Beim Frühwarnnetzwerk der Verbraucherzentralen und des vzbv handelt es sich um ein qualitatives Erfassungs- und Analysesystem für auffällige Sachverhalte aus der Verbraucherberatung. Grundlage stellt eine ausführliche Sachverhaltsschilderung durch Beratungskräfte dar, die eine Kategorisierung sowie eine anschließende qualitative Analyse ermöglicht. Eine Quantifizierung der Daten aus dem FWN heraus bzw. ein Rückschluss auf die Häufigkeit des Vorkommens in der Verbraucherberatung oder in der Gesamtbevölkerung insgesamt ist daher nicht möglich.

Mit der aktuellen Analyse unterzog die Marktbeobachtung des Verbraucherzentrale Bundesverbands (vzbv) für Verbraucher:innen zugängliche Kontoinformationsdienste einer genaueren Analyse. Hierzu wurden zunächst in KW 9 und 10/2021 alle bei der BaFin und der europäischen Aufsicht EBA registrierten KID, die eine Geschäftstätigkeit in Deutschland angeben, recherchiert und dokumentiert (insgesamt 56 Anbieter, Recherchestand KW 9/10-2021). Anschließend wurden die Dienste selektiert, die ihre Leistungen explizit an Verbraucher:innen richten und getestet werden können. Es entfielen also Dienste von B2B-Anbietern (Schnittstellenanbietern)[4] und von Anbietern, bei denen kein Produkt erkennbar war, das eine Kontoinformationsdienstleistung nahelegte (z B. Angebot von Prepaid-Gutscheinkarten). Hieraus resultierten Testkonstellationen bei 18 Anbietern.

Zusätzlich wurden anhand von vier Beispielen Kreditantragsstrecken überprüft, bei denen Recherchen vermuten ließen, dass sie auch über einen KID als Drittdienst abgewickelt werden. Nach Prüfung der Referenzkunden fünf großer KID-Schnittstellenanbieter, weiterer Erkenntnisse zur Kreditantragsstrecke und den Meldungen bei den Verbraucherzentralen wurden die DKB, ING, Smava und die Targobank in das Testfeld aufgenommen. Sie haben ein relevantes Kreditgeschäft mit Nichtkunden, verfügen über eine breite Marktdurchdringung und ließen vermuten, in der Antragsstrecke einen KID eingebunden zu haben.

Insgesamt wurden somit folgende 22 Anbieter für die Analyse selektiert.

Kontoinformationsdienste	**Kreditantragsstrecken**
bankz family-App (CodeCamp:N GmbH)	DKB (Deutsche Kreditbank AG)
bonify-App (Forteil GmbH)	ING (ING-DiBa AG)
BudgetBakers (BudgetBakers s.r.o.)	Smava (smava GmbH)
finanzblick (BUHL-DATA-SERVICE GmbH)	Targobank (TARGOBANK AG)
Finanzcheck (FFG FINANZCHECK Finanzportale GmbH)	
Finanzguru-App (dwins GmbH)	
Klarna Rechnungskauf (Klarna Bank AB (publ))	
M-iTrust (M-iTrust SAS)	
MoneyMoney (MRH applications GmbH)	
Money Tracker (CHECK24 Kontomanager GmbH)	
Ownly (W&Z FinTech GmbH)	
Rentablo (Rentablo GmbH)	
Sofortüberweisung (SOFORT GmbH)	

[4] Einen Sonderfall stellt der untersuchte Anbieter M-iTrust dar, der kein eigenständiges Produkt unmittelbar an Verbraucher:innen richtet. Im Rahmen einer Anmeldung zu einem anderen Dienst konnten Verbraucher:innen aber gezielt auswählen, dass sie eine Legitimierung über diesen Dienst vornehmen möchten.

Spendee (SPENDEE a.s.)
TEO App (Comeco GmbH & Co KG)
Toshl (TOSHL, razvoj aplikacij, d. o. o.)
treefin-App (treefin GmbH)[5]
Verimi App (Verimi GmbH)

Tabelle: Analysierte Dienste

Die Analysen erfolgten im Zeitraum vom 29. September bis 20. Dezember 2021.[6] Hierbei wurde jeweils ein Testkonto bei dem KID angelegt und die Dienstleistung insoweit in Anspruch genommen, dass mindestens ein Girokonto eingebunden wurde. Sofern ein Konto nicht direkt in der Anwendung des KID eingebunden werden konnte, sondern weitere Schritte wie beispielsweise die Anmeldung bei einem zusätzlichen Dienst oder der Kauf einer Ware erforderlich waren, wurden diese Schritte durchgeführt. Bei den zusätzlichen Kreditantragsstrecken wurde bei den Anbietern ein Kreditangebot angefragt. Im Prozessablauf wurden nach Möglichkeit die Schritte durchgeführt, bei denen möglichst finale Kreditkonditionen durch direkten Zugriff auf das Konto zugesichert wurden. Das Girokonto der Testpersonen wurde jeweils nicht bei dem getesteten Anbieter geführt.

Bei folgenden Anbietern ließ sich die Kontoinformationsdienstleistung, also die Einbindung des Bankkontos, im Laufe des Tests nicht überprüfen:

- bankz family-App (Dienst wurde eingestellt)
- ING (kein Kontoinformationsdienst im getesteten Prozess integriert)
- Klarna Rechnungskauf (kein Kontoinformationsdienst im getesteten Prozess integriert)
- M-iTrust (kein Kontoinformationsdienst im getesteten Prozess integriert[7])
- Moneytracker (nur noch bei C24-Konten angeboten)
- Smava (kein Kontoinformationsdienst im getesteten Prozess integriert)
- Targobank (kein Kontoinformationsdienst im getesteten Prozess integriert)

Final getestet wurden somit 15 Kontoinformationsdienste.

BEOBACHTUNGEN

Die Kontoinformationsdienste gestalteten die Einbindung des Bankkontos und die damit verbundene Eingabe der sensiblen Banking-Zugangsdaten unterschiedlich. In elf der insgesamt 15 auswertbaren Fälle mussten die Zugangsdaten unter der URL des KID eingegeben werden. In drei Fällen erfolgte eine Weiterleitung zur

[5] treefin wurde nach Testabschluss in die App des Digitalversicherers Adam Riese integriert.
[6] Die Erhebung bei den Anbietern führte SWI Schad GmbH & Co KG im Auftrag von und nach einem Konzept des vzbv durch.
[7] Beim KID wurde stattdessen die Verifizierung über ein Handelskonto getestet.

Bank des Verbrauchers. In dem Fall, in dem der KID als Schnittstellenanbieter gegenüber Verbraucher:innen auftrat, erfolgte eine Weiterleitung auf die Seite des eingebundenen Schnittstellenanbieters[8].

Im Zuge der Kontofreigabe erfolgte die im Zahlungsverkehr vorgeschriebene Abfrage eines zweiten Faktors. Auch diese war sehr unterschiedlich gestaltet. Ein Anbieter wies bereits im Vorfeld darauf hin, dass die Einbindung des Kontos „teilweise mehrfach per Freigabeverfahren (z. B. TAN-Eingabe) bestätigt werden muss“. Bei einem anderen Anbieter wurden drei TANs hintereinander abgefragt: zur Anmeldung, zum Online-Abschluss und zur Authentifizierung. Diese Vorgehensweisen waren im Fall des KID zulässig. Allerdings lernen Verbraucher:innen hier möglicherweise ein gefährliches Muster: auf nicht mit ihrem Zahlungskonto verbundenen Seiten persönliche Zugangsdaten anzugeben und diese auch noch mit teilweise mehreren TANs zu bestätigen. Das Vorgehen ähnelt Verfahren, vor denen das Bundesamt für Sicherheit in der Informationstechnik im Zusammenhang mit Betrugsversuchen warnt.[9] Sechs der 15 KID blendeten Siegel ein (z. B. TÜV, SSL Datensicherheit, BaFin[10]). Sechs weitere nutzten keine Siegel, und bei drei Anbietern war ein Siegel unnötig, da eine Weiterleitung zur kontoführenden Bank erfolgte[11]. Mit den Siegeln verfolgen Anbieter vermutlich das Ziel, die wahrgenommene Vertrauenswürdigkeit ihrer Angebote zu erhöhen.

Wenn die KID Zugang auf die Bankkonten der Verbraucher:innen erlangen, können sie für einen bestimmten Zeitraum verschiedene Daten wie Kontoinhaber, Kontotyp, Kontostände und auch Transaktionsdaten auslesen. Unter diesen Daten finden sich unter Umständen auch besonders schützenswerte Daten wie Gesundheitsdaten oder die Zugehörigkeit zu einer bestimmten Religion, Partei, Gewerkschaft oder Ethnie. Nach der Datenschutzgrundverordnung (DSGVO) ist für die Verarbeitung personenbezogener Daten eine Einwilligung der betroffenen Person erforderlich. In der Art und Weise, in der diese Einwilligung eingeholt wird, unterscheiden sich die KID ebenfalls. Lediglich fünf Anbieter holten eine explizite aktive Einwilligung zur Verarbeitung ihrer Daten von den Nutzer:innen ein, d.h. sie mussten der Verarbeitung ihrer Daten beispielsweise mit einem zu setzenden Haken oder Schieberegler zustimmen. Bei den übrigen Anbietern bestand keine Möglichkeit der aktiven Einwilligung. Die Einwilligungen erfolgten hier nur über die Zustimmung zu Datenschutzhinweisen, der Datenschutzerklärung oder zu den Allgemeinen Geschäftsbedingungen oder über einen Hinweis, dass diese gelten würden. Nur drei Anbieter integrierten direkt im Webinterface die Zustimmung zur Erhebung besonders schützenswerter Daten, wobei nur ein einziger Anbieter direkt an dieser Stelle auch Beispiele solcher Daten anführte.

---

[8] Dies galt auch für den zweiten Fall dieser Konstellation bei M-iTrust, bei dem allerdings kein Bank-, sondern ein Handelskonto eingebunden wurde (und der deshalb nicht als final getestet eingestuft wurde).

[9] https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Online-Banking-Online-Shopping-und-mobil-bezahlen/Online-Banking/Was-tun-im-Ernstfall/was-tun-im-ernstfall_node.html, 22.4.2022.

[10] Folgende Siegel wurden bei den getesteten KID genutzt: BaFin, buhl:banking, Deutsches Institut für Servicequalität, fintecsystems, Fokus Money, Händlerlogo, Klarna, SSL Datensicherheit, TÜV Saarland.

[11] Einer dieser Anbieter nutzte in einem gesondert anklickbaren Info-Pop-Up dennoch ein Siegel (PCI-DSS).

Fünf der 15 getesteten KID versendeten im Testverlauf Angebote oder Werbung an die hinterlegte E-Mail-Adresse. Darüber hinaus erhielt in einem Fall die Testperson eine E-Mail eines Anbieters, dessen API-Schnittstelle der KID nutzte, also nicht des KID-Anbieters, bei dem sich die Testperson angemeldet hatte. Die E-Mail enthielt die Information, dass neben dem Konto beim KID auch beim Schnittstellenbetreiber ein Konto für ihn erstellt wurde und die anklickbare Aufforderung, ein Passwort dafür zu vergeben. Ob Verbraucher:innen diesen Anbieter bei der Anmeldung zum KID-Dienst überhaupt bewusst wahrnehmen und dann später auch noch erinnern, dass ihnen die E-Mail nicht suspekt vorkommt, muss bezweifelt werden. Vor E-Mails von Unbekannten, in denen Links angeklickt werden sollen, wird üblicherweise gewarnt.[12]

FAZIT

Insgesamt ist zu konstatieren, dass die untersuchten Kontoinformationsdienste die Ausgestaltung ihrer Produkte sehr unterschiedlich vornehmen und es dadurch Verbraucher:innen nicht erleichtern, anhand von gelerntem Wissen einen seriösen Dienst eindeutig zu identifizieren. Dies dürfte umso schwerwiegender sein, als selbst bei den durchgeführten Tests Fehler auftraten (z. B. nach Eingabe der Zugangsdaten nicht mehr ladende App; auch nach mehrfachem Versuch nicht funktionierende Anmeldung über den KID bei einem Partnershop; Auftreten eines unbekannten Fehlers nach Einbindung des Girokontos; Hängenbleiben auf einer Seite ohne Rückmeldung oder Weiter-Button). Wenn selbst bei seriösen Anbietern wie den getesteten KID technische Probleme dieser Art auftreten, kann dies aus Sicht des vzbv zu einer höheren Toleranzschwelle führen, ab der Verbraucher:innen Missbrauch vermuten. Sie laufen dadurch Gefahr, leichter auf nicht seriöse Anbieter hereinzufallen. In ihren subjektiven Wahrnehmungen berichteten die Testpersonen entsprechend von einem „Gefühl des Kontrollverlustes“ oder dass es „unübersichtlich für den Kunden [sei] was passiert“.

[12] https://www.verbraucherzentrale.de/wissen/digitale-welt/phishingradar/phishingmails-woran-sie-sie-erkennen-und-worauf-sie-achten-muessen-6073, 13.5.2022.

Kontakt

Verbraucherzentrale
Bundesverband e.V.

Team
Marktbeobachtung Finanzmarkt

Rudi-Dutschke-Straße 17
10969 Berlin

MBFinanzmarkt@vzbv.de

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