REPORTER

SCHWACHSTELLE BEI "DIGICASH"-APPS

Eine Einladung für Hacker

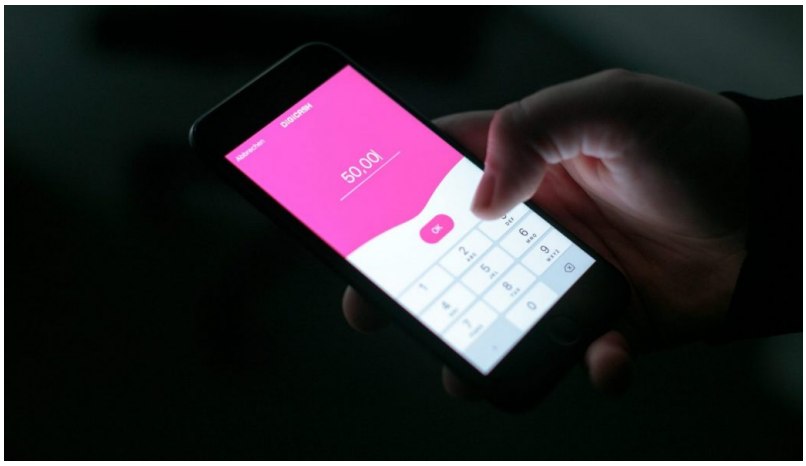

Foto: Matic Zorman

von Christoph Bumb

18. Oktober 2019

Eine Schwachstelle in der mobilen Bezahl-App „Digicash“ könnte laut IT-Experten als erste Etappe für Hackerattacken genutzt werden. Auch die Konformität mit Datenschutzregeln ist zweifelhaft. Es ist nicht das erste Mal, dass beim Betreiber eine Sicherheitslücke entdeckt wird.

„Erleichtern Sie sich das Leben“, lautet der Werbespruch von „Digicash“. „Bargeld? Brauchen Sie nicht mehr.“ „Garantiert schnell und sicher!“ Für den mobilen Bezahldienst, der mit fünf luxemburgischen Banken und etlichen Geschäften und Behörden zusammenarbeitet, ist die Benutzerfreundlichkeit seines Produkts das größte Verkaufsargument.

Doch die Leichtigkeit der Bedienung der Apps hat auch eine Kehrseite. Eine zentrale Funktion von Digicash besteht darin, dass sich Personen über ein Smartphone schnell kleinere Beträge überweisen können. Das geschieht über die Eingabe von Handy-Nummern. Das Problem: Auch wenn man eine Nummer eingibt, deren Besitzer man nicht kennt, erscheint in der Digicash-App der Vor- und Nachname des Besitzers der Telefonnummer – vorausgesetzt die betreffende Person hat die App ebenso heruntergeladen.

„Damit erhält man Zugriff auf Daten, die einem eigentlich nicht zustehen“, sagt Stéphane Ewerling. Der IT-Experte ist durch Zufall auf die Schwachstelle in der App aufmerksam geworden. Dass es sich um eine Sicherheitslücke handelt, ist für ihn offensichtlich. Denn, wenn man als einzelner Benutzer der App mit einer zufälligen Telefonnummer den passenden Vor- und Nachnamen herausfinden kann, sei das nicht im Sinne des Datenschutzes. Vor allem handele es sich aber um eine Verwundbarkeit, die von Hackern ausgenutzt werden könnte.

Digicash, eine „halb-öffentliche Datenbank“

Ein mittelmäßig begabter Informatiker könne sich laut dem Experten über die Funktionalität der Digicash-App nämlich leicht die persönlichen Daten aller Nutzer des Bezahldienstes aneignen. Das geschehe über den Weg einer systematischen Simulation der App auf einem leistungsstarken Rechner. „Wenn man über die Eingabe einer Telefonnummer den Namen des Besitzers herausfindet, ist es für einen Informatiker ein Kinderspiel, das systematisch für alle Nummern und Namen durchzuspielen“, so Stéphane Ewerling.

Sam Grüneisen vom „Chaos Computer Club Lëtzebuerg“ spricht in diesem Sinn von einer „halb-öffentlichen Datenbank“, die durch die App betrieben wird. Auch er bestätigt: Für einen Informatiker sei es „nicht allzu schwer“, sich über diesen Weg die persönlichen Daten von Tausenden Digicash-Nutzern anzueignen. Der Grund: Es handelt sich um eine Funktionalität, welche die App selbst zur Verfügung stellt.

> *Jeder Verbraucher muss im Vorfeld darüber informiert werden, was mit seinen persönlichen Daten geschieht.“*
>
> – Raymond Faber, Anwalt für Datenschutz- und IT-Recht

Was könnte man mit diesen Daten anstellen? Es sei durchaus plausibel, dass eine Drittperson diese Daten sammelt und verkauft, sagt Sam Grüneisen. „Persönliche Daten sind in der heutigen Zeit äußerst wertvoll.“ Vor- und Nachnamen sowie passende Handy-Nummern könnten etwa zu Werbezwecken, zum Verschicken von Spam-Botschaften oder zur Erstellung von gezielten Marketingprofilen genutzt werden.

Beide Experten für IT-Sicherheit weisen aber auch auf andere mögliche Missbräuche hin. So könnte man über die Digicash-App gezielt nach Telefonnummern von Personen suchen, die nicht im Telefonbuch stehen. Oder auch nach Politikern, Unternehmern oder anderen Prominenten, womit die Tür für Stalking oder andere Formen von Belästigungen geöffnet wäre. Wegen der möglichen Formen des Missbrauchs sei ein bewusster Umgang mit persönlichen Daten heutzutage so wichtig, sagt Sam Grüneisen. „Eine App darf nicht einfach mit unseren persönlichen Daten hausieren gehen.“

Digicash: „Das ist genau so gewollt“

Auf die Schwachstelle angesprochen, erklärt Digicash, dass die besagte Funktionalität „genau so gewollt“ sei. Dass bei der Übermittlung einer Zahlung via App der Name sichtbar sei, verstehe man als Service, damit der Zahlende kein Geld an eine falsche Person überweist, erklärt eine Pressesprecherin von „Payconiq International“, jener Firma, die das luxemburgische Startup „Digicash“ 2017 aufgekauft hat.

Die Funktion, wonach bei Eingabe einer Telefonnummer der entsprechende Name angezeigt wird, sei auch in den Nutzungsbedingungen der mit Digicash zusammenarbeitenden Banken so festgehalten. Letztlich bieten die Banken jeweils eine App als Dienstleistung an, die jedoch alle auf der gleichen Programmierung von Digicash beruhen.

> *(…) l’Abonné est informé que les données le concernant peuvent circuler sur les réseaux sans garanties de sécurité et qu’elles risquent d’être lues et utilisées par des tiers non autorisés.“*

– Digicash-Nutzungsbedingungen von „Post Luxembourg“

Die „BGL BNP Paribas“ macht in der Tat in ihren „Conditions d’utilisation Digicash“ in Artikel 8.5. auf die mögliche Nutzung der Daten konkret aufmerksam. Auch „Post Luxembourg“ schreibt in seinen „Conditions particulières“, dass der Nutzer „informiert“ wird, dass seine persönlichen Daten „ohne Sicherheitsgarantien“ zirkulieren und von nicht-autorisierten Drittpersonen „gelesen und genutzt“ werden könnten. Ähnliche Passagen stehen in den Nutzungsbedingungen von „BCEE“, „BIL“ und „ING Luxembourg“. Alle Banken betonen zudem, dass die Speicherung der persönlichen Daten von „Digicash Payments S.A.“ verantwortet wird.

„Digicash“: eine Erfolgsgeschichte

Der Bezahldienst „Digicash“ wurde 2012 als luxemburgisches Startup mit finanzieller Unterstützung der Regierung ins Leben gerufen. Mit der mobilen Zahlungslösung können Nutzer in Geschäften, online oder mit dem Smartphone bezahlen sowie anderen Nutzern Geld überweisen. Neben Privatunternehmen gehören auch Gemeinden und staatliche Behörden zu den Kooperationspartnern. Unter anderem lassen sich Protokolle der Polizei per QR-Code via Digicash begleichen. Vor rund zwei Jahren wurde „Digicash Payments S.A.“ vom belgischen Unternehmen „Payconiq“ aufgekauft. Laut einer Umfrage von 2017 nutzen 18 Prozent der Luxemburger „Digicash“. 84 Prozent kennen zumindest die Marke.

Was den einfachen Zugang zu diesen Daten betrifft, erklärt die Sprecherin von Digicash, dass es immer die Möglichkeit eines „Opt-out“ gebe. Wenn ein Nutzer nicht will, dass seine persönlichen Daten von anderen Nutzern einsehbar sind, könne er dies in der App ausschalten. Allerdings kann man so keine Zahlungen von anderen Nutzern mehr erhalten, was eben ein zentraler Zweck der App ist.

Für alle weiteren Fragen verweist die Sprecherin auf die Banken, die jeweils die Apps zur Durchführung der Zahlungen anbieten. Ein Sprecher der „Spuerkeess“ will auf Nachfrage von REPORTER indes nicht weiter auf die Frage eingehen und verweist seinerseits auf die Antworten von Digicash, denen man sich anschließe und denen man nichts hinzuzufügen habe. Zwei weitere Banken wollten auf Nachfrage keine Stellungnahme abgeben.

„Suboptimale Lösung“ zum Datenschutz

Ist die Funktionalität mit der Datenschutz-Grundverordnung (GDPR) vereinbar? Der Anwalt Raymond Faber weist darauf hin, dass die Nutzer in jedem Fall über den Umgang mit ihren Daten Bescheid wissen müssen. „Jeder Verbraucher muss im Vorfeld darüber informiert werden, was mit seinen persönlichen Daten geschieht“, so der in Datenschutz- und IT-Recht spezialisierte Jurist. Diese Information müsse aus den Nutzungsbedingungen der Banken klar hervorgehen.

Das Risiko eines Missbrauchs der durch Digicash gespeicherten Daten schätze er zwar als „eher klein“ ein. Name und Telefonnummer seien im Vergleich etwa mit Konto- oder Kreditkartennummern keine allzu sensiblen Daten. Der einfache, ja von den App-Betreibern gewollte Zugang zu diesen persönlichen Daten sei jedoch eine „suboptimale Lösung“, so Raymond Faber.

Auch der IT-Experte Stéphane Ewerling betont, dass die besagte Schwachstelle im System nicht unbedingt notwendig sei. Es gebe etliche Wege, wie man die Benutzerfreundlichkeit und die Sicherheit der persönlichen Daten technisch besser miteinander in Einklang bringen könnte.

Es gehe auch nicht darum, die verantwortliche Firma bloßzustellen – im Gegenteil, so der Experte. Deshalb habe er Digicash und eine der kooperierenden Banken auch sofort über die Verwundbarkeit der App informiert. Die betroffene Bank habe sofort reagiert und eine Überprüfung der App-Funktionen in Aussicht gestellt. Digicash selbst habe jedoch erst nach der dritten Benachrichtigung reagiert, ohne allerdings im Kern auf den Inhalt einzugehen.

Digicash nicht zum ersten Mal auffällig

Laut Sam Grüneisen vom „Chaos Computer Club Lëtzebuerg“ ist es zudem nicht das erste Mal, dass seine Organisation auf Beschwerden in Bezug auf Digicash aufmerksam wird. Vor einigen Monaten habe man herausgefunden, dass man über den Bezahldienst im Namen einer anderen Person oder Firma Rechnungen ausstellen kann. Die Digicash-Nutzernamen für Händler seien zum Teil einfach zu erraten, so Grüneisen. So ließen sich leicht funktionsfähige QR-Codes im Namen einer Firma, die Digicash nutzt, generieren. Damit sei es möglich, gefälschte Rechnungen auszustellen und Nutzer zu täuschen bzw. Überweisungen an falsche Adressaten zu veranlassen.

> *Eine App darf nicht einfach mit unseren persönlichen Daten hausieren gehen.“*
>
> – Sam Grüneisen, „Chaos Computer Club Lëtzebuerg“

Im Vergleich dazu sei die die Funktionalität beim Transfer zwischen Privatpersonen zwar keine kritische Sicherheitslücke, so der Experte. Doch auch die systematische Verfügbarkeit von Telefonnummern und entsprechenden Namen sei durchaus ein Problem, das die Entwickler der App schnellst möglich nachbessern müssten.

Digicash weist in seiner Reaktion darauf hin, dass die Anzeige von persönlichen Daten in der App eine gängige Praxis sei. Nur Nutzer von Digicash, was laut der Sprecherin mittlerweile immerhin knapp ein Viertel der luxemburgischen Bevölkerung ausmacht, hätten Zugang zu diesen Daten. Und auch nur unter der Voraussetzung, dass sie Kunden bei einer der kooperierenden Banken sind und per Luxtrust-Token über einen Zugang zum Online-Banking verfügen. Über das Prinzip „Know-Your-Customer“ würden die Banken wissen, wer ihre Apps benutze und könnten somit auch Missbrauch vorbeugen bzw. mögliche Straftaten verfolgen.

Was die mögliche Speicherung und Nutzung von Daten aus der Digicash-Datenbank durch Drittpersonen betrifft, bewege man sich eindeutig im strafbaren Bereich, erklärt der Anwalt Raymond Faber. Egal wie man die leichte Verfügbarkeit der persönlichen Daten in einer Digicash-App bewerte, sei eine Nutzung dieser Daten unabhängig vom Zweck der App durch nicht befugte Drittpersonen nicht erlaubt.