Sicherheits- und Datenschutzrisiken beim Zugriff Dritter auf Bankkonten

Schweizer Banken bieten ihren Kunden umfassende und sichere Dienstleistungen über elektronische Kanäle. Nun haben neue Anbieter angekündigt, über Web- und App-Lösungen bankübergreifende Zahlungsauslöse- und Kontoinformationsdienstleistungen für Privatkunden anzubieten. Die Anbieter verlangen dafür meist die E-Banking-Legitimationsmittel ihrer Kunden, um Zugang zu deren Bankkonten zu erhalten. Insbesondere in Europa wird vor einer solchen Preisgabe der persönlichen Zugangsdaten aufgrund erheblicher Sicherheitsrisiken für Kunden und Banken gewarnt. Signifikante Risiken ergeben sich auch durch die Übertragung grosser Mengen an Bankkundendaten aus den Systemen der Banken heraus in aufsichtsrechtlich weniger streng geregelte Umgebungen. UBS zeigt Ansätze auf, wie sich diese Risiken durch sichere Interaktionsmodelle mit den neuen Anbietern und deren Unterstellung unter eine adäquate Regulierung und Aufsicht adressieren lassen.

Sichere Online-Finanzdienstleistungen der Banken

Durch neue technische Gegebenheiten wie die Verdrängung von PCs durch Tablets und Smartphones sowie den Umstieg von lokal installierter Software zu Online-Diensten ergeben sich neue Möglichkeiten, wie Bankkunden auf Ihre Konten und das Zahlungsverkehrssystem zugreifen können. So bieten Banken ihren Kunden über das Web und zunehmend auch über Apps verschiedene Optionen, ihre Konten zu überwachen, Zahlungen zu tätigen oder ein persönliches Budget zu verwalten. Dabei ist der Kunde durch die Sicherheitssysteme seiner Bank geschützt. Die Bank wiederum ist durch die Regulationen der Finanzaufsichtsorgane (FINMA), das Bankengesetz (BankG) und die Vereinbarung über die Standesregeln zur Sorgfaltspflicht der Banken (VSB) zu einem besonders sorgsamen Umgang mit Bankkundendaten verpflichtet.

Neu treten auch nicht regulierte Drittanbieter als Online-Finanzdienstleister auf

Nachdem in Amerika und Europa auch bankfremde Drittanbieter Zahlungsauslöse- und Kontoinformationsdienste erbringen, haben nun auch in der Schweiz mehrere Dritte angekündigt, in Kürze ähnliche Dienstleistungen anbieten zu wollen.

Erfahrungen mit Drittanbietern im Ausland zeigen, dass diese für den Zugriff auf Bankkonten ihrer Kunden teilweise die sogenannte *Impersonation* einsetzen. Sie erfragen von ihren Kunden also die Legitimationsmittel (z.B. Vertragsnummer und Passwort) zu deren E-Banking-Zugängen und nutzen diese Daten, um als Mittelsmann mit uneingeschränkter Autorisierung auf die Konten der Kunden zuzugreifen. Technisch entspricht dieses Vorgehen dem eines Phishing-Betrugsfalls.

Während Banken strengen Vorgaben zur Sicherheit ihrer Systeme unterliegen, um die Kundendaten bestmöglich zu schützen, lagert und speichert ein Teil der Drittanbieter grosse Mengen an Bankkundendaten in meist weniger geregelten IT-Systemen. Oft sind diese Systeme weder im Besitz noch unter der Kontrolle der Drittanbieter. Denn häufig kommen Cloud-Lösungen zum Einsatz, bei denen der Speicherort der Daten unbekannt ist. Für diese Systeme gilt in der Regel auch das Schweizer Bankkundengeheimnis nicht.

Sowohl die Verwendung von *Impersonation* als auch die nicht regulierte Verwendung von Bankkundendaten bergen signifikante und für die Kunden nur schwer einschätzbare Risiken.

Impersonation als erhöhtes Sicherheitsrisiko

Anders als beim Einsatz traditioneller, beim Kunden lokal installierter Software, greift bei der Verwendung Cloud-basierter Dienstleistungen nicht der Kunde direkt, sondern der Drittanbieter auf die Bankkonten zu, indem er sich mit den Legitimationsmitteln des Kunden ausweist. Diese *Impersonation* ist allerdings ein risikoreicher Ansatz zur Erreichung dieses Zugriffs. So warnt z.B. die Europäische Bankiervereinigung: "[T]his model fails to meet the high security standards which authorities and authorized [Payment Service Providers] as well as consumers would like to see in the current and future payment services in the Single Market"[1]. Die Europäische Zentralbank fordert unmissverständlich: "The third party payment service provider shall not be allowed to obtain the payment service user's personalised [e-banking] security features issued by the account servicing payment service provider [i.e. by the banks]"[2].

Der Kunde gewährt durch die Weitergabe seiner Legitimationsmittel dem Dritten (meist unbeabsichtigt) signifikant mehr Rechte, als dieser zur Erbringung seiner Dienstleistungen benötigt. Typischerweise erhält der Dienstleister damit sogar unbeschränkten Zugriff auf die Konten des Kunden. Bildlich gesprochen verrät der Kunde die Zahlenkombination zu seinem Tresor an den Dienstleister, damit dieser unbeaufsichtigt das Geld im Tresor zählt oder 100 Franken für eine Überweisung an einen Dritten herausnimmt, im Vertrauen, dass der Dienstleister nach getaner Arbeit einfach die Tresortür schliesst und ins Schloss fallen lässt. Es ist offensichtlich, dass dies den Kunden einem unnötig hohen Risiko aussetzt.

Auch die Bank des Kunden kann durch die nicht bestimmungsgemässe Verwendung persönlicher Zugangsdaten kaum noch unterscheiden, ob ihr Kommunikationspartner der Kunde selbst ist, oder ein vom Kunden beauftragter Mittelsmann, oder – schlimmstenfalls – ein krimineller Mittelsmann, der sich anderweitig Zugang zu den Legitimationsmitteln des Kunden verschafft hat. Die Bank kann dadurch ihren Sorgfalts-

pflichten wie z.B. dem Schutz der Bankkundendaten nicht mehr genügend nachkommen.

Zudem ist die Abfrage von E-Banking-Legitimationsmitteln ausserhalb des E-Banking aus Kundensicht ein typisches Kennzeichen eines Phishing-Angriffs eines Kriminellen. Wenn neu auch vertrauenswürdige Anbieter E-Banking-Legitimationsmittel ausserhalb des E-Banking abfragen, wird es für die Kunden noch schwerer, die Risiken bei der Preisgabe ihrer Zugangsdaten an Dritte korrekt einzuschätzen. Als Folge davon könnte die Zahl von E-Banking-Betrugsfällen via Phishing deutlich zunehmen.

Kontrollverlust über Bankkundendaten

Schweizer Banken sind bezüglich Schutz der Bankkundendaten stark reguliert[3] und verfügen über langjährige Erfahrung diesbezüglich.

Demgegenüber unterstehen weder die Cloud-Provider noch die dritten Dienstleister dem Bankengesetz und unterliegen somit auch nicht dem Bankkundengeheimnis. Zudem können Bankkundendaten durch die Übertragung auf die Systeme der Drittanbieter sogar die Schweiz verlassen, möglicherweise ohne dass dies dem Kunden bewusst ist. So gibt es beispielsweise aktuell ausländische Zahlungsdienstleister, denen auch Kunden in der Schweiz durch die Preisgabe ihrer E-Banking-Legitimationsmittel ermöglichen, ihr Bankkonto vor Auslösung einer Zahlung detailliert zu analysieren, um die Verfügbarkeit der Mittel zu prüfen.

Die Auswirkungen dieses Kontrollverlusts über potentiell sehr grosse Mengen persönlicher Daten vieler Kunden sind kaum abschätzbar. Nicht zuletzt kann dies es Kriminellen erleichtern, sich Zugang zu Bankkundendaten zu verschaffen, z.B. zur einfacheren Durchführung von Social Engineering-Angriffen gegen Kunden oder auch gegen Mitarbeiter im Kundenservicecenter einer Bank. Die Bank kann die Sicherheit der Daten so nicht mehr auf dem bisherigen Niveau gewährleisten, und der Kunde kann nicht mehr vom gewohnten Schutz seiner Interessen durch die Bank profitieren.

Voraussetzungen für einen sicheren Zugriff auf Bankkonten durch Dritte

Schweizer Banken bieten ihren Kunden über elektronische Kanäle vielfältige Dienstleistungen für Zahlungsauslösung und Kontoinformation, welche die erforderliche Sicherheit bieten.

UBS begrüsst es ausdrücklich, wenn auch Drittanbieter Schweizer Bankkunden innovative Dienstleistungen anbieten. Diese sollen aber die hohen Sicherheitsstandards des Schweizer Bankengeschäfts nicht beeinträchtigen. Innovation darf nicht zu Lasten der Sicherheit von Kunden und Banken gehen. Insbesondere darf es nicht möglich sein, dass durch indirekten E-Banking-Zugang via Drittanbieter die Sicherheitsvorkehrungen einzelner Banken umgangen werden.

Deshalb sollten in der Schweiz klare Regeln für den Zugriff durch Drittanbieter auf Bankkonten gelten.

So sollte die Nutzung von *Impersonation* untersagt werden um eine Verschärfung der Phishing-Gefahr zu verhindern und um die Risiken eines uneingeschränkten Zugriffs der Drittanbieter auf Bankkonten der Kunden etwas zu reduzieren.

Allerdings ist eine Beschränkung auf sicherheitstechnisch besser geeignete Zugriffsmethoden nur ein erster Schritt zur Regelung des Zugriffs von Drittanbietern. Eine solche erfordert unter anderem auch eine umfassende Aufklärung der Kunden über die Risiken beim Zugriff auf ihre Bankkonten durch Dritte. Insbesondere sollte der Drittanbieter nur mit expliziter Autorisation des Kunden der Bank gegenüber auf die Bankkonten zugreifen dürfen, gleich wie jeder andere Dritte heute schon nur mit einer Vollmacht zugreifen darf.

Ebenso sollten für die Erfassung, Speicherung, Bearbeitung und Weitergabe von Bankkundendaten durch Dritte ausserhalb des Kontrollbereichs von Kunde oder Bank klare Regeln aufgestellt werden. Diese Regeln sollten sich im Sinne eines optimalen Schutzes der Kundeninteressen an vergleichbaren Regeln für den Schweizer Bankensektor orientieren. Zum Beispiel müsste der Wahrung des Bankkundengeheimnisses Rechnung getragen werden, was zum Beispiel bedingt, dass Bankkundendaten die Schweiz nicht verlassen.

Um die erlassenen Regeln durchzusetzen, gilt es unter anderem die Verantwortlichkeiten bezüglich Haftung in Schadensfällen klar zuzuordnen und die Fähigkeit der Dienstleister zur Deckung allfälliger Schäden sicherzustellen. Überdies sollte die Einhaltung der Regeln auch durch eine entsprechende Aufsicht gewährleistet werden.

1 EBF Position Paper on Payment Account Access Service: Innovation and security should go hand in hand; 16 July 2013
2 Opinion of the European Central Bank (CON/2014/9), 5 February 2014
3 Siehe z.B. Anhang 3 "Umgang mit elektronischen Kundendaten" des teilrevidierten FINMA-Rundschreibens 2008/21 "Operationelle Risiken Banken"

UBS AG
Bahnhofstrasse 45
P.O. Box
CH-8098 Zürich
Tel. +41-44-234 11 11

ubs.com