Zugriff durch Drittanbieter auf Bankkonten

Verschiedene Drittanbieter bieten bankübergreifende Zahlungs- und Kontoinformationsdienstleistungen für E-Banking-Kunden an. Das ist zwar bequem, birgt aber einige Risiken.

Schützen Sie sich, indem Sie ...

- Ihre persönlichen Zugangsdaten fürs E-Banking (Passwort, PIN, Identifikationsnummer etc.) niemandem bekannt geben – weder einer anderen Person noch einem Dienst eines Drittanbieters.

Für den Zugriff auf die Bankkonten werden meist die E-Banking-Zugangsdaten der Kunden eingefordert und verwendet. Durch die Weitergabe der persönlichen Zugangsdaten an Dritte setzen Sie sich als Kunde einem erheblichen Sicherheitsrisikoaus. Ausserdem können Ihre Bankkundendaten durch die Drittanbieter von den stark regulierten Systemen der Schweizer Finanzinstitute (FINMA, Bankengesetz etc.) in weniger streng geregelte Umgebungen übertragen werden.

Seien Sie vorsichtig!

Sowohl die Verwendung von Impersonation als auch die nicht regulierte Bearbeitung und Speicherung von Bankkundendaten bergen signifikante Risiken für Sie.

«eBanking – aber sicher!» rät deshalb von jeder Weitergabe der persönlichen E-Banking-Zugangsdaten an Dritte ab.

Copyright – Alle Rechte vorbehalten. Hochschule Luzern – Informatik

Weiterführende Informationen für Interessierte

Risikoreiche Nutzung bankübergreifender Online-Dienste

Mögliche Dienstleistungen von Drittanbietern, welche die persönlichen E-Banking-Zugangsdaten der Kunden verwenden, umfassen beispielsweise den Zugriff auf Bankkonten von verschiedenen Finanzinstituten über eine einzige Plattform. Aber aufgepasst, Sie setzen sich durch die Weitergabe Ihrer persönlichen E-Banking-Zugangsdaten an eine solche Plattform einem erheblichen Sicherheitsrisiko aus.

Impersonation als Sicherheitsrisiko

Für den Zugriff auf Bankkonten ihrer Kunden setzen Drittanbieter meist die sogenannte Impersonation (Nachahmen, Auftreten als jemand anders) ein. Dazu erfragen sie von ihren Kunden die persönlichen Zugangsdaten (z. B. Passwort und Identifikationsnummer) für deren E-Banking und nutzen diese Daten, um als Mittelsmann mit uneingeschränktem Zugriff auf die Konten zuzugreifen.

Wenn Sie als Kunde Ihre persönlichen Zugangsdaten auf diese Art weitergeben, ist dies mit der Situation vergleichbar, als würden Sie im Reisebüro Ihre Ferien buchen, zur Bezahlung einfach Ihr Gegenüber an Ihrem E-Banking-Konto anmelden, und das Geschäft verlassen – im blinden Vertrauen, dass die Angestellten wirklich nur den vereinbarten Betrag abbuchen und sich danach sofort wieder abmelden. Die Person könnte allerdings genauso gut noch nachschauen, wie viel Lohn Sie jeden Monat überwiesen erhalten und sogar versucht sein, sich die eigenen Ferien von Ihrem Konto zu finanzieren. Technisch gesehen entspricht die Nutzung von Impersonation einer Identitätsübernahme – dem gleichen Vorgehen eines klassischen Phishing-Angriffs (https://www.ebas.ch/phishing/) – selbst wenn es sich um einen seriösen Drittanbieter handelt!

Durch die nicht bestimmungsgemässe Verwendung der persönlichen Zugangsdaten kann das Finanzinstitut kaum noch unterscheiden, ob es mit Ihnen als Kunden selbst, mit einem von Ihnen beauftragten Drittanbieter oder – schlimmstenfalls – mit einem kriminellen Mittelsmann kommuniziert. Das Finanzinstitut kann dadurch seinen Sorgfaltspflichten, wie z. B. dem Schutz der Bankkundendaten, nicht mehr genügend nachkommen. Im Schadensfall drohen Ihnen als Kunde gar Haftungsausschlüsse.

Kontrollverlust über Bankkundendaten

Während Schweizer Finanzinstitute strengen Vorgaben zum Schutz der Bankkundendaten und zur Sicherheit ihrer Systeme unterliegen, können Drittanbieter mit Ihrer Einwilligung Daten in weniger regulierten Umgebungen und Systemen speichern und bearbeiten. Zum Teil sind diese Systeme weder im Besitz noch unter der Kontrolle der Drittanbieter. Häufig kommen nämlich sogenannte Cloud-Lösungen zum Einsatz, bei denen der genaue Speicherort der Daten oft nicht bekannt ist. Für solche Systeme gilt in der Regel auch das Schweizer Bankkundengeheimnis nicht!

Die Auswirkungen dieses Kontrollverlusts über die Speicherung persönlicher Daten sind kaum abschätzbar. Nicht zuletzt kann dies Kriminellen erleichtern, sich Zugang zu persönlichen Bankkundendaten zu verschaffen.

Copyright – Alle Rechte vorbehalten. Hochschule Luzern – Informatik