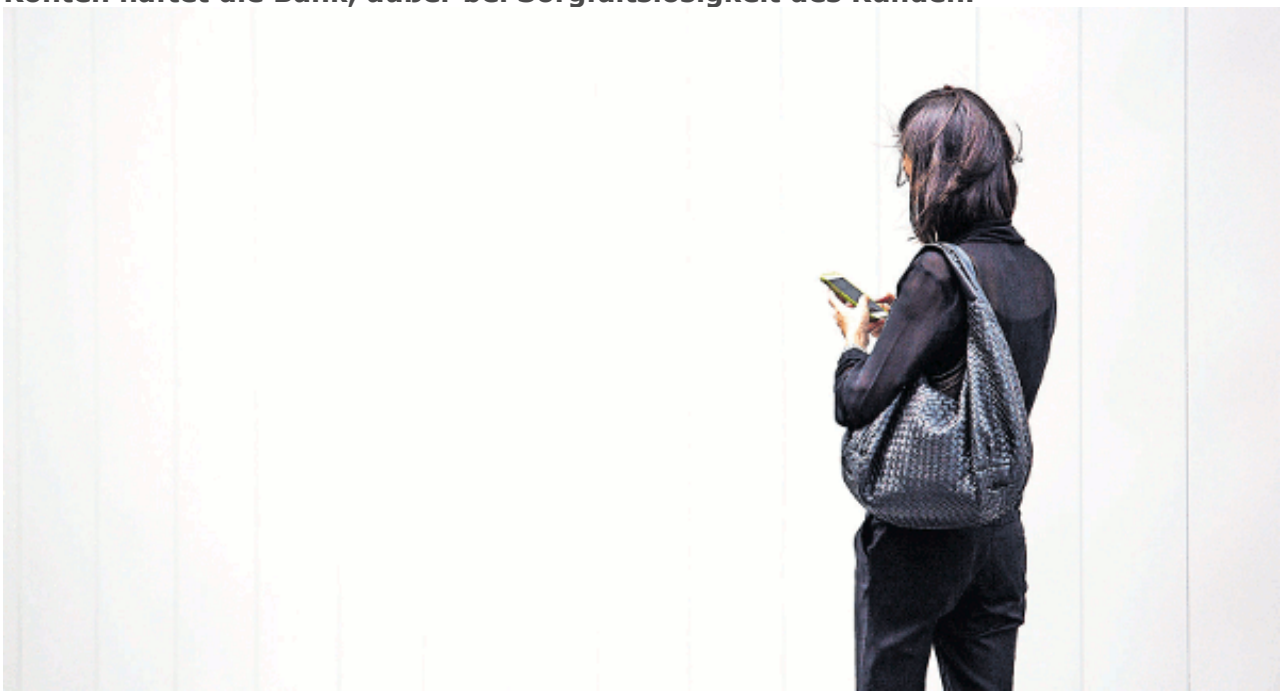
Die Presse – Recht

Die Presse

Wenn Hacker Konten plündern: Wie sich die Haftung verteilt

Rechtspanorama · Bernhard Brehm/Nikolaus Socher · Die Presse - Recht 2019/384 · Die Presse - Recht 2019, 14 · Heft 49 v. 2.12.2019

E-Banking. **Die starke Kundenauthentifizierung, die Banken neuerdings online verlangen müssen, soll den Zahlungsverkehr sicherer machen. Bei Hackerangriffen auf Konten haftet die Bank, außer bei Sorgfaltslosigkeit des Kunden.**



Wien. Als Folge der zunehmenden Digitalisierung des Zahlungsverkehrs unter Verwendung von mobilem Onlinebanking kommt es vermehrt zu Missbrauchsfällen und Attacken von Cyberkriminellen auf Kundenkonten. Die Sicherheitsrisken im elektronischen Zahlungsverkehr haben sich in den vergangenen Jahren erhöht, was aber von Banken nicht gern öffentlich diskutiert wird.

Immer wieder gelingt es Cyberkriminellen, geheime Bankzugangsdaten von Kunden auszuspionieren, deren Bankkonten zu hacken und leer zu räumen. Dabei verwenden die Täter mittlerweile innovative technische Methoden unter Einsatz künstlicher Intelligenz. Zudem agieren Cyberkriminelle zunehmend aus dem außereuropäischen Ausland und arbeitsteilig und entziehen sich dadurch geschickt der Strafverfolgung. So kaufen Cyberkriminelle zum Beispiel vertrauliche von Kunden gestohlene Kundendaten im Darknet, um damit gezielte Cyberattacken auf konkrete Kundenkontos durchzuführen.

Scheinbar harmloses Surfen

Eine beliebte und bekannte Methode des Datendiebstahls ist das Phishing, bei dem gefälschte E-Mails oder Websites verwendet werden, die dem Kunden vortäuschen, er würde sich bei seinem Online-Bankkonto anmelden. In anderen Fällen gelingt es den Angreifern, Schadsoftware ("Malware") auf dem Computer des Kunden zu installieren und dessen Zugangsdaten

abzusaugen. Manchmal genügt bereits harmloses Surfen im Internet, um einen Kunden-PC mit Schadsoftware, wie etwa Trojanern, Spyware oder Tastatur-Trackern, zu infizieren.
Der Gesetzgeber hat auf die wachsenden Gefahren reagiert. Basierend auf der zweiten Zahlungsdiensterichtlinie der EU ist das österreichische Zahlungsdienstegesetz (ZaDiG) 2018 am 1. Juni 2018 in Kraft getreten. Verschärft wurden die Vorschriften zur Transaktionssicherheit für den digitalen Zahlungsverkehr sowie die Haftung der Banken bei Nichterfüllung dieser Vorgaben. Die Ziele sind der Schutz der Onlinebanking-Kunden vor Betrugsrisken und Cyberattacken sowie der Ausbau des Verbraucherschutzes.
Im Zusammenhang mit den geschilderten Cyberattacken stellt sich die rechtliche Frage, wer bei den nicht vom Kunden autorisierten Zahlungen den Schaden zu tragen hat: Der Bankkunde, dessen Konto geplündert wurde, oder aber die Bank, die das Onlinebanking-System zur Verfügung stellt?
Grundsätzlich trifft die Bank eine verschuldensunabhängige Haftung. Der Bankkunde hat gegenüber der Bank einen vollen Berichtigungs- oder Erstattungsanspruch, sofern er den Schaden nicht verschuldet hat. Hat der Kunde den Schaden aber verschuldet, etwa wenn er eine ihm auferlegte Sorgfaltspflicht schuldhaft verletzt hat, so haftet er. Zu dieser Sorgfaltspflicht zählt etwa die Geheimhaltung der persönlichen Zugangsdaten wie Passwort oder PIN.
Bei lediglich leichter Fahrlässigkeit ist die Haftung des Kunden im Schadensfall auf 50 Euro beschränkt. Bei grober Fahrlässigkeit hingegen haftet der Kunde für den gesamten Schaden, sofern es nicht wegen eines Mitverschuldens der Bank zu einer Schadensteilung kommt. Dass der Kunde leicht bzw. grob fahrlässig gehandelt hat, muss ihm aber die Bank nachweisen.

Bei der Prüfung der Verschuldensfrage ist das Verhalten des Bankkunden mit dem fiktiven Verhalten eines ordentlichen Bankkunden zu vergleichen. Der OGH konkretisierte in seiner Entscheidung 9 Ob 48/18a diesen Sorgfaltsmaßstab. Ein Bankkunde hatte seinen Verifizierungscode (TAC-Code) telefonisch an einen vermeintlichen Bankmitarbeiter weitergegeben, der in Wirklichkeit ein Betrüger war. Dank der Bestätigung durch den TAC-Code konnte der Betrüger knapp 13.000 Euro abbuchen, für welche der Kunde wegen der grob sorgfaltswidrigen Verletzung seiner Sorgfaltspflicht zu haften hatte.
Dem Bankkunden ist also zuzumuten, offensichtliche Phishing-Angriffe zu erkennen und persönliche Daten geheim zu halten. Hingegen wird es der Bank wohl nur schwer gelingen, ein Verschulden des Bankkunden nachzuweisen, wenn der PC des Kunden trotz Virenschutzprogramms unbemerkt mit einer Schadsoftware infiziert wurde und so die Zugangsdaten abgesaugt wurden.
Um diese Sicherheitslücken zu schließen, führt das ZaDiG die Verpflichtung für Banken ein, eine starke Kundenauthentifizierung zu verlangen. Sie besteht aus drei Sicherheitsmerkmalen: Wissen – etwas, was nur der Kunde weiß (PIN, Verfügernummer); Besitz – etwas, was nur der Kunde besitzt (Mobiltelefon); Inhärenz – ein Merkmal des Kunden, das ihm eindeutig zugeordnet werden kann (Fingerabdruck, Gesichtsscan). Um den neuen Vorgaben zu entsprechen, muss die Bank vom Kunden zwei dieser drei Elemente abfragen, wenn dieser eine Online-Transaktion durchführen will.

Starke Authentifizierung

Führt die Bank für die Online-Transaktion keine starke Kundenauthentifizierung durch, haftet sie bei Missbräuchen auch dann, wenn der Kunde seine Sorgfaltspflichten grob fahrlässig verletzt hat. Die neuen Vorschriften über die starke Kundenauthentifizierung in Verbindung mit den geschilderten Haftungserleichterungen für die Bankkunden erhöht also die Sicherheit im elektronischen Geschäfts- und Zahlungsverkehr.
Um potenzielle Haftungen der Bankkunden in Missbrauchsfällen zu vermeiden, ist es Bankkunden jedenfalls zu empfehlen, ihre Daten geheim zu halten, keinesfalls an Dritte weiterzugeben und sichere Passwörter zu verwenden. Die geheimen Daten sollten nicht im PC gespeichert werden; auf diesem sollten darüber hinaus ein aktuelles Betriebssystem und ein Virenschutz installiert sein. Es kann nämlich nicht mit Sicherheit gesagt werden, ob nicht im Einzelfall bereits die Unterlassung dieser Schutzvorkehrung von den Gerichten als Verletzung einer Sorgfaltspflicht qualifiziert werden könnte.

Jedenfalls aber sollten Kunden die jeweiligen Bankempfehlungen, Sicherheitsinformationen und Sicherheitstipps beachten, die auf den Sicherheitsportalen der Banken bzw. über E-Banking kommuniziert werden. [Nicky Loh/Bloomberg]
