Gefahren des Online-Banking – Ansprüche gegen Banken möglich

Bereits seit einigen Jahren preisen die Banken ihre Online-Banking-Modelle an. Warum auch nicht, denn dass Online-Banking ist für viele Bankkunden eine sehr bequeme Möglichkeit, Bankgeschäfte von zu Hause aus abzuwickeln.

Für die Banken hat es den großen Vorteil, dass ein Massengeschäft schnell und ohne großen Personalaufwand kostengünstig angeboten werden kann. Durch die vereinfachte Abwicklung und die Einsparung von Personalkosten haben die Banken ein verstärktes Interesse daran, dass ihre Kunden Online-Banking nutzen.

Dabei werden die eigenen Online-Banking-Modelle durch die Banken nur allzu gerne als völlig sicher beschrieben. Dabei sind Anweisungen und Buchungsvorgänge über das Internet alles andere als „völlig sicher“. Wie sich nicht zuletzt auch durch die von Edward Snowden ausgelöste Spionageaffäre gezeigt hat, können Daten sehr leicht abgefangen und manipuliert werden. Nicht nur Staaten versuchen im großen Stil an die Daten der Internetuser zu kommen. Auch die Bankdaten der Online-Banking-Nutzer sind bereits seit längerem ein beliebtes und gewinnbringendes Ziel für Betrüger geworden.

Die Anwaltskanzlei Lenné berät immer wieder Bankkunden, die Opfer eines Internetbetruges beim Online-Banking geworden sind.

Es kommt keineswegs selten vor, dass ein Online-Banking-Nutzer Tage nachdem er die letzte Anweisung gegeben hat oder in seinem Benutzerkonto angemeldet war, plötzlich feststellt, dass Geld von seinem Konto an für ihn fremde Personen überwiesen wurde.
Oftmals ist es dann aber auch schon zu spät, denn die Betrüger leiten die Zahlungen umgehend ins Ausland weiter.

Wie funktioniert das? Phishing, Malware und DNS-Spoofing

Die Betrüger haben es in diesen Fällen zumeist geschafft, eine Schadsoftware auf dem PC des Opfers zu installieren. Diese Schadsoftware, zumeist bekannt unter dem Namen „Trojaner“, kundschaftet die geheimen Bankdaten aus und übermittelt diese an die Betrüger. Mit PIN und TAN der Opfer können die Betrüger dann die Überweisungen vornehmen.

Eine andere Möglichkeiten an die Daten der Opfer zu kommen ist das sog. „Phishing“. Dabei wird der Bankkunde per Email oder Telefon unter einem Vorwand aufgefordert seine geheimen Bankdaten preiszugeben. Tun Sie dies niemals!

Ihre Bank wird Sie niemals auffordern Ihre PIN, TAN oder sonstige Zugangsdaten zu übermitteln, außer beim eigentlichen Online-Banking-Vorgang natürlich.

Bereits das bloße Anklicken einer „Phishing-Email“ kann dazu führen, dass ein sog. Trojaner unbemerkt Zugang zu Ihren Daten bekommt.

Andere Möglichkeiten wie die Betrüger an Ihre Daten gelangen, sind z. B. die Nutzung von „Malware“ und „DNS-Spoofing“. In solchen Fällen bemerken Sie gar nicht, dass Sie die Daten nicht an Ihre Bank, sondern an einen Dritten übermitteln.

Wie schütze ich mich?

Schützen Sie Ihren PC mittels eines **Antivirenprogramms** und einer **Firewall**. Sie sind verpflichtet Vorkehrungen zum Schutz Ihrer Daten zu treffen. Öffnen Sie keine Anhänge von Emails deren Absender Sie nicht kennen. Oft ist in dem Anhang einer Phishing-Email ein Virusprogramm enthalten, welches Ihre Daten an die Betrüger übermittelt.

Wenn Sie bereits Nutzer des TAN/iTAN-Verfahrens sind, wechseln Sie zu den neueren Chip-TAN und M-TAN-Verfahren. Aber auch bei diesen Verfahren kontrollieren Sie immer die von Ihnen eingegeben Daten des Lesegerätes. Auch diese Systeme sind nicht hundertprozentig sicher.

Achten Sie auf Unregelmäßigkeiten bei der Ausführung von Zahlungsanweisungen (z. B. kurzes Flackern des Bildschirms, ungewöhnliche Aufforderung einen Kontrollbetrag einzugeben, Fehlermeldungen, ungewöhnliches Layout der Seite, fehlerhafte Grammatik und Rechtschreibfehler auf der Seite). Zögern Sie nicht, melden Sie ungewöhnliche Vorgänge sofort.

Was tun im Schadensfall?

Wenn Sie eine Fehlbuchung bemerken, informieren Sie unverzüglich und nachweisbar Ihre Bank. Denn der Nutzer des Online-Banking ist verpflichtet seine Bank unverzüglich nach Feststellung eines nicht autorisierten oder fehlerhaft ausgeführten Zahlungsvorgangs zu unterrichten.

Es besteht dann oftmals die Möglichkeit, den überwiesenen Betrag von der Bank wieder gutgeschrieben zu bekommen. Der Gesetzgeber hat bei der letzten Gesetzesnovelle für solche Fälle einen **Anspruch auf Gutschrift des unberechtigt abgebuchten Betrages** geschaffen.

Rechtsanwalt Kutz aus der Anwaltskanzlei Lenné: *„Grundsätzlich haftet eine Bank gegenüber ihrem Kunden, wenn diese eine nicht autorisierte Überweisung vornimmt und der Kunde seinen PC vor Angriffen von außen geschützt hat. Die Bank zieht schließlich ihre Vorteile aus dem Online Banking und muss daher auch mit für die Risiken einstehen.“*

Für eine zuverlässige Bewertung der Erfolgsaussichten, ist eine Einzelfallbetrachtung jedoch unerlässlich. Wenn Sie Opfer eines solchen Internetbetruges geworden sind, kontaktieren Sie uns. Wir helfen Ihnen gerne, die oftmals bestehenden Ansprüche gegen Ihre Bank durchzusetzten.

Kontaktieren Sie uns.

Lenné
Anwaltskanzlei

Anwaltskanzlei Lenné · Max-Delbrück-Str. 18 · 51377 Leverkusen · Telefon (0214) 909840-0 · Telefax (0214) 909840-29 · info@anwalt-leverkusen.de · www.anwalt-leverkusen.de
Standort München · Brienner Straße 44 · 80333 München · Telefon (089) 21552745 · Telefax (0214) 21552746 · info@anwalt-muenchen.de · www.anwalt-muenchen.de