30. August 2023

IBAN & Co geklaut: Gefahren für Betroffene des Bank-Datenlecks

Immer wieder sind wegen Software-Sicherheitslücken Kundendaten großer Banken und Versicherungen durchgesickert. Von solchen Datenlecks waren unter anderem die Deutsche Bank, Verivox und die Barmer Versicherung betroffen. Abgefangen wurden dabei unter anderem auch Daten zu Bankverbindungen. Ein Großteil der Datenlecks stand in Verbindung mit der Software MOVEit. Dabei handelt es sich um ein weit verbreitetes Tool zur Datenübertragung. Die Sicherheitslücke in dem Programm scheint Medienberichten zufolge von Cyberkriminellen massiv ausgenutzt worden zu sein.

Was müssen Bankkunden jetzt beachten?

Daher sollten insbesondere Bankkunden aktuell regelmäßig ihre Kontoaktivitäten überprüfen. Wer eine unbekannte Abbuchung entdeckt, sollte umgehend die Bank kontaktieren und die Buchung stornieren. Das ist bis zu 13 Monate später noch möglich. Dabei sollte vor allem nach kleineren Buchungen Ausschau gehalten werden. Die Abbuchung großer Summen fällt schnell auf aber die Cyberkriminellen nehmen häufig viele kleinere Abbuchungen vor. Es wurde von Fällen berichtet, in denen im Verwendungszweck der Überweisung der Name eines Discounters auftauchte.

Banken wie die Sparkasse raten in den Medien zunächst einmal dazu, Ruhe zu bewahren. Alleine mit den Kontodaten könnten die Hacker noch keinen großen Schaden anrichten. Schließlich seien die Kontodaten ohnehin nicht nur dem Kontoinhaber bekannt. Daten wie IBAN und BIC sind jeder Person zugänglich, der man Geld überwiesen, eine Rechnung geschickt oder eine Einzugsermächtigung erteilt habe.

So können Kriminelle die abgegriffenen Daten nutzen

Das ist allerdings nicht ganz richtig. Zwar können die Daten nicht genutzt werden, um beispielsweise Geld abzuheben, dafür aber um Einkäufe im Internet zu tätigen. Denn die Hacker können mittels der abgegriffenen IBAN und dem Namen des Kontoinhabers in einem Online-Shop durchaus per Lastschrift bezahlen.

Außerdem nimmt für betroffene Bankkunden die Gefahr zu, Opfer von Phishing-Attacken zu werden. Denn mit den Kontodaten können Cyberkriminelle solche Betrugsmails sozusagen auf den jeweiligen Kunden personalisieren. Phishing-Mails sind ohnehin immer schwerer zu erkennen, da sie nahezu authentisch aufgebaut sind. Mit dem Namen des Kontoinhabers und der entsprechenden Kontonummer wirken sie dann umso echter. Phishing-Mails könnten jetzt außerdem Bezug auf das Datenleck nehmen und beispielsweise aus Sicherheitsgründen zu einem Passwortwechsel raten oder um die Eingabe einer TAN bitten. Hier ist Vorsicht geboten. Grundsätzlich sollte in solchen Mails niemals auf den enthaltenen Link geklickt werden, sondern die Mail sicherheitshalber gelöscht werden.

Auch bei Telefonanrufen von vermeintlichen Bankmitarbeitern ist Vorsicht geboten. Im Zweifelsfall sollte man den Anruf beenden und die Bank selbst über eine bereits bekannte Telefonnummer anrufen. Es könnte außerdem zu Erpressungsversuchen kommen, bei denen die Kriminellen den Datenleck-Opfern mit der Veröffentlichung ihrer persönlichen Daten drohen. Grundsätzlich gilt: Je mehr Daten abgegriffen wurden, umso mehr Missbrauchsmöglichkeiten gibt es. Wenn also neben der Kontonummer weitere persönliche Informationen wie Geburtsdatum, Postanschrift, E-Mail-Adresse usw. erbeutet wurden, steigt die Gefahr von Betrugsversuchen.

Erhöhte Gefahr fürs Online-Banking?

Für das Online-Banking selbst besteht erst einmal keine erhöhte Gefahr, denn um Überweisungen vom Konto vorzunehmen, genügt die Kontonummer bzw. IBAN allein nicht. Mit dem Passwort für die Anmeldung im Online-Banking-Portal, der TAN-Abfrage, der App auf dem Smartphone und einer möglichen Zwei-Faktor-Authentifizierung sind die Zugänge zum Online-Banking vergleichsweise sicher.

Das heißt jedoch nicht, dass die abgegriffenen Daten hier keinerlei Bedrohung darstellen. Das Risiko für den Missbrauch des Kontos ist definitiv erhöht. So könnten Kriminelle die IBAN unter Umständen nutzen, um z. B. über eine Telefonhotline das Passwort zurücksetzen zu lassen.

Konto wechseln: ja oder nein?

Wer von seiner Bank, Versicherung usw. darüber informiert wurde, dass er konkret vom Datenklau betroffen ist, der kann sicherheitshalber seine Kontonummer bzw. die IBAN wechseln. Dass bisher nichts passiert ist, muss in diesem Fall keine Entwarnung darstellen. Denn die Betrüger schlagen nicht zwangsläufig sofort zu. Auch Jahre später können die geklauten Daten noch zu Betrugszwecken eingesetzt werden.

Zwar ist der Wechsel zu einem neuen Konto mit großem Aufwand verbunden, weil sämtliche Sepa-Lastschriftverfahren neu ausgefüllt und die neue Nummer auch Dritten, die Überweisungen auf das betreffende Konto vornehmen, übermittelt werden muss. Ein solcher Wechsel ist jedoch zweifelsfrei die sicherste Option.

Wichtig: Es sollte dabei nicht auf Dienstleister zurückgegriffen werden, die die Abwicklung solcher „Kontoumzüge“ anbieten. Denn hier droht das nächste Datenleck. Schließlich ist MOVEit ein ebensolcher Anbieter.

Bankkunden, die sich nicht sicher sind, ob sie vom Datenleck betroffen sind, können durchaus erst einmal abwarten. Wer jedoch eine auffällige Kontobewegung bemerkt oder Ziel einer personalisierten Phishing-Attacke wird, der sollte nicht länger abwarten und schnellstmöglich wechseln, denn dann ist klar, dass die persönlichen Daten abgegriffen wurden.

Haben Betroffene Anspruch auf Schadensersatz?

Opfer solcher Datenlecks haben u. U. die Möglichkeit, auf Schadensersatz zu klagen. Nach einer Sicherheitslücke bei Mastercard erhielten die Opfer z. B. über 300 Euro. Wenn auch Sie von dem Datenleck betroffen sind, beraten wir Sie gern im Rahmen eines kostenlosen Erstgesprächs zu den möglichen rechtlichen Schritten in Ihrem Fall.

Guido Lenné

Rechtsanwalt aus der Anwaltskanzlei Lenné.
Rechtsanwalt Lenné ist auch Fachanwalt für Bank- und Kapitalmarktrecht.

Wir helfen Ihnen gerne! Kontaktieren Sie uns. Oder vereinbaren Sie hier online einen Termin für eine telefonische kostenfreie Erstberatung.

Lenné
Anwaltskanzlei

Zurück

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