

17. November 2023

## **Datenleck bei „Move it“: So viele Bankkunden sind wirklich betroffen**

Nach dem Hackerangriff auf den Kontowechsel-Dienstleister Majorel wurde nun bekannt, dass deutlich mehr Datensätze von Bankkunden erbeutet wurden als bislang angenommen. Medienberichten zufolge erbeuteten die Hacker über 144.000 Datensätze.

### **Von diesen Banken wurden Kundendaten abgegriffen**

Wie bereits aus den Medien hervorging, war die Postbank am stärksten von der Hackerattacke betroffen: Hier wurden etwa 60.444 Datensätze von Kunden abgegriffen. Vom Mutterkonzern Deutsche Bank wurden Informationen zu 13.179 Kunden erbeutet. Am zweitstärksten von dem Hackerangriff betroffen ist die ING Deutschland mit ca. 17.129 Datensätzen. Von der Direktbank Norisbank wurden 5.222 personenbezogene Daten abgegriffen.

Wie sich nun herausstellt, haben die Hacker außerdem 9.744 Datensätze der Oldenburgischen Landesbank (OLB) abgegriffen. Die GLS-Bank ist mit 1.706 erbeuteten Kundendaten ebenfalls von dem Datenleck betroffen. Gleiches gilt für die österreichische Bank99 mit 18.835 Datensätzen.

### **Das Datenleck bei Majorel**

Erbeutet wurden diese Daten im Zuge eines Hackerangriffs auf das Luxemburger Unternehmen Majorel. Das deutsche Tochterunternehmen Kontowechsel24.de war ebenfalls betroffen. Kontowechsel24.de arbeitet im Auftrag von Geldhäusern, um den Kunden den Bank- bzw. Kontowechsel zu erleichtern. Diese Dienstleistung erfolgt im Hintergrund, das heißt, die Kunden wissen in der Regel nicht, von wem der Kontowechsel tatsächlich durchgeführt wird.

Bei dem Cyberangriff auf Majorel wurde konkret eine Exceltabelle erbeutet, die Informationen zu sämtlichen Wechselaufträgen aus den Jahren 2016 bis 2020 enthielt, unter anderem die Vor- und Nachnamen der Bankkunden sowie deren neue Kontonummern bzw. IBANs.

## **Hackergruppe CI0p verantwortlich**

Der Angriff erfolgte durch die Hackergruppe CI0p, die in erster Linie im russischsprachigen Raum aktiv ist. Die Gruppe arbeitet vorrangig mit Ransomware. Das heißt, die Hacker verschaffen sich Zugriff auf die IT-Systeme ihrer Opfer, kopieren die Daten und fordern dann Lösegeld. Wer die Zahlung verweigert, dessen Daten werden im Darknet veröffentlicht.

Für die Cyberattacke auf Majorel nutzte die Hackergruppe CI0p eine Schwachstelle im Dateitransferprogramm „Move it“. Die Sicherheitslücke in der Software blieb monatelang unentdeckt. Mehr als 260 Unternehmen, Banken und Behörden sind davon betroffen. Im Juni 2023 hatte Majorel den Angriff bestätigt. Kurz darauf hieß es seitens des Kontowechsel-Dienstleisters, die Lücke sei „nach Bekanntwerden unverzüglich geschlossen und alle notwendigen Maßnahmen ergriffen“ worden. Doch zu dem Zeitpunkt waren bereits über 144.000 Datensätze von Bankkunden ins Darknet gelangt.

## **IT-Systeme der Banken scheinbar nicht betroffen**

Die Deutsche Bank bestätigte gegenüber den Medien, dass es sich bei den abgegriffenen Informationen um Daten gehandelt habe, die „zum Zeitpunkt des Vorfalls zu einem erheblichen Teil nicht mehr aktuell“ gewesen seien. Der Datenklau betreffe außerdem ausschließlich Kunden, die von der Kontowechselhilfe Gebrauch gemacht hätten. Da in der Tabelle einige Kunden scheinbar mehrfach gelistet waren, seien außerdem mehr Datensätze als Personen betroffen.

Sowohl die Deutsche Bank als auch die ING betonten außerdem, dass ihre eigenen IT-Systeme zu keinem Zeitpunkt von dem Datenleck betroffen waren.

## **Vermehrt Kritik an Majorel**

In Presseberichten wird inzwischen seitens der Banken Missfallen über das Verhalten des Kontowechsel-Dienstleisters laut. So soll Majorel die ING Deutschland nicht darüber informiert haben, dass bei dem Angriff mehr Kundendaten betroffen waren als ursprünglich gedacht. Das habe das Finanzinstitut erst durch eigene Recherchen herausgefunden.

Außerdem kritisieren einige Banken die Tatsache, dass der Dienstleister die betroffenen Daten überhaupt noch gespeichert hatte. Diese hätten längst gelöscht werden müssen. So heißt es auf der Website von Kontowechsel24.de, dass personenbezogene Daten „in der Regel nach spätestens 365 Tagen gelöscht“ würden. Vom Datenklau betroffen waren aber Daten aus den Jahren 2016 bis 2020.

## **Banken schalten externe Prüfer ein**

Die Deutsche Bank will die Aufklärung des Vorfalls nun scheinbar selbst in die Hand nehmen und hat inzwischen eine Wirtschaftsprüfungsgesellschaft damit beauftragt, die Vorgänge rund um die Cyberattacke zu prüfen. Die ING soll Majorel gedrängt haben, selbst einen Wirtschaftsprüfer

einzuschalten. Medienberichten zufolge sollen die Wirtschaftsprüfungsgesellschaften bereits mit der Untersuchung des Vorfalls begonnen haben.

In der Anwaltskanzlei Lenné machen wir uns für die Rechte der vom Datenklau betroffenen Bankkunden stark. So haben Opfer solcher Datenlecks häufig die Möglichkeit, auf Schadensersatz zu klagen. Wenn auch Sie zu den betroffenen Bankkunden zählen, deren persönliche Daten im Darknet veröffentlicht wurden, beraten wir Sie gern im Rahmen eines kostenlosen Erstgesprächs zu möglichen rechtlichen Schritten.

[Guido Lenné](#)

Rechtsanwalt aus der Anwaltskanzlei Lenné.

Rechtsanwalt Guido 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.

- [Facebook](#)
- [Twitter](#)
- [WhatsApp](#)
- [E-mail](#)

[Zurück](#)

