15. Dezember 2023

Skimming 2.0: Konto am Geldautomaten geplündert

Aktuell kursiert eine modernisierte Form der Skimming-Betrugsmasche, die scheinbar gezielt jüngere Bankkunden ins Visier nimmt. Dabei versenden Kriminelle eine manipulierte SMS, um an die Konto-Zugangsdaten zu gelangen und später mithilfe von Smartphones die Konten ihrer Opfer zu plündern. Der Fall, durch den die Behörden auf das sogenannte Skimming 2.0 aufmerksam wurden, wird derzeit vor dem Amtsgericht Frankfurt verhandelt.

Die ursprüngliche Betrugsmasche

Beim bereits bekannten Skimming lasen Kriminelle die Informationen auf dem Magnetstreifen der Kredit- oder Girokarten (Debitkarten) an Geldautomaten bzw. Zahlungsterminals aus, um so ein Duplikat der Karte zu erstellen, mit der sie dann Bargeld abheben oder Einkäufe tätigen konnten. Da der Magnetstreifen in Deutschland aber nicht mehr zum Einsatz kommt, weil Transaktionen und Geldabhebungen inzwischen über den Chip auf der Karte abgewickelt werden, stellte diese Betrugsmasche zuletzt keine besondere Gefahr mehr dar. Allerdings wird der Magnetstreifen von Banken im nicht-europäischen Ausland nach wie vor genutzt.

Konkret manipulierten die Betrüger beim Skimming 1.0 zum Beispiel Geldautomaten, indem sie ein zusätzliches Lesegerät vor dem Kartensteckplatz installierten, welches dann die Konto-Informationen auf dem Magnetstreifen speicherte. Um an die zugehörige PIN zu gelangen, wurde dann noch eine kleine Kameraleiste über der Tastatur angebracht, mit der die PIN-Eingabe gefilmt wurde. Und schon konnten die Kriminellen mit dem Duplikat der Karte mit allen Kontodaten und der dazugehörigen PIN Bargeld abheben oder an Kartenterminals bezahlen.

So funktioniert Skimming 2.0

Auf die neue, modernisierte und wesentlich unaufwendigere Betrugsmasche sind die Behörden durch reinen Zufall aufmerksam geworden. Eine Polizeistreife hatte in Königstein einen Mann bemerkt, der einen Geldautomaten auszuspähen schien. Die Polizisten gingen davon aus, dass er diesen möglicherweise sprengen wollte. Bei der Kontrolle stellten die Beamten jedoch fest, dass der Verdächtige ungewöhnlich viele Smartphones bei sich hatte, auf denen jeweils die Zugangsdaten verschiedener fremder Bankkonten gespeichert waren.

Wie die Ermittlungen ergaben, versenden die Kriminellen beim Skimming 2.0 zunächst eine SMS, die vermeintlich von der Bank kommt und die Empfänger auffordert, ihre Online-Banking-Zugangsdaten anzugeben. Tun sie das, kann automatisch eine neue digitale Debitcard erstellt werden. In den meisten Fällen ist es für die Opfer dann bereits zu spät. Die einzige Chance, den Betrug noch rechtzeitig aufzudecken, bestünde darin, dass der Kontoinhaber die Einstellungen im Online-Banking zeitnah prüft und dort auf die neue Zahlungsdienst-App aufmerksam wird. Dann könnte diese noch rechtzeitig entfernt werden, bevor die Betrüger Geld abheben können. In der Regel bemerken Geschädigte den Betrug jedoch erst, wenn die Kriminellen das Konto bereits geplündert haben.

Bargeldabhebungen vor und nach Mitternacht von mehreren Konten

Bei dem Mann, der von der Polizei aufgegriffen wurde, handelte es sich scheinbar um einen sog. „Abholer“. Nach erfolgreichem Datenklau per SMS werden diese Abholer von den Drahtziehern mit verschiedenen Mobiltelefonen ausgestattet, die jeweils mit einer digitalen Debitkarte verknüpft sind. So kann dann an Geldautomaten Bargeld von mehreren Konten abgehoben werden. Der Grund, warum dafür viele verschiedene Smartphones benötigt werden, ist, dass die Geldautomaten erkennen können, ob mit einem Telefon bereits eine bestimmte Summe abgehoben wurde.

Mithilfe einer Vielzahl von Handys, die jeweils mit unterschiedlichen digitalen Debitkarten verbunden sind, können die Täter dann an Geldautomaten sowohl vor als auch nach Mitternacht das jeweilige Tageslimit abheben und so pro Konto gleich zweimal abkassieren. Im Fall des in Königstein verhafteten Mannes hat sich herausgestellt, dass er offenbar Teil einer organisierten Gruppe ist, die in ganz Deutschland zu operieren scheint. Die Ermittlungen haben ergeben, dass der Mann mindestens einen Komplizen gehabt haben muss. Denn obwohl er bei seiner Festnahme kein Bargeld bei sich hatte, konnte nachgewiesen werden, dass mit den Smartphones fortlaufend Geld abgehoben wurde.

Opfer von Skimming 2.0: Was kann ich tun?

Kontoinhaber, die Opfer dieser Betrugsmasche geworden sind, sollten schnell handeln und ihr Konto bzw. alle Transaktionen sperren lassen, um weiteren Schaden zu vermeiden. Zumindest aber sollten sämtliche Passwörter und Sicherheitsfragen geändert werden, die mit dem Bankkonto in Verbindung stehen. Wenn möglich und sofern noch nicht geschehen, empfiehlt es sich, die Zwei-Faktor-Authentifizierung für das Konto zu aktivieren. Außerdem sollten Betroffene Anzeige bei der Polizei stellen.

In der Anwaltskanzlei Lenné stehen wir Geschädigten in solchen Situationen mit Rat und Tat zur Seite. So beraten wir Sie zu Ihren Rechten und Pflichten als Geschädigter, helfen Ihnen ggf. dabei, relevante Beweismittel korrekt zu sichern, und unterstützen bei der Kommunikation mit der Bank. Zudem prüfen wir, ob in Ihrem Fall Anspruch auf Schadensersatz besteht, und setzen diesen für sie

durch. Bei einem kostenlosen Erstgespräch beraten wir Sie gern.

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.

- Facebook
- Twitter
- WhatsApp
- E-mail

Zurück