bankenverband

Blog

SIM-Swapping: Wenn Betrüger die Mobilfunknummer kapern

07.10.2021

von

Altmann, Kathleen

Schlagworte

Cybersicherheit
Online-Shopping
Verbraucher
Onlinebanking
TAN
Cyberkriminalität
Sicherheit Verbraucher

„Swapping“ kann sehr nützlich sein. In der Computerwelt bezeichnet es den Vorgang, Daten auf ein anderes Medium zu transferieren, um beispielsweise mehr Speicher und Arbeitskapazität zu gewinnen. Unangenehm wird es aber, wenn Kriminelle Daten widerrechtlich auf ein fremdes Handy umleiten. Und das funktioniert so: Das Handy wird inzwischen sehr häufig für den Zugang zum eigenen Onlinekonto oft als zweiter Faktor für den Identitätsnachweis genutzt. Passwörter oder SMS werden auf das Handy gesandt und so der Zugang freigegeben. Die Betrugsmethode SIM-Swapping setzt genau an dieser Stelle an. Zunächst verschaffen sich die Kriminellen Zugriff auf die Handynummer bzw. die SIM-Karte ihres Opfers. Sind sie damit erfolgreich, werden alle SMS und Anrufe auf ein

fremdes Handy umgeleitet. Wie funktioniert die Methode und wie können Sie sich schützen?

Mobilfunknummern sind mit der Zeit immer wichtiger geworden. Inzwischen sind sie regelmäßig auch mit den Social-Media-Konten verknüpft oder notwendig, um solche Accounts wiederherzustellen. Und speziell bei Bankgeschäften wird das Mobiltelefon oft zum Einloggen zum Onlinebanking verwendet oder ist für die Freigabe von Aufträgen wichtig. Denn grundsätzlich muss jede einzelne Überweisung, jedes Wertpapiergeschäft oder jeder Anmeldevorgang zusätzlich mit einer Transaktionsnummer (TAN) freigegeben werden. Je nach TAN-Verfahren funktioniert das z. B. über die photoTAN-App oder per SMS.

Wofür die Mobilfunknummer missbraucht werden kann

Missbrauchen Kriminelle Ihre Mobilfunknummer, können sie sich Ihre SMS und Anrufe weiterleiten. Zudem können Online- oder E-Mail-Konten übernommen werden, sobald Ihre Mobilfunknummer über die Funktion „Passwort vergessen“ mit den betreffenden Konten verknüpft ist. Gelangen Kriminelle zudem an die Zugangsdaten zu Ihrem Onlinebanking, können sie mit den TANs, selbst Überweisungen von Ihrem Konto auf fremde Konten vornehmen.

So funktioniert die Masche im Einzelnen

Ein Weg wie Kriminelle an die SIM-Karte gelangen können: Sie täuschen den Mobilfunkanbieter über ihre Identität. Dem Mitarbeiter der Kundenhotline gegenüber oder über das Kundenportal geben sie sich überzeugend als Besitzer dieser Telefonnummer aus und beantragen eine neue SIM-Karte.

Die Geschichte, die dabei erzählt wird, kann beispielsweise wie folgt lauten: Das Handy mit der SIM-Karte sei verloren gegangen und nun benötige man eine neue SIM-Karte. Oder: Für das angeblich neue Smartphone passt das Format der SIM-Karte nicht mehr, daher wird dringend eine neue Karte benötigt.

Der Mobilfunkanbieter könnte dann Ihre Telefonnummer für eine neue SIM-Karte aktivieren. Was folgt, ist für die Kriminellen einfach umzusetzen: Sie greifen den an Sie adressierten Brief mit der neuen SIM-Karte ab oder lassen sich noch einfacher die SIM-Karte an eine „neue“ Adresse schicken.

In einer anderen Variante dieser Betrugsmethode kündigen die Kriminellen Ihren Mobilfunkvertrag und beantragen die Rufnummernmitnahme zu einem neuen Mobilfunkanbieter.

Grundsätzlich lassen Mobilfunkanbieter natürlich Sorgfalt walten und geben nicht einfach neue SIM-Karten heraus. Zudem stellen sie meist hohe Anforderungen an die Kündigung eines Mobilfunkvertrages. Aber dennoch ist es möglich, dass

Kriminelle es schaffen, mit ihrer Lügengeschichte durchzukommen: mit zusätzlich persönlichen Informationen, die sie vorab im Internet ausgespäht oder über die sozialen Netzwerke über Sie gesammelt haben. Auch Phishing ist eine beliebte Methode, um solche Daten abzugreifen. Die Betrüger können dann dem betroffenen Mitarbeiter gegenüber unter Umständen mit Informationen über Ihre Geburtsdaten, Ihre Adresse oder ein Kundenkennwort aufwarten.

SIM-Swapping erkennen

Wer aufmerksam bleibt und ein gesundes Misstrauen an den Tag legt, kann diese Angriffsmethode schnell aufdecken. Ein Indiz dafür, dass jemand Ihre Rufnummer quasi gestohlen haben könnte, ist beispielsweise, wenn Sie Sie von Ihrem Handy keine SMS mehr versenden können. Ein weiteres, dass auch Telefonate oder Anwendungen, die über die mobilen Daten laufen, nicht mehr möglich sind. Aber prüfen Sie, ob es sich nicht doch um ein Funkloch handeln könnte.

Tipps, um sich vor SIM-Swapping zu schützen

1. Spezielle Sicherheitsfrage für Identitätscheck bei Mobilfunkanbieter

Sie können bei vielen Mobilfunkanbietern für die Kontaktaufnahme eine PIN oder eine Sicherheitsfrage hinterlegen, die in allen Angelegenheiten rund um Ihren Mobilfunkvertrag zunächst abgefragt wird.

Das sollte eine PIN oder eine Sicherheitsfrage sein, die Sie bei keinem anderen Anbieter verwenden. Idealerweise sollte es für Außenstehende nicht möglich sein, auf diese über eine Recherche im Internet oder über die sozialen Netzwerke zu stoßen oder aus dort gefundenen Inhalten abzuleiten.

2. Über SIM-Karten-Wechsel informieren lassen

Meist können Sie sich von Ihrem Mobilfunkanbieter über alle Aktivitäten rund um Ihr Telefon bzw. SIM-Karte informieren lassen. Veranlassen Sie, dass Sie über einen Auftrag, auch noch einmal auf einem anderen Weg informiert werden, wie beispielsweise über eine Push-Nachricht.

3. Wenig Informationen über Internet und soziale Netzwerke preisgeben

Gerade weil Kriminelle gern die Daten ihrer späteren Opfer ausspähen, sollten Sie mit sämtlichen Informationen, die Sie über sich im Internet und vor allem über Ihre Social Media Accounts veröffentlichen, sparsam umgehen. Geben Sie nicht mehr von sich preis als unbedingt nötig.

4. Starke Passwörter für alle Konten wählen

Starke Passwörter brauchen Sie für alle Ihre Konten. Wichtig: Jedes Konto braucht ein eigenes Passwort. Wichtig: Verwenden Sie also nicht nur ein Passwort für alle! Ein starkes Passwort zu genieren erscheint auf den ersten Blick als große Herausforderung, aber tatsächlich ist es relativ einfach: Wählen Sie beispielsweise einen Satz, den Sie als kurios empfinden. An diesem Beispiel wird deutlich, wie es funktionieren kann: „Trinke Dein viertes Bier immer heimlich unter dem Tisch!“ Dieser Satz lässt sich gut merken, weil er kurios ist. Sie nehmen nunmehr jeweils die Anfangsbuchstaben bzw. Satzzeichen und Ziffern und schon haben Sie ein so genanntes starkes Passwort: „TD4.BihudT!“. Übrigens: Längere Passwörter sind schwerer zu knacken. Gönnen Sie Ihrem Passwort also eine gewisse Länge.

5. Keine Links in E-Mails oder SMS von Unbekannten öffnen

Mit abgefischten Informationen geben Sie den Kriminellen für sie wichtige persönliche Informationen in die Hand. Achten Sie darauf, dass Sie auf keine Links in SMS oder E-Mails klicken. Banken fragen niemals persönliche Daten über Links ab. Mehr Tipps zum Schutz vor Phishing erfahren Sie hier.

6. Kontobewegungen regelmäßig überprüfen

Wichtig ist, dass Sie Ihre Kontobewegungen im Blick behalten. Schauen Sie regelmäßig, möglichst ein bis zweimal in der Woche nach Ihren Kontoumsätzen. Fällt Ihnen etwas Ungewöhnliches auf, kontaktieren Sie umgehend Ihre Bank.