E- und I-Voting

INSIDE THE HACK

Handy tot, Bankkonto leer

Zwei Stunden nicht aufs Handy geschaut, und schon ist das Bankkonto leer, obwohl es per Zweifaktor-Authentifizierung geschützt ist. Die neue Methode krimineller Hacker heißt SIM-Swapping und wird bei Angreifern immer beliebter. ■ DAVID GÖHLER

Im Januar 2020 hat die spanische Polizei zusammen mit Europol einen Ring von zwölf Cyber-Kriminellen ausgehoben, die in mehr als 100 Fällen zwischen 6000 und 137.000 Euro – insgesamt über drei Millionen Euro – erbeutet hatten. Sie haben dazu über Phishing und Trojaner Bankzugangsdaten und andere persönliche Informationen abgefischt, um damit die Mobilfunkprovider zu überzeugen, eine neue SIM-Karte mit der alten Telefonnummer auszugeben. Sobald diese aktiv war, wurde das Konto durch Überweisungen leergeräumt und durch weitere Transfers verschleiert. Mit diesem Trick lässt sich auch die Zweifaktor-Authentifizierung zum Schutz des Kontos aushebeln.

Ausgangspunkt des Angriffs ist das Sammeln von persönlichen Daten der Opfer wie Geburtsdatum, Wohnort, Name, Handy-Telefonnummer und das Ausspähen der Bank-Zugangsdaten. Diese Daten greifen die Angreifer über Phishing-Angriffe, Trojaner, Social Engineering, über Social-Media-Seiten oder Daten ab, die bei einem Angriff erbeutet und im Darknet gehandelt werden. Die Bankzugangsdaten allein nützen den Hackern aber noch nicht viel, weil Bank-Transaktionen durch einen zweiten Faktor geschützt sind. Das ist oft eine TAN, die an das Handy mitgeteilt wird: per SMS oder Banking-App.

Die Angreifer müssen sich also irgendwie Zugriff auf den „Handy-Kommunikationskanal" verschaffen. Dazu wenden sie sich mit den abgegriffenen Informationen und gefälschten Dokumenten an den Mobilfunkprovider, um eine zweite SIM-Karte oder eine Ersatz-Karte zu bestellen und sich zuschicken zu lassen. Es gibt auch Varianten, bei der die Handy-Nummer auf eine bestehende SIM-Karte des Angreifers transferiert wird. Ist diese neue SIM-Karte aktiviert, steht den Kriminellen das Bankkonto offen und wird in aller Regel innerhalb von ein bis zwei Stunden komplett leergeräumt – meist, bevor das Opfer realisiert, dass nicht nur sein Handy keine Verbindung mehr ins Internet hat, sondern dass auch sein Geld weg ist. Das Geld fließt dann über weitere Konten in dunkle Kanäle.

Bei einem Verdacht sofort handeln

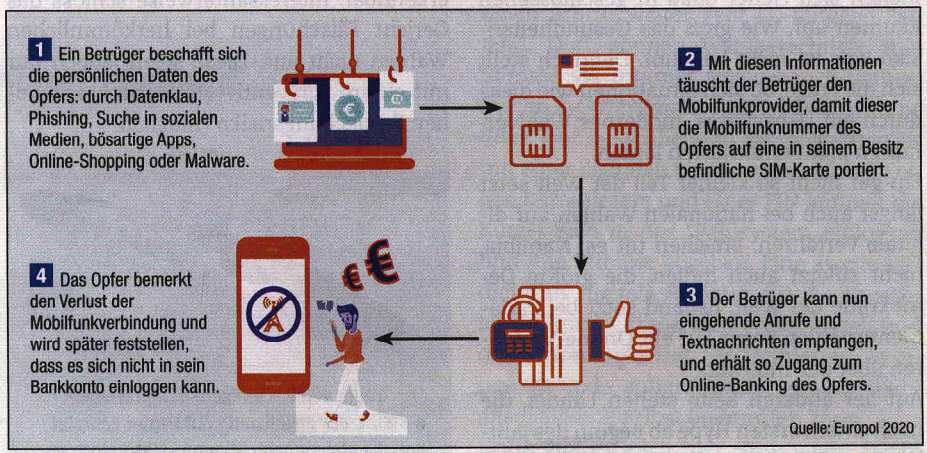
Wenn Ihr Smartphone plötzlich keine Verbindung mehr hat und in der Statusleiste die SIM-Karte als deaktiviert anzeigt, kontaktieren Sie umgehend Ihren Mobilfunk-Provider. Wenn dieser bestätigt, dass die Nummer auf eine andere SIM-Karte übertragen wurde, informieren Sie sofort die Polizei. Können Sie sich nicht mehr online in Ihrem Bankkonto einloggen, lassen Sie sofort den Online-Banking-Zugang sperren.

Der Knackpunkt dieses Angriffs ist das Abgreifen der persönlichen Daten für das Social Hacking, um den Mitarbeiter des Providers am Telefon zu überzeugen, dass man der legitime Besitzer des Anschlusses ist. Schützen Sie daher Ihre Daten:

- Klicken Sie nie auf Links in E-Mails oder SMS-Nachrichten, die Sie zu Ihrem Bankkonto führen wollen.
- Geben Sie keine persönlichen Daten an Unbekannte heraus.
- Verwenden Sie für jeden Internet-Account ein eigenes, sicheres Passwort.
- Laden Sie Apps nur in offiziellen App-Stores oder direkt beim Hersteller herunter.
- Vermeiden Sie die Herausgabe Ihrer Handy-Nummer.

Wenn Sie ganz sichergehen wollen, können Sie ein altes Handy mit einer eigenen Prepaid-Nummer nur für das Online-Banking einsetzen. ■

SIM-Swapping – ein Handy-Betrug



Beim SIM-Swapping ergattert ein Betrüger mithilfe von Social-Engineering-Techniken persönliche Daten, um anschließend die Kontrolle über Ihre SIM-Karte zu übernehmen.