Verbraucherzentrale Südtirol
Centro Tutela Consumatori Utenti
Die Stimme der VerbraucherInnen
La voce dei consumatori

Verbraucherzentrale Südtirol

Zwölfmalgreiner Straße 2
39100 Bozen
Tel. 0471 975597
info@verbraucherzentrale.it

Facebook-Datenklau: worauf VerbraucherInnen jetzt achten sollten

Mi, 14.04.2021 - 09:08

Auch Telefonnummern wurden verbreitet – Konten und Karten im Blick behalten!

Update zum 16.04.2021
Einige VerbraucherInnen fragen uns, warum wir auf eine ausländische Seite für die Kontrolle der betroffenen Daten verweisen. Die italienische Seite, welche diesen Dienst ebenfalls anbot, musste gemäß Auflagen des Garanten für Privacy den Dienst unterbrechen; die Entscheidung des Garanten scheint nicht wirklich nachvollziehbar.

Die Daten von 533 Millionen Personen, darunter mehr als 35 Millionen ItalienerInnen, wurden heuer online zum Verkauf angeboten. Die Daten wurden zwar anscheinend schon 2019 gesammelt, und das „Datenleck“ sei versiegelt, sagt Facebook – dennoch kann keine Entwarnung gegeben werden.

Welche Daten wurden verbreitet?
Man geht davon aus, dass Namen, Geburtsdaten, E-Mail-Adressen, Informationen aus der Facebook-Biografie sowie die Telefonnummern verbreitet wurden (auch jene, die als „uneinsehbar“ in Facebook eingetragen waren). Wirklich gravierend sind die Telefonnummern, denn vielfach werden die Sicherheitsabfragen für Online-Zahlungs- oder -Bankdienste per SMS verschickt, und die geklauten Telefonnummern könnten für Telefonbetrug oder Smishing verwendet werden.

Bin ich betroffen?
Auf der Website https://haveibeenpwned.com/ kann man kontrollieren, ob die eigenen Daten zu den geklauten gehören. Man gibt die E-Mail-Adresse ein, oder die Handynummer mit der internationalen Vorwahl, aber ohne die 2 führenden Nullen (also 39 gefolgt von den 10 Stellen der Handynummer, ohne Leerzeichen).

Was tun, um sich zu schützen?
Grundsätzlich gilt, auch abseits vom aktuellen Datenklau: die Kreditkarten- und Kontoauszüge sollten regelmäßig kontrolliert werden, um im Ernstfall schnell eingreifen zu können. Sollten Daten geklaut worden sein, sind diese „unsicher" zu betrachten, daher dürfen Sie nicht mehr für eine Zwei-Faktor-Identifizierung verwendet werden. Besser: direkt die Apps verwenden, auch wenn zu sagen ist, dass sich in vielen solcher Banking- oder Kreditkarten-Apps auch Softwareteile finden, die datenschutztechnisch nicht ganz einwandfrei sind. Doch in der Not, weiß der Volksmund, frisst der Teufel Fliegen …

Im Ernstfall
Sollte tatsächlich Geld von Karte oder Konto verschwinden, verlieren Sie keine Zeit: lassen Sie alles sperren, erstatten Sie Anzeige und fordern Sie die Beträge vom Finanzdienstleister zurück. Rat und Hilfe gibt es beim Beratungsdienst der VZS.

„Seit Einführung der zweiten Zahlungsdienstrichtlinie gibt es die Pflicht zur „starken" Authentifizierung bei den Online-Zahlungen. Viele Finanzdienstleister haben – wohl aus Kostengründen oder Marketingüberlegungen – das Handy der NutzerInnen als zweiten Faktor gewählt. Nicht nur VerbraucherschützerInnen, auch die europäischen Bankenaufsicht EBA sind nicht angetan von der Authentifizierung via SMS, denn zu leicht können diese abgefangen werden. Jedoch können wir auch die Verwendung von Apps anstelle der SMS zur Erstellung von Einmal-Passwörtern nicht befürworten: zu viele von ihnen scheinen zu sehr an den Daten der NutzerInnen interessiert. Die beste Lösung wäre ein „Token", der allein Passwörter generiert, und ansonsten nicht mit der Außenwelt kommuniziert, wie ihn auch einige lokale Banken bereits anbieten" fasst die Geschäftsführerin der Verbraucherzentrale Südtirol, Gunde Bauhofer, zusammen.

Gänzlich ungeklärt sind derzeit eventuelle rechtliche Folgen, die dieser Datenklau für Facebook haben könnte: aus den Aussagen des Konzerns, die nur auf Beschwichtigung abzuzielen scheinen, lässt sich wenig Bereitschaft für eine Übernahme der Verantwortung ablesen.

Die sichersten Daten sind immer noch jene, die nirgendwo veröffentlicht sind.