Foto: skyla80 Shutterstock.com

Für eine Handvoll Cent

Personendaten sind ein wertvolles Gut – für Unternehmen, aber auch für Betrüger. Wir haben getestet, wie viel Firmen für Verbraucherdaten zahlen und welche Informationen am Schwarzmarkt zu haben sind.

„Heute ist Wahltag in Wien! Nütze deine Stimme und entscheide, in welche Richtung Wien in Zukunft gehen soll. Beate Meinl-Reisinger". Zigtausende Bewohner der Bundeshauptstadt bekamen am 11. Oktober vergangenen Jahres eine SMS mit diesem Inhalt von der NEOS-Partei zugeschickt. Es dauerte nicht lange und es hagelte Kritik von allen Seiten. Es handle sich um verbotene Direktwerbung, monierten viele und fragten sich auch, woher die Partei überhaupt ihre Handynummer hatte. Wie diese später zugab, hatte sie die Nummern bei der Österreichischen Post erworben. Zu diesem Zweck verwenden hätte sie sie aber nicht dürfen, ließ ein Post-Sprecher daraufhin verlauten und legte Wert darauf, die Partei über die Einhaltung des Telekommunikationsgesetzes informiert zu haben.

Doch was sind solche Personendaten – beispielsweise Informationen wie Name, Adresse, Telefonnummer, Kaufkraft und Einkaufsverhalten – eigentlich wert? Woher werden sie bezogen? Was darf gespeichert und weitergegeben werden – und welche Infos sind tatsächlich über Unternehmen und im Internet organisierbar? Diesen Fragen sind wir mithilfe eines Experiments auf den Grund gegangen.

Zunächst richteten wir unsere Anfrage an die Firma Herold. Sie hat vor zwei Jahren mit der Übernahme von Teilen der Schober AG ihr Geschäftsfeld auf dem Gebiet stark erweitert und bietet seitdem nicht mehr nur den Kauf von Unternehmens-, sondern auch von Privatdaten an. Das Ergebnis: Herold arbeitet sauber. Das Unternehmen bot uns 7.500 passende Adressen zum Preis von 1.835 Euro netto an, jedoch nur im rechtlich erlaubten Lieferumfang, sprich: Anrede, Titel, Name, Postadresse und DVR-Nummer (eine siebenstellige Registrier-Nummer, die vom Datenverarbeitungsregister – DVR – vergeben wird) werden weitergegeben. Alle weiteren Merkmale, heißt es in dem Schreiben von Herold, dürfe man nicht übermitteln, sie seien aber in der Selektion berücksichtigt. Auch die Herausgabe von privaten E-Mail-Adressen ist rechtlich nicht erlaubt. Dafür bot die Firma aber an, an die gewünschte Personengruppe Werbe-Mails zu unserem Ansinnen zu verschicken. Die in der modernen Fachsprache als Stand-Alone-Mailing bezeichnete Werbeform, umgangssprachlich auch Spam genannt, ist für Herold ein weiteres Geschäftsfeld, wo gutes Geld gemacht werden kann. In einem Absatz informierte uns das Unternehmen zudem, dass es sich beim eventuellen Deal um eine Adressmiete handle. Man sei zur einmaligen Nutzung der Adressen berechtigt, dürfe diese aber weder speichern, verändern, noch an Dritte weitergeben. Eine Klausel, mit der sich Herold dagegen absichern möchte, eventuell datenschutzrechtlich belangt zu werden.

Der zweite Ansprechpartner, die Cebus AG mit Sitz in der Schweiz, war ebenfalls nur bereit, uns die rechtlich erlaubten Daten weiterzugeben, also den Namen und die Adresse der jeweiligen Konsumenten. Es wurde lediglich mitgeteilt, dass die Personen zu 60 Prozent weiblich seien und es eine sehr kauffreudige Personengruppe sei, für die Gesundheit und ein positives Leben an erster Stelle stünden. Die Kosten des Datensatzes beliefen sich auf 1.485 Euro netto. Weiters bot uns die Firma an, unser Werbeansinnen für 990 Euro netto an 25.000 private E-Mail-Adressen zu verschicken. Generiert habe sie diese Kundengruppe (fitness- & sportinteressierte Personen zwischen 18 und 40 Jahren, mittlere Kaufkraft) über Online-Gewinnspiele.

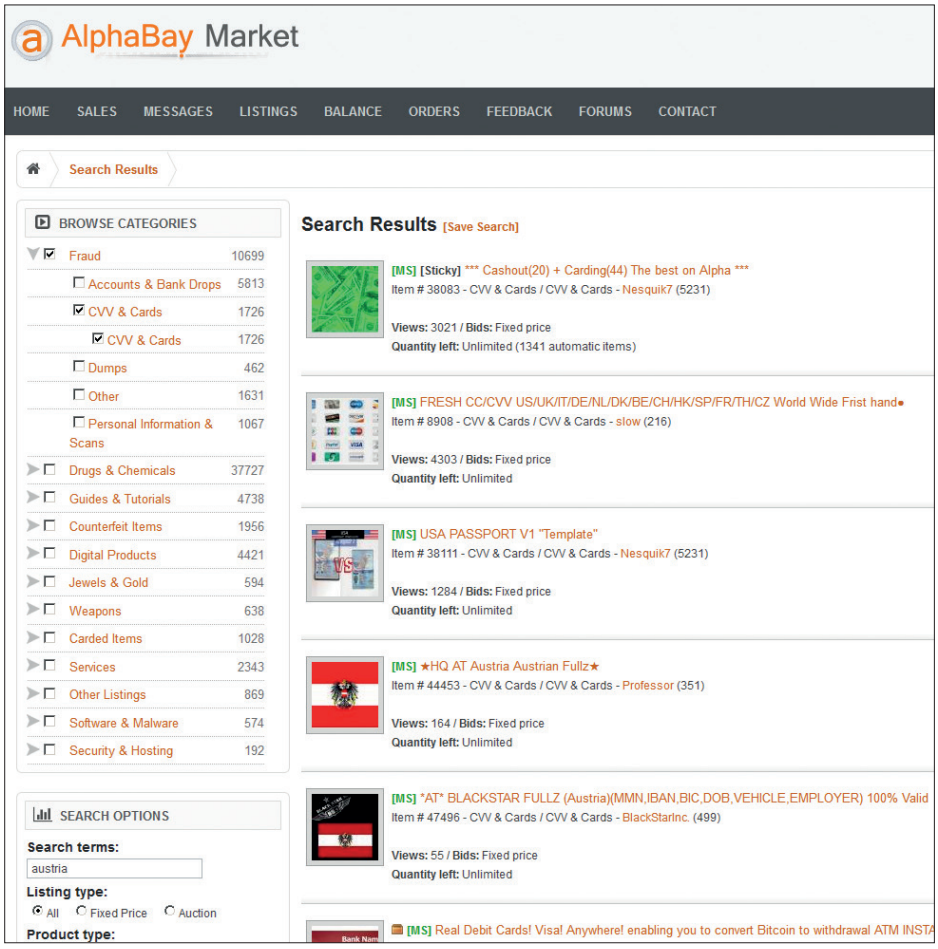
Datenkrake winkt ab

Eine Absage erhielten wir von Acxiom. Man habe nicht die passende Zielgruppe im Portfolio, antwortete der Konzern auf unser Schreiben. Das Unternehmen gilt als eine der größten Datenkraken der Welt. Es hilft dabei, über 250.000 Werbekampagnen jährlich an die passenden Konsumenten zu richten, gibt Jahr für Jahr 1,2 Milliarden E-Mail-Adressen weiter und prüft 8,4 Millionen Menschen hinsichtlich eventueller krimineller Hintergründe oder ihrer Kreditwürdigkeit. Ein wenig Bekanntheit erlangte das eigentlich eher im Schatten operierende Unternehmen zur Zeit des ersten US-Wahlkampfes von Barack Obama, der seine potenziellen Wähler damals dank Acxiom mit passgenauen Ansprachen umwarb. Die Spezialität des Unternehmens sind generell von Behörden gesammelte Offline-Daten – Informationen also, an die Google & Co nicht so leicht herankommen. Auch deshalb dürfte Facebook schon vor zwei Jahren eine Partnerschaft mit Acxiom abgeschlossen haben.

Fotos: JEFeatherston, Lane V. Erickson / Shutterstock.com Montage: Doris Seyser

Tiefendaten aus dem „Darknet"

Wesentlich brisantere Daten lassen sich auf dem Schwarzmarkt kaufen, wie Recherchen im sogenannten Darknet ergaben, jenem Netzwerk im Internet, in dem User anonym miteinander kommunizieren. Via Tor-Browser gelangten wir auf einen der derzeit



größten Internet-Schwarzmarktplätze, Alpha Bay Market, der – ähnlich aufgebaut wie eBay oder Amazon – allerhand kriminelle Waren und Dienstleistungen anbietet: von Waffen und Drogen aller Art über gestohlenen Schmuck, Gold und gefälschte Markenware bis hin zu Pässen, Führerscheinen und Kundendaten aus jeglichen Branchen und Ländern. Häufig feilgeboten werden Daten der Zahlungsdienstleister PayPal und Skrill (Userdaten und Passwörter), Premium-Accounts von Spotify und – in Hülle und Fülle – Kundendaten von Zalando. Auch Bank- und Kreditkartendaten lassen sich nach Belieben einkaufen. Zwei Beispiele: Für je 12,25 Dollar pro Kundenprofil bietet ein gewisser „Professor" folgende Infos zu in Österreich wohnhaften Personen an: Name, Geburtsdatum, Adresse, Telefonnummer, Bank- bzw. Kreditkartendaten, dazu seine IP-Adresse und die Plattform, von der aus die Daten abgesaugt worden sind. Der Dealer „BlackStar.Inc" bietet für 30 Dollar pro Profil noch viel mehr: Über die obigen Daten hinaus gibt es bei ihm Auskunft zum aktuellen Fahrzeug der Person, über ihren Beruf und noch genauere Daten zur Kreditkarte.

Vorsicht vor Phishing-Versuchen

Zu Bank- und Kreditkartendaten kommen die Hacker meist über digitale Einkaufsportale. Daher ist beim Shopping im Netz besondere Vorsicht geboten. Bei eher unbekannten Onlineshops einzukaufen stellt ebenso ein Risiko dar wie der Einkauf auf vielen E-Commerce-Portalen aus fernen Ländern, von denen wir nichts über datenschutzrechtliche Anforderungen wissen. So richtig sicher sind jedoch auch die bekannten großen Internetshops nicht, wie die vielen Offerte von Zalando-Konten im Darkweb zeigen. Neben einer gesunden Skepsis bei Onlineshops gilt es auch, sich vor Phishing-Aktionen zu hüten. Phishing, das sind Versuche, über gefälschte Webseiten, E-Mails oder SMS an Nutzerdaten zu gelangen. Meist wird eine vertrauenswürdige Seite nachgeahmt; etwa, wenn die Betrüger sich als Bank ausgeben und Nutzer an ungewöhnlicher Stelle dazu auffordern, beispielsweise Login-Daten anzugeben. Hierbei sollte der User darauf achten, dass die Seite, auf der er sich etwa in sein Bankkonto einloggt, HTTPS-geschützt ist. Wenn die Adresse mit „https://" beginnt, ist eher davon auszugehen, dass es sich um eine sichere Seite handelt. Weiters empfiehlt sich die Verwendung von sogenannten Reputation Plug-ins, zum Beispiel Webrep von Avast. Das Plug-in gibt Infos über die Seriosität einer Website, indem es die Bewertungen der Avast-Community hinsichtlich Inhalt und Sicherheit weitergibt.

Das Experiment

In dem Experiment gaben wir uns als Unternehmen aus, das ein neues Gesundheitsprodukt auf den Markt bringen möchte. Dafür sollten rund 7.500 Haushalte aus dem Raum Wien und Umgebung angeschrieben bzw. zu einem „Launch-Event" eingeladen werden. Die Zielgruppe sollte aus Privatpersonen (keine Firmenadressen) im Alter zwischen 25 und 55 Jahren bestehen, sie sollten über mittlere bis hohe Kaufkraft verfügen und in Familien leben. Auch alleinstehende Menschen wären möglich, wenn sie über ein hohes Einkommen verfügten. Weiters verlangten wir in der Personenbeschreibung nach lifestyle- und gesundheitsorientierten Menschen, am besten solchen, die sich im Internet ausgiebig über Krankheiten erkundigten und ein gewisses Angstverhalten gegenüber Krankheiten an den Tag legten. Von dieser Personengruppe wollten wir den Namen, die Adresse, die E-Mail-Adresse, die Kaufkrafteinschätzung und die Gesundheitsthemen, für die sich der jeweilige Verbraucher interessierte, übermittelt bekommen.

Rat und Hilfe für Verbraucher in Europa ECC-Net
Co-funded by the European Union

Dieser Artikel entstand im Rahmen der „Action 670702 – ECC-NET AT FPA", für welche das Europäische Verbraucherzentrum Österreich Förderungen aus den Mitteln des Verbraucherprogramms der Europäischen Union (2014–2020) erhält.

Mehr zum Thema

Bisher in KONSUMENT erschienen:

Google und der Datenschutz	1/15
Facebook und der Datenschutz	2/15
Amazon und der Datenschutz	3/15
WhatsApp und der Datenschutz	4/15
Mjam und der Datenschutz	5/15
Zalando und der Datenschutz	6/15
PayPal und der Datenschutz	7/15
Freemail-Dienste und der Datenschutz	8/15
Runtastic und der Datenschutz	9/15
Booking.com und der Datenschutz	10/15
Spotify und der Datenschutz	11/15
Virenschutzanbieter und der Datenschutz	12/15