Essen mit Folgen

Zahlreiche Personen werden seit Monaten von Telefonkeilern belästigt. Dabei hatten sie eigentlich nur über die Plattform mjam.at etwas zu essen bestellt.

Wenn der Magen ebenso leer ist wie der Kühlschrank und die Lust, jetzt noch außer Haus zu gehen, ihren Tiefpunkt erreicht hat, dann ist die Essensbestellung per Mausklick eine willkommene Alternative. Vereinfacht wird die Suche nach dem passenden Restaurant dank Onlineplattformen wie Mjam.at oder Lieferservice.at. Sobald sich der User registriert hat, sucht die Plattform nach geeigneten Anbietern in der Umgebung und listet sie auf. Hat der Kunde schon öfter bestellt, so werden ihm seine Lieblingsrestaurants vorgeschlagen. Ebenso einfach ist es mit der Bezahlung. Die ist per Sofortüberweisung, Kreditkarte, PayPal oder als Barzahlung an der Haustüre möglich. Auf jeden Fall genügen ein paar Klicks und wenig später wird die Mahlzeit ins Haus geliefert. Besonders attraktiv ist die Auswahl an Restaurants natürlich im städtischen Bereich, weshalb die Zahl der Nutzer vor allem in Wien recht groß ist.

Daher sind es vor allem Wiener, die seit Herbst letzten Jahres wiederholt mit aufdringlichen Anrufern konfrontiert sind. Teils mehrmals am Tag werden sie von sogenannten Scammern belästigt – Betrügern, die mit unterdrückter Nummer anrufen, über irgendwelche Gewinnspiele sprechen wollen, eine Kontonummer verlangen und nicht lockerlassen.

Zunächst war unklar, woher die penetranten Telefonkeiler die Nummern hatten. Dann fiel einigen Betroffenen auf, dass sie von den Anrufern mit einem falschen Namen angesprochen wurden. Es waren Namen, die sie bei der Essensbestellung genannt hatten. Außerdem kannten die Scammer die Adressen der Angerufenen. Wobei es nicht immer die Wohnadresse war, sondern eine, an die sich die Betroffenen zumindest einmal Mahlzeiten hatten liefern lassen. Die Online-Plattform, über die sie bestellt hatten, war in allen Fällen Mjam.at.

Daten öffentlich zugänglich

Im Dezember 2014 sah sich Mjam schließlich dazu veranlasst, auf den Vorwurf, dass es ein Datenleck im Unternehmen gegeben habe, zu reagieren. Am 16.12.2014 veröffentlichte Mjam in seinem Blog:

„Wir wissen von einigen Kunden, deren Kundendaten in die Hände einer Firma für Telefonwerbung gelangt sind. Als wir davon erfahren haben, wurde sofort Sec Consult GmbH eingeschaltet, eine international renommierte Security-Firma. Die Analyse hat ergeben, dass es bei Mjam kein Datenleck gibt." Den Betroffenen versprach das Unternehmen, in alle Richtungen zu ermitteln (blog.mjam.net/2014/12/16/klarstellung).

Mjam: vom Start-up zum Rädchen im Konzern

Das Essenslieferungsportal Mjam wurde im Jahr 2008 im Wiener Hacker-Labor Metalab von Angelo Laub gegründet. Zwei Jahre später übernahm Laub die Seiten asiazustellung.at und pizzaportal.at, 2011 ging er eine Partnerschaft mit willessen.at ein. Daraufhin wurde Mjam vom Konkurrenten Online-Pizza geschluckt, der wiederum vom deutschen Mitbewerber lieferheld.de gefressen wurde – der vom globalen Essensnetzwerk Delivery Hero übernommen worden ist. 2015 kaufte das Beteiligungsunternehmen Rocket Internet 39 Prozent der Anteile an dem Konzern. Das Unternehmen der Samwer-Brüder Marc Oliver und Alexander ist mit Jamba, einem Angebot an Klingeltönen und Mobiltelefonanwendungen, reich geworden. Dabei stand es immer wieder wegen des Verkaufs von Abos an Minderjährige in der Kritik.

Foto: Nils Z, Denis Semenchenko, solarseven / Shutterstock.com Montage: Erwin Haberl

Richtiges Verhalten im Internet

- Die eigene Telefonnummer im Internet nur dann preisgeben, wenn es notwendig ist, und im Zweifelsfall auf die jeweilige Anwendung verzichten.
- Nur Apps herunterladen, die man tatsächlich braucht und bei der Einwilligung zur Installation darauf achten, worauf die Anwendung Zugriff haben möchte
- Ändern Sie ein vom Anbieter zugeteiltes Passwort nach dem ersten Einloggen individuell und wechseln Sie auch sonst in regelmäßigen Abständen Ihre Passwörter.

Währenddessen forschten einige Betroffene auf eigene Faust im Internet – und machten dabei einen interessanten Fund. Auf der Seite Github.com, einem Hosting-Dienst für Software-Entwicklungsprojekte, war eine fünfstellige Zahl an Datensätzen von Mjam-Kunden öffentlich zugänglich. Mittlerweile wurden sie entfernt, jedoch dürften sie dort über ein Jahr gelegen sein. Doch es handelte sich bei diesen Daten nicht um jene, die von den Telefonbetrügern verwendet wurden, sondern um ältere E-Mail-Adressen, laut Mjam ohne Namensbezug, die von pizzaportal.at-Kunden stammten. Diese Webseite hat Mjam vor fünf Jahren übernommen.
Sowohl der Datenfund auf Github als auch der Umstand, dass neuere Kundendaten des Unternehmens in falsche Hände geraten sind, zeigt: So sicher, wie Mjam das in seinen AGB erklärt („ein hohes Datenschutzniveau ist uns ein Anliegen"), sind die Daten nicht – und dies lässt sich wohl auf andere Anbieter übertragen. Außerdem legt der Fall ein weiteres Manko offen – nämlich, dass potenziell gefährdete Kunden von Unternehmen, die von einem Datenleck betroffen sind, nicht zwingend informiert werden müssen.

IFNF fordert Informationspflicht

In dem Zusammenhang fordert der Verein Initiative für Netzfreiheit (IFNF), dass die Kundschaft unverzüglich über ein Leck in Kenntnis zu setzen ist, sobald ein Unternehmen davon erfährt. Wobei der IFNF zufolge in Österreich eine Rechtslücke besteht. Denn für Unternehmen gibt es keine allgemeine Verpflichtung, Betroffene über Datendiebstahl zu informieren – außer wenn dem Unternehmen bekannt wird „dass Daten aus einer seiner Datenanwendungen systematisch und schwerwiegend unrechtmäßig verwendet wurden und den Betroffenen Schaden droht" (§ 24 Abs. 2a Datenschutzgesetz). Das heißt: Die Voraussetzungen für die sogenannte „Data Breach Notification Duty" sind so hoch angesetzt, dass diese in der Praxis kaum zur Anwendung kommt, schreibt die Initiative in einer Aussendung. Denn es sei schwierig, einen Nachweis zu erbringen, dass ein Unternehmen nicht nur von einer schwerwiegenden Datenverletzung wisse, sondern auch noch ein konkreter Schaden drohe. Wobei sich hierbei auch das Problem zeigt, dass es noch immer keine abstrakte Definition eines Schadens beim Missbrauch personenbezogener Daten gibt.
Unterm Strich heißt das: Die Data Breach Notification Duty, die nur dann in Kraft tritt, wenn der Schaden halbwegs bezifferbar ist, ist eher zahnlos – eben darum, weil Schäden beim Datenmissbrauch kaum konkret abschätzbar sind. Wer kann schon eine Aussage darüber treffen, in wie viele Hände geleakte Daten letztlich gelangen?

Mjam vermittelt

Von Mjam selbst wollten wir wissen, ob die Keiler die Daten direkt von ihrem Unternehmen abgegriffen hatten und ob man mittlerweile erforscht hat, wer alte Kundendaten auf Github gestellt hat. „Zu den Themen haben wir schon ausführlich Stellung genommen, unter anderem im Blog auf der Homepage", erklärte das Unternehmen knapp. Wie Mjam den Betroffenen weiterhilft? „Wir haben die Kommunikation zwischen Betroffenen und Behörden übernommen. Wir haben unseren Anwalt beauftragt, unsere User zu unterstützen, um auf unsere Kosten gegen die Anrufer vorzugehen", heißt es aus der Zentrale. Außerdem werde jeder Fall an die Datenschutzbehörde weitergeleitet. Seit Ende Oktober beschäftige man IT-Sicherheitsexperten, um ein Höchstmaß an Datensicherheit herzustellen. Um zu vermeiden, dass neue Nummern in falsche Hände geraten, habe man die Telefonnummern der Kunden in den E-Mail-Bestätigungen in der Datenbank anonymisiert.
Die Frage nach dem Datenleck bleibt damit zwar bis auf Weiteres unbeantwortet, doch immerhin können sich die Kunden wieder mit dem weitaus angenehmeren Problem beschäftigen, was sie sich zu essen bestellen sollen. Völlig beruhigt sein kann freilich niemand. Während die großen Mitspieler am Markt wie Facebook & Co im Mittelpunkt des öffentlichen Interesses stehen, lauern anderswo Fallen, mit denen niemand rechnet – nur weil er Appetit auf eine Pizza hatte.

Bisher erschienen:
Google und der Datenschutz KONS. 1/2015
Facebook und der Datenschutz KONS. 2/2015
Amazon und der Datenschutz KONS. 3/2015
WhatsApp und der Datenschutz KONS. 4/2015

Was tun, wenn Telefonkeiler anrufen?

- Anonyme Anrufe bzw. bestimmte Rufnummern auf dem Handy sperren.
- Keine persönlichen Daten preisgeben.
- Anfrage ablehnen und auflegen.
- Wenn sie nicht lockerlassen: nachfragen, welche Firma dahintersteckt, sich den Namen des Unternehmens und des Anrufers geben lassen und ihnen erklären, dass man der Sache rechtlich nachgehen werde.
- Anrufe beim Netzbetreiber melden.
- Anzeige bei der Fernmeldebehörde erstatten (www.bmvit.gv.at/telekommunikation/organisation/nachgeordnet/fmb/index.html)

Europäisches Verbraucherzentrum Österreich ECC-Net
www.europakonsument.at
Co-funded by the European Union

Dieser Artikel entstand im Rahmen der Tätigkeiten des Netzwerkes der Europäischen Verbraucherzentren (ECC-Net).