Betrüger fahren mit Daten ab

Dem Fahrdienstvermittler Uber wurden rund 57 Millionen Datensätze gestohlen. Der massive Datenraub betrifft zwangsweise auch andere Onlinedienste.

RALF HILLEBRAND

Der Smartphone-Dienst Uber vermittelt monatlich rund 40 Millionen Privatfahrten als Taxi-Alternative.
BILD: SN/APA/AFP/CABALLERO

SAN FRANCISCO. Apple, Adobe, Facebook, Yahoo. Es gibt kaum noch einen IT-Riesen, dem noch nicht in riesigem Ausmaß Daten gestohlen wurden. Wie am Mittwoch bekannt wurde, gehört nun auch Uber zu dieser wenig ruhmreichen Riege. Dem Fahrdienstvermittler wurden bereits vor einem Jahr die Daten von rund 50 Millionen Fahrgästen und von etwa sieben Millionen Uber-Fahrern gestohlen. Statt Behörden oder Betroffene zu informieren, bezahlte Uber den Hackern 100.000 Dollar (85.000 Euro), damit sie die Daten vernichten. Ob sich die Cyberkriminellen daran gehalten haben, kann nicht final belegt werden.

„Den Diebstahl so lang zu verschweigen ist für mich klar fahrlässig", sagt Dominik Engel, Cybersecurity-Experte und Leiter des Zentrums für sichere Energieinformatik an der FH Salzburg. Vielmehr hätte man den Vorfall offen ansprechen sollen. Selbst wenn Uber dazu rechtlich nicht verpflichtet sei, gebe es „die moralische Pflicht". Mit der europäischen Datenschutz-Grundverordnung, die am 25. Mai 2018 in Kraft tritt, wird es zumindest in der EU auch rechtlich strafbar, solche Vorfälle länger zu verschweigen.

Alois Kobler sieht das Schweigen ähnlich kritisch. Der Geschäftsführer von Blue Shield, einer oberösterreichischen Cybersecurity-Firma, geht sogar noch einen Schritt weiter: Seiner Ansicht nach hätte Uber den Datendiebstahl problemlos abblocken können. „Das hätte man leicht verhindern können. Es hätte schon gereicht, wenn die Sicherheitsinfrastruktur auf dem aktuellen Stand gewesen wäre." Die Hacker sind durch eine Datenbank in einen Cloud-Dienst (Datensicherung im Web, Anm.) eingedrungen.

Dass bei dem Datenraub „nur" Namen, E-Mail-Adressen, Telefonnummern etc., aber keine Kreditkartendaten gestohlen wurden, nimmt dem Vorfall nur wenig an Brisanz. Denn zum einen wurden auch Fahrerlaubnisnummern von 600.000 US-Uber-Fahrern entwendet. Führerscheine werden in Amerika oft als Ausweisdokumente verwendet, was die Daten für Betrüger wertvoll macht. Zum anderen betrifft solch ein Datendiebstahl nie nur den Dienst selbst, wie FH-Experte Engel erläutert. Viele Nutzer würden dieselbe Kombination aus E-Mail-Adresse und Passwort für mehrere Dienste verwenden. Oder anders: Wer sein Uber-Passwort ebenso für seinen E-Mail-, eBay- oder Amazon-Account verwendet, könnte auch dort Probleme kriegen.

Wie sollte man sich nun aber als Firma verhalten, wenn man Opfer eines solchen Datenraubs wird? Man müsse prüfen, ob die Angreifer noch im System sind, die Schwachstellen schließen und sicherstellen, dass sich ähnliche Lücken nicht mehr auftun, sagt Engel. Und er rät davon ab, das Lösegeld zu zahlen – vor allem, wenn man das Ganze im Blick hat: „Würde sich niemand mehr auf die Forderungen einlassen, ist das System nicht mehr profitabel – und die Hacker geben es auf." Auch Cybercrime agiere nach wirtschaftlichen Faktoren, teilweise sogar servicierend. „Ich kenne den Fall einer Volksschule, die von Erpressern 50 Prozent Rabatt auf ihr Lösegeld gekriegt hat, nachdem sie geschildert haben, dass sie ja nur eine arme Volksschule sind."

Doch wie kann es überhaupt sein, dass Tech-Riesen – jene Unternehmen, die wohl die weltbesten IT-Experten beschäftigen – immer wieder gehackt werden? „Das Problem liegt im Normalfall im Management", beschreibt Kobler von der Blue Shield Security GmbH. Oft fehle bei den Geschäftsführern das Verständnis, „dass für die IT-Security Geld ausgegeben werden muss." Auch deshalb fordert Kobler


BILD: SN/FH/KOLARIK

„Hacker gaben Volksschule Rabatt."
Dominik Engel, FH Salzburg

ein Umdenken in Sachen Cybersicherheit. Der 30-Jährige und sein Team haben eine Österreichische Cybersicherheits-Strategie ausgearbeitet, bestehend aus fünf Punkten. Im Kern steht „der Aufbau einer österreichischen/europäischen Cybersecurity-Intelligence", die auf sogenannte Hack-hunts und Hack-backs setzen soll. Als Hack-hunts wird die systematische Suche nach Cyberverbrechern bezeichnet, als Hack-backs die Strategie, Hacker mit ähnlichen Waffen zu schlagen, wie diese angewandt haben. „Meiner Meinung nach ist das die einzige Möglichkeit, den Trend wirklich zu bekämpfen."

Dominik Engel ist da anderer Ansicht. „Das geht für mich in die falsche Richtung", sagt der FH-Experte. „Wir brauchen keine Kopfgeldjäger oder Selbstjustiz." Für ihn sei es wesentlicher, den Fokus auf sichere Infrastruktur zu richten. Zudem seien Hack-back-Aktionen illegal. Dies ist Alois Kobler bewusst. Aber das müsse eben geändert werden: „Es geht darum, wie ich am besten zum Ziel komme, nämlich die Angriffe zu stoppen."

In zwei weiteren Punkten sind sich Engel und Kobler einig. Es brauche mehr Bewusstsein für Cybersicherheit. Und die Abwehr von Angriffen müsse auch auf europäischer Ebene stärker werden. „Es kann nicht sein, dass Cybercrime-Experten an Staatsgrenzen aufhören müssen, zu ermitteln." Kobler untermauert das mit einem Beispiel: „Ich bin mir ziemlich sicher, dass mir nichts passieren würde, wenn ich von London aus eine österreichische Bank erpresse."

Wie Neue Medien die Demokratie verändern

Experten diskutieren im SN-Saal über die Folgen von Fake News und Bots.

SALZBURG. Die Wissenschaft sucht nach einer Erklärung, die Bevölkerung ist verunsichert und der Journalismus will gegensteuern. Fake News, also Falschmeldungen, sind spätestens seit Donald Trump in aller Munde – so auch in Salzburg. Heute, Donnerstag, suchen namhafte Experten gemeinsam mit SN-Chefredakteur Manfred Perterer und Medienjournalist Ralf Hillebrand nach Antworten auf die dringlichsten Fragen: Kann man den Medien vertrauen? Wie entwickeln sich Fake News und was muss der Qualitätsjournalismus tun?

Welche Rolle soziale Medien im Wahlkampf spielen und wie gefährlich „Social Bots" für die demokratische Meinungsbildung sind, wird am Podium im SN-Saal ebenfalls besprochen. Zu den Diskutanten zählen Experten aus den Bereichen Wissenschaft, Journalismus und Kommunikation. So wird Judith Denkmayr vom Mateschitz-Rechercheprojekt „Addendum" ebenso dabei sein wie der Hamburger Medienforscher Uwe Hasebrink.

Organisiert wird der Abend von Studierenden der Kommunikationswissenschaft, die ihre neuesten Forschungsergebnisse vorstellen.

Die Veranstaltung startet um 18 Uhr im SN-Saal. Kostenlose Anmeldung unter WWW.SN.AT/RESERVIERUNG. **kat**

Facebook erlaubte erneut rassistische Werbeanzeigen

MENLO PARK. Wieder Ärger um das Werbesystem bei Facebook: Nach Recherchen der US-Organisation ProPublica konnten auf dem Portal erneut Anzeigen geschaltet werden, die Bevölkerungsgruppen ausschließen, etwa Juden oder Menschen, die sich für Rollstuhlrampen interessieren. In einer schriftlichen Reaktion bedauerte Facebook den Vorgang und sprach von einem „technischen Fehler". Durch ein Antidiskriminierungssystem seien bereits Millionen von Anzeigen identifiziert worden. Aber: „Wir können uns verbessern." SN, APA

Wie wir selbst dem Datenklau vorbeugen können

Die Hackerattacke auf Uber sollte zu denken geben. Etwa daran, wie man seine eigenen Daten sicherer macht.

KLICKFIT
Ralf Hillebrand

„Es ist doch völlig egal, dass jemand meine Uber-Daten gestohlen hat. Was soll der Hacker denn damit anfangen? Sich ein Taxi in meinem Namen bestellen?" Solche und ähnliche Kommentare liest man im Netz zuhauf, seit bekannt wurde, dass dem Fahrdienstvermittler Uber rund 57 Millionen Datensätze gestohlen wurden. Doch diese Kommentare sind – gelinde gesagt – naiv. Denn ein Datendiebstahl kann sich schnell auch auf alle anderen Plattformen auswirken, auf denen man unterwegs ist. Schließlich neigt der gemütliche Internetnutzer dazu, dieselbe Kombination aus E-Mail-Adresse und Passwort für mehrere Accounts zu verwenden. Kommen Onlinebetrüger also in den Besitz eines Zugangs, haben sie schnell mehrere in der Hand (siehe auch Artikel oben).

Wie kann man solch einer Kettenreaktion vorbeugen? Der beste Rat liegt auf der Hand. Man sollte für jede Plattform ein eigenes, starkes Passwort anlegen. Ein guter Tipp für starke Kennwörter: Das Passwort sollte nicht lexikal vermerkt sein. Es bietet sich also an, Dialektausdrücke zu verwenden oder Sprachen zu mischen. Ferner sollten Ziffern und Sonderzeichen eingewoben werden. Das Ganze kann schließlich einen Satz ergeben wie „MyHundisschon17Johreold!".

Freilich ist es aufwendig, sich für jede Plattform ein eigenes Passwort zu merken. Dabei helfen können sogenannte Passwort-Manager wie 1Password oder LastPass. Die Programme kosten im Regelfall ein paar Euro.

Ein weiterer Rat ist, nicht mehr genutzte Konten auch wirklich zu löschen – und sie nicht ungenutzt vor sich hin vegetieren zu lassen. Dadurch minimiert man das Risiko, dass man von Datenraubzügen betroffen ist, doch merklich.

Wer in der Vergangenheit solche und ähnliche Tipps nicht beherzigt hat, sollte überprüfen, ob er nicht bereits einmal Opfer eines Hackerangriffs geworden ist. Deshalb ein Hinweis, der in dieser Kolumne bereits einmal gegeben wurde: Steuern Sie die Website SEC.HPI.DE/ILC (so in den Internetbrowser eingeben – ohne www) an, eine Sicherheitsplattform des Hasso-Plattner-Instituts der Universität Potsdam, und lassen Sie überprüfen, ob Ihre Daten jemals gestohlen wurden.

Indes bewegen sich all jene auf dünnem Eis, die darauf bauen, dass die Uber-Daten tatsächlich gelöscht wurden, nachdem der Fahrdienstvermittler das Lösegeld überwiesen hatte – so wie von den Hackern versprochen. Das weiß offenbar auch Uber selbst: Wohl nicht umsonst bot Uber-Boss Dara Khosrowshahi an, den Betroffenen dabei zu helfen, nach einem möglichen Missbrauch der gestohlenen Daten Ausschau zu halten.

Anregungen um die **Digitalwelt?**
RALF.HILLEBRAND@SN.AT