

Außen vor

Daten bei Facebook kontrollieren und löschen



Facebook bietet eine Reihe von Funktionen, mit denen sich gespeicherte Informationen überprüfen und löschen lassen und mit denen man für seine Daten festlegt, wer sie zu sehen bekommt. Man muss die Einstellungen dafür nur finden.

Von Jo Bager

Mache Facebook zu deinem Facebook – Ende Oktober hat Facebook eine millionenschwere Werbekampagne gestartet. Anzeigen in Tageszeitungen, Publikumszeitschriften

und Außenwerbung sollen Deutsche davon überzeugen, dass sie jederzeit die Kontrolle darüber haben, was von ihnen bei Facebook zu sehen ist.

In der Tat kann man viele der Dinge kontrollieren, die Facebook über einen weiß und die Dritte zu sehen bekommen. Leider ist es nicht so einfach, wie es die Anzeigen suggerieren. Dort steht zum Beispiel „Ich hab mal etwas gepostet, was ich nie, nie, nie hätte teilen sollen.“ Als Lösung bietet das Banner an: „Auf Facebook etwas zu löschen heißt: Es ist weg. Schnell und unkompliziert.“

Das ist allerdings grob irreführend. Denn wenn etwas erst einmal in einem digitalen Medium wie Facebook veröffent-

licht wurde, kann man nie mehr sicherstellen, dass es „weg“ ist. Man kann es zwar in seiner eigenen Timeline löschen. Aber andere können es bis dahin kopiert haben und jederzeit wieder veröffentlichen.

Plattformfrage

Deshalb lautet eine gute Faustregel im Umgang nicht nur mit Facebook, sondern mit digitalen Medien generell: Alles, was man veröffentlicht, sollte man auch Fremden auf der Straße zeigen können. Nur wenn man diese Regel immer beherzigt, kann man sicher sein, dass zum Beispiel Fotos, die nur für die Augen enger Freunde bestimmt sind, nicht plötzlich in der Öffentlichkeit auftauchen.

Der Zugriff auf Posts lässt sich in der Facebook-Timeline auf bestimmte Adressaten einschränken. Zudem hält die Plattform auch geschlossene und geheime Gruppen bereit, in denen sich Gleichgesinnte austauschen können, ohne dass Dritte mitlesen. Selbsthilfegruppen zum Beispiel machen davon Gebrauch. Will man über intime oder vertrauliche Dinge kommunizieren, gibt es aber geeignetere Medien, denn Facebook liest immer mit.

Als Alternative bieten sich zum Beispiel Messenger an, die Nachrichten Ende-zu-Ende-verschlüsseln. Dazu gehören etwa Threema und WhatsApp. Denn durch die Verschlüsselung bekommen nur die Teilnehmer einer Konversation die Inhalte zu Gesicht, nicht aber der Plattform-Betreiber. Auch der Facebook Messenger beherrscht Ende-zu-Ende-Verschlüsselung, ist aber zu unflexibel. So lassen sich Chats dort nur von einem bestimmten Gerät zu einem bestimmten anderen verschlüsseln. Im Unterschied zu Threema und WhatsApp erlaubt er zudem keine verschlüsselten Gruppenchats.

Inventur

Im Laufe der Nutzung fallen bei Facebook viele Informationen an, die insgesamt ein recht scharfes Profil Ihrer Persönlichkeit abgeben. Sie sollten sich daher von Zeit zu Zeit einen Überblick über die gespeicherten Daten verschaffen und gegebenenfalls aufräumen. Einen ersten Eindruck über die eigenen Aktivitäten gibt einem das Aktivitätenprotokoll, zu erreichen über den Link im Banner-Bereich des eigenen Profils. Hier listet Facebook

minutiös auf, was man wann gemacht hat. Jeder Eintrag lässt sich einzeln editieren oder löschen.

Mit dem Privatsphäre-Check können Sie sich Ihr Profil auch mit den Augen eines anderen Mitglieds ansehen, um zu kontrollieren, dass dieses wirklich nur zu Gesicht bekommt, was es sehen soll. Sie finden ihn über das Schloss-Icon in der Menüleiste. Dort können Sie auch mit „Wer kann meine zukünftigen Beiträge sehen?“ den Standard-Empfängerkreis für das Posten zukünftiger Beiträge vorgeben: „Öffentlich“, „Freunde“, „Nur ich“, oder oft die beste Wahl – „Weitere Optionen“. Hier können Sie eigene Empfängerlisten definieren.

Sie können sich auch eine Kopie aller persönlicher Informationen, die Sie auf Facebook geteilt haben, erzeugen lassen (alle URLs unter dem c't-Link). Facebook stellt die Daten als Zip-Datei zum Herunterladen bereit. Das Paket zu schnüren dauert ein paar Minuten. Facebook weist Sie mit einer Mail darauf hin, wenn der Download bereitsteht.

Das Paket gibt Ihnen einen guten Eindruck davon, wie viel Facebook über Sie weiß. Beim Autoren dieses Artikels, wahrlich kein Facebook-Junkie, sind nur an Text-Inhalten 2 MByte zusammengekommen. Das entpackte Download-Paket stellt die Informationen übersichtlich in Form von HTML-Seiten dar, je eine für „Kontaktinformationen“, „Chronik“, „Fotos“, „Nachrichten“ und zehn weitere Kategorien.

Der Download umfasst aber nur Informationen, die Sie selber explizit auf Facebook hochgeladen haben. Facebook weiß aber noch mehr über Sie, zum Beispiel indem es Ihr Verhalten auswertet. Diese Rückschlüsse gehen in Ihr Werbeprofil ein, die Grundlage für Werbung, die Facebook Ihnen präsentiert.

In seinen Werbeeinstellungen zeigt Facebook Interessengebiete an, von denen es glaubt, dass sie Sie interessieren. Sie erreichen diese Einstellungen, wenn Sie den Menüeintrag „Warum wird mir das hier angezeigt“ des zu jeder Facebook-Anzeige gehörenden Menüs auswählen und im Pop-up, das dann erscheint, auf „Deine Einstellungen für Werbeanzeigen verwalten“ klicken. Dort können Sie dann Ihr Werbeprofil anpassen – zum Beispiel, indem Sie alle Interessen löschen. Face-



Jo Bager

Mittwoch, 26. Oktober 2016 um 16:38 UTC+02
Jo Bager und Iulian Mardarie sind jetzt Freunde.

Mittwoch, 19. Oktober 2016 um 11:44 UTC+02
Jo Bager hat Leafs Video geteilt.

Montag, 17. Oktober 2016 um 12:44 UTC+02
Jo Bager hat Das alte Hannovers Beitrag geteilt.

In der chinesischen Stadt Changde ist so eine Art Mini-Hannover gebaut worden.

Dienstag, 11. Oktober 2016 um 12:07 UTC+02

<http://www.heise.de/newsticker/meldung/Module-statt-Betriebssystem-Android-Anpasser-Cyanogen-aendert-Strategie-3344994.html> Der ambitionierte Versuch, ein alternatives Android zu entwickeln, ist gescheitert.

Donnerstag, 29. September 2016 um 10:03 UTC+02
Jo Bager hat חתונה Video geteilt.

Donnerstag, 22. September 2016 um 07:59 UTC+02

Die Familienministerin spannt Dagi Bee und andere A-YouTuber für eine Kampagne gegen Hate Speech ein. Grundsätzlich eine gute Idee, aber ...

Dienstag, 20. September 2016 um 08:59 UTC+02

Bisschen chillen mit Rammstein

Dienstag, 6. September 2016 um 11:04 UTC+02
Jo Bager hat Meeboons Video geteilt.

Freitag, 26. August 2016 um 15:19 UTC+02
Jo Bager gefällt Linux Inside.

- Profil
- Kontaktinformationen
- Chronik**
- Fotos
- Synchronisierte Fotos
- Videos
- Freunde
- Nachrichten
- Anstupsen
- Veranstaltungen
- Sicherheit
- Ads
- Handys
- Places Created
- Umfrageergebnisse

Facebook stellt eine Kopie aller persönlichen Informationen, die man auf Facebook geteilt haben, als Paket zum Herunterladen bereit.

book zeigt Ihnen dann weniger relevante Werbung, andere Konsequenzen hat dies nicht.

Im Schaltraum

Weitere den Datenschutz betreffende Optionen finden sich in den Einstellungen. Unter „Privatsphäre“ etwa lässt sich festlegen, wer einen kontaktieren und wer nach einem suchen darf. Möchten Sie die Reichweite sämtlicher alter Beiträge komplett auf die Freunde einschränken, findet Sie dort ebenfalls den Schalter dafür.

Unter „Chronik und Markierungseinstellungen“ lässt sich feintunen, was für wen in der eigenen Chronik zu sehen sein soll, und wer dort posten darf. Dort legen Sie zum Beispiel fest, dass nur Ihre Freunde in Ihrer Chronik posten dürfen und dass auch nur Sie und Ihre Freunde diese Posts zu Gesicht bekommen – eine solche Einstellung ist immer ganz gut, wenn der Chef die privaten Partyfotos nicht sehen soll, die Freunde in der Timeline posten.

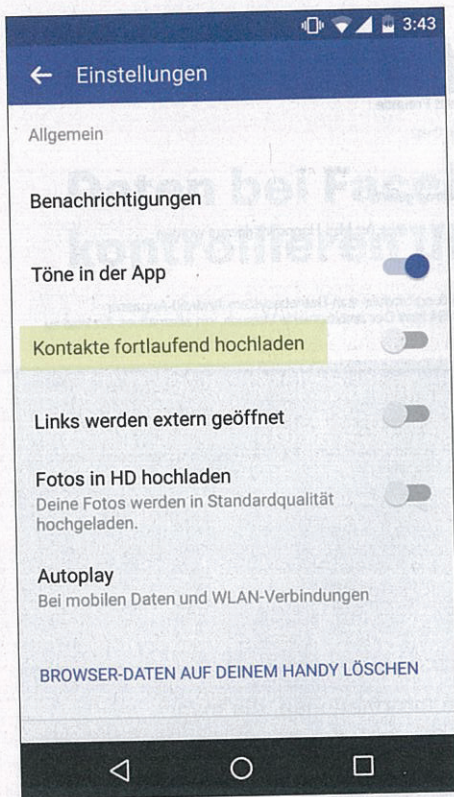
Facebook nutzt Informationen über seine Mitglieder nicht nur selbst, sondern fungiert auch als Plattform für Drittanbieter-Apps – denen es Informationen bereitstellt. Von Zeit zu Zeit sollte man auch in den App-Einstellungen mal nachsehen,

wer da eigentlich alles auf welche Daten zugreifen kann, und aufräumen. Unter „Werbeanzeigen“ kommen Sie zu den allgemeinen Werbeeinstellungen, legen fest, ob Sie überhaupt interessenbasierte Anzeigen sehen wollen und ob Facebook Banner mit Ihren sozialen Handlungen verknüpfen darf – ob sich also der Pizzabäcker mit seiner Kampagne für die neue Lasagne auf Ihr „Like“ für Nudelgerichte beziehen darf.

Daten von Dritten

Man gibt Facebook nicht nur Daten über sich selbst. Insbesondere der Freundefinder lädt einen dazu ein, auch Daten über Dritte preiszugeben, indem man sein Adressbuch hochlädt. Die Facebook-Apps für Android und iOS zum Beispiel laden Adressbuchdaten hoch, wenn dort die sogenannte „laufende Synchronisierung“ aktiviert ist.

Unter Android deaktivieren Sie dies in den Optionen unter „App-Einstellungen“, unter iOS unter „Einstellungen/Allgemein“. Dort nennt sich der Schalter „Kontakte hochladen“. Haben Sie bereits Kontakte hochgeladen? Auf der Seite „Einladungen und importierte Kontakte verwalten“ können Sie es kontrollieren – und auch einzelne oder alle importierten Kontakte wieder entfernen.



„Kontakte fortlaufend hochladen“ bedeutet: Facebook schaufelt sich alle Adressbucheinträge rein – besser abschalten.

Nach der Lektüre der vorigen beiden Artikel wollen Sie nur noch weg von Facebook und alle Ihre dort gespeicherten Informationen löschen lassen? Das ist möglich, Facebook bietet auch dafür ein Formular. Der Dienst weist darauf hin, dass es nur die selbst geposteten Beiträge löscht. Insgesamt dauert es laut Facebook bis zu 90 Tage, bis alle Inhalte gelöscht sind.

Draußen

Auch wenn Sie nicht bei Facebook sind, sieht das Unternehmen Sie auf jeder Website, welche den Like-Button, andere sogenannte Social Plugins oder Werbung von Facebook anzeigen. Mit einem Cookie kann das Unternehmen alle Seitenaufrufe auf einen Anwender zurückführen. Auch bei Nichtmitgliedern kommen so umfangreiche Profile zusammen.

Sie können dem Unternehmen aber verbieten, Nutzungsdaten für das Targeting zu erheben. Dazu lassen Sie auf www.youronlinechoices.eu ein sogenanntes Opt-out-Cookie setzen. Die Plattform vereint übrigens so ziemlich alle Werbe-

vermarkter, die mit Targeting arbeiten, sodass sie diese Cookies auch für viele andere Werbeunternehmen setzen können.

Die Opt-out-Cookies bewahren Sie aber nicht davor, Werbung angezeigt zu bekommen: Ihre IP-Adresse landet also auf jeden Fall bei Facebook. Abgesehen davon birgt diese Methode das Risiko, dass man die Opt-out-Cookies mitlöscht, wenn man seinen Browser mal aufräumt. Dann muss man sie neu setzen lassen. Nachhaltiger schützen Browser-Add-ons gegen neugierige Anzeigenvermarkter wie Facebook, zum Beispiel Adblocker wie das für Chrome, Safari und Firefox verfügbare uBlock.

Für Android und iOS gibt es ebenfalls Werbeblocker, die neugierige Ausspäher ausperren. Soll Facebook per App den Aufenthaltsort mitloggen? Falls nicht, können Sie mit den Einstellungen des Mobilsystems der Facebook-App und der anderen Apps des Unternehmens das Recht entziehen, auf den Standort zuzugreifen.

Benutzt man Facebooks Login, um sich mit dem Facebook-Account woanders einzuloggen, bekommt das Unternehmen mit, welche Dienste man nutzt und wann. Wer das nicht möchte, muss wohl in den sauren Apfel beißen und sich für Drittanbieterdienste eigene Accounts anlegen beziehungsweise bestehende von Facebooks Login auf herkömmliche Logins umstellen. Mit einem Passwortmanager ist es aber gar nicht so schwierig, auch mit vielen Zugangsdaten zu hantieren.

Als Webmaster stehen Sie vor einem Dilemma: Der Like-Button von Facebook sowie andere Social-Media-Buttons helfen, Ihre Seiten bekannter zu machen. Gleichzeitig melden diese aber die IP-Adresse und gegebenenfalls weitere Nutzerdaten Ihrer Besucher bei jedem Seitenaufruf an Facebook und Co.

c't hat dafür eine Lösung entwickelt. Der c't Shariff ersetzt die Standard-Buttons für das Teilen von Inhalten durch eigene. Shariff-Buttons stellen den direkten Kontakt zwischen Social Network und Besucher erst dann her, wenn Letzterer aktiv auf den Share-Button klickt. Shariff hat sich auf tausenden Websites bewährt und steht als kostenlose Open-Source-Lösung für die verschiedensten Plattformen zum Herunterladen zur Verfügung.

Facebook stellt eine Reihe von Kontroll- und Steuermöglichkeiten für die von

seinen Nutzern hochgeladenen Informationen bereit: Wer Facebook verlässt, kann seine Daten wieder löschen lassen; Nichtmitglieder können das Datensammeln für Werbepreise unterbinden; Webmaster schützen ihre Besucher mit Shariff vor dem neugierigen Like-Button: Ist also alles bestens?

Eher nicht. Die vom Nutzer selbst hochgeladenen Informationen sind nur ein Bruchteil dessen, was Facebook über ihn weiß – siehe auch den Artikel ab Seite 76. Facebook hat also viel mehr Informationen über jeden einzelnen, als alle zur Verfügung stehenden Kontroll- und Löschmechanismen überhaupt erreichen können. Bei der Kontrollösung spricht Facebook explizit nur davon, die vom Nutzer selbst geposteten Beiträge zu löschen.

Und was heißt eigentlich Löschen bei Facebook: Endgültiges Entfernen aus den Datenbanken? Die Recherchen des Datenschützers Max Schrems deuten darauf hin, dass Facebook Inhalte möglicherweise gar nicht endgültig löscht, sondern nur mit einem Löschvermerk versieht.

Wir wissen nicht, wie genau Facebook mit Ihren Daten verfährt. Das Unternehmen ist bei solchen Informationen zu sich selbst sehr zurückhaltend. In den USA gibt es keine Aufsichtsbehörde, die die Datensammelei effektiv kontrolliert und im Zaum hält.

Nur Druck hilft

Wann immer deutsche Datenschützer mehr herausfinden oder die Datengier bremsen wollen, versucht Facebook, sich mit vielfältigen juristischen Winkelzügen zu entziehen. Dazu gehört das Argument, die irischen, nicht die deutschen Datenschützer seien in der EU für Facebook zuständig, weil Facebook seinen EU-Hauptsitz in Irland hat. Die irische Behörde wiederum hat sich in der Vergangenheit im Umgang mit Facebook als überforderter, zahnloser Tiger erwiesen.

Es gibt wohl nur einen Weg, Facebook zu mehr Transparenz und Datenschutz zu bewegen: Man muss das Unternehmen vor Gericht dazu zwingen. Der folgende Artikel fasst die derzeit gegen Facebook angestrebten Verfahren zusammen.

(jo@ct.de) **ct**

Weiterführende Informationen:
ct.de/ym9z