Schadensbegrenzung

Anonymität am Smartphone ist illusorisch. Was Sie tun können ist, die weitergereichte Datenmenge zu reduzieren.

Grafik: Alhovik / Shutterstock.com Montage: Doris Seyser

Wir haben bereits in KONSUMENT 6/2016 darauf hingewiesen: Wer ein Smartphone verwendet, leistet seinen persönlichen Beitrag zum weltweiten Datensammelspiel. Jedes Gerät ist schon allein aufgrund seiner permanenten Verbindung zum Mobilnetz lokalisierbar, und um ein persönliches Google- oder Apple-Benutzerkonto kommt man praktisch nicht herum. Den verbleibenden Handlungsspielraum würde man in anderem Zusammenhang als Möglichkeit zur Schadensbegrenzung bezeichnen. Und genau darum geht es diesmal. Anonymität ist am Computer genauso ein Wunschtraum wie am Smartphone. Als Nutzer können Sie lediglich Art und Menge der weitergegebenen Daten etwas reduzieren. Die in unserer Juni-Ausgabe behandelte Kontrolle der App-Berechtigungen ist ein wichtiger Teil dieser Maßnahmen. Darüber hinaus können Sie direkt am iPhone bzw. online beim persönlichen Google-Konto bestimmte Einstellungen vornehmen, die wir uns nun näher anschauen werden.

iPhone

Öffnen Sie die »Einstellungen«, scrollen Sie ein wenig nach unten und tippen Sie auf »Datenschutz/Ortungsdienste«. Diese waren bereits bei den App-Berechtigungen Thema. Allerdings gibt es hier zusätzlich den Unterpunkt »Standortfreigabe«. Ist er aktiviert, sehen Freunde und Familienmitglieder bei Verwendung der Apps „Nachrichten" bzw. „Freunde suchen", wo Sie sich gerade befinden. Umgekehrt können Sie zum Beispiel den Aufenthaltsort Ihres Partners oder Ihrer Kinder abrufen. Inwieweit diese Überwachungsmöglichkeit erwünscht ist, muss jeder für sich entscheiden. Es sollte Ihnen jedenfalls bewusst sein, dass auch Apple diese Standortdaten übermittelt bekommt.
Kehren wir zurück zum Menüpunkt »Datenschutz«. Unten auf der Seite finden Sie »Diagnose und Nutzung«. Tippen Sie darauf und vergewissern Sie sich, dass der Haken bei „Nicht senden" gesetzt ist. Damit verhindern Sie die Übertragung von anonymisierten Daten, mit deren Hilfe Apple Fehlfunktionen analysieren, aber auch Ihr Nutzungsverhalten nachverfolgen kann. Diese Daten werden zum Teil auch Drittanbietern zur Verfügung gestellt, mit denen Apple kooperiert.

iAd

Ein zweiter wichtiger Punkt unter »Datenschutz« ist die »Werbung«. Hier müssen wir etwas ausholen. Vergleichbar der deutlich größeren Werbeplattform von Google gibt es auch bei Apple eine solche, iAd genannt. Sie verkauft an Unternehmen Werbeflächen in Apps, die auf dem iPhone vorinstalliert sind oder (kostenlos) aus dem App Store heruntergeladen wurden. Je zielgenauer die Werbung die Interessen eines Nutzers trifft, desto besser ist es für alle Beteiligten, so die Annahme. Steht nun der Schalter neben „Kein Ad-Tracking" auf „Aus" (linke Position), verfolgt Apple Ihre Einstellungen (Sprache, Art der Verbindung) und Aktivitäten auf dem Gerät (Musik, Bücher, Spiele, sonstige Interessen) und nutzt diese in Kombination mit den von Ihnen bekannt gegebenen persönlichen Daten (z.B. Alter, Geschlecht, Wohnort, nicht aber Name, Adresse oder Gesundheitsdaten aus der „Health"-App), um Sie einer Zielgruppe zuzuordnen. Auf dieser Basis sehen Sie dann zielgerichtete Werbeeinschaltungen. Schieben Sie den Schalter neben „Kein Ad-Tracking" auf die rechte Position (= „Ein"), dann wird die Ihnen zugeordnete Ad-ID (= Werbe-Identifikationsnummer) gelöscht. Sie sehen zwar trotzdem Werbung in den Apps, nur ist diese von allgemeiner Natur. Abstellen lässt sich die Werbung jedenfalls nicht.
Womit wir nochmals zu den »Ortungsdiensten« hinaufblättern und dann gleich wieder ans Ende der Seite zum Punkt »Systemdienste«. Um es kurz zu machen: Die einzige Funktion, die sinnvoll ist und daher aktiviert bleiben sollte, ist „Mein iPhone suchen". Den Rest können Sie – unter minimalen bis gar nicht vorhandenen Komforteinbußen – getrost deaktivieren. Eingeschaltet bleiben sollte lediglich noch ganz unten auf der Seite die Anzeige des „Statusleistenobjekts".
Was Sie abschließend sonst noch tun können: Deaktivieren Sie unter »Einstellungen/iCloud« die Optionen »Backup« und »Schlüsselbund«. Sie verhindern damit, dass Ihre Einstellungen, persönlichen Daten und

Rat und Hilfe für Verbraucher in Europa ECC-Net Finanziell unterstützt durch die Europäische 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.

die auf dem iPhone gespeicherten Passwörter in Apples iCloud gespeichert werden. Vergessen Sie aber nicht, alternativ dazu über die Software iTunes regelmäßig ein lokales Backup auf Ihrem Computer durchzuführen. Nur so können Sie im Fall des Falles Ihre Daten retten und sie entweder auf das iPhone zurückspielen oder auf ein neues Gerät übertragen.

Android

Google als Unternehmen, das hinter der Originalversion des Betriebssystems Android steckt, ist auch nicht gerade müßig, wenn es ums Datensammeln geht. Um genau zu sein, ist Google sogar wesentlich fleißiger, betreibt es doch diverse Dienste wie die gleichnamige Suchmaschine, den E-Mail-Dienst Gmail, die Social-Media-Plattform Google+ oder die Videoplattform YouTube, die ihm über Geräte und Betriebssysteme hinweg eine Fülle an Informationen zuliefern. Abseits der im vorigen Heft besprochenen App-Berechtigungen und einzelner herstellerspezifischer Einstellungsmöglichkeiten wurde hier vieles von den Geräten auf das online zugängliche Google-Konto ausgelagert. Dort fließen alle Informationen zusammen, sofern Sie bei der Nutzung der diversen Google-Dienste angemeldet sind – und auf den mobilen Geräten sind Sie das in der Regel.
Wenn Sie am Computer, Smartphone oder Tablet den Browser starten und die Adresse accounts.google.com aufrufen oder (bei den mobilen Geräten) über die Einstellungen auf die Google-Dienste zugreifen, gelangen Sie zur Anmeldeseite, auf der Sie Ihren Benutzernamen und Ihr Kennwort eingeben. Sie landen auf der Startseite Ihres persönlichen Kontos, auf der uns diesmal speziell die Optionen unter »Persönliche Daten & Privatsphäre« interessieren. Sie können hier wahlweise das als „Privatsphärecheck" bezeichnete Werkzeug nutzen, das Sie durch die Einstellungsmöglichkeiten leitet, oder Sie gehen selbstständig Punkt für Punkt vor.

Preis für den Komfort

Beachten Sie unter »Meine persönlichen Daten« auf jeden Fall die folgenden Unterpunkte: »Über mich«, »Google+ Einstellungen«, »Soziale Empfehlungen« und »Standortfreigabe«. Hier legen Sie fest, welche Informationen für Dritte sichtbar sind. Für Google selbst interessanter sind die Daten, die unter den »Aktivitätseinstellungen« gesammelt werden. Unter dem Deckmantel von höherem Komfort und Nutzerfreundlichkeit (was ja an sich nicht gelogen ist) geben Sie unter anderem Ihre Suchanfragen, Ihren jeweiligen Standort, Ihre Kontakte und Kalender, Ihre Sprachbefehle und die von Ihnen auf YouTube angesehenen Videos preis.
Unter den »Einstellungen für Werbung« können Sie – wie auch anderswo üblich – Werbeeinblendungen im Browser oder in Apps nicht abstellen, aber Sie können entscheiden, ob Sie lieber auf Ihre Interessen abgestimmte Werbung sehen möchten oder allgemein gehaltene. Im Falle der interessenbasierten Werbung werden werblich relevante Informationen auch an Drittanbieter weitergegeben, indem Sie einer bestimmten Zielgruppe zugeordnet werden (z.B. nach Alter, Geschlecht, Wohnort, Interessen auf Basis Ihrer Suchanfragen). Ihre Identität oder Ihre exakte Wohnadresse werden aber nicht offengelegt.
Ein interessanter Punkt ist weiters die »Kontoübersicht«, das sogenannte Google-Dashboard. Dort finden Sie eventuell noch zusätzliche Informationen, die Google über Sie gespeichert hat, bzw. können Sie weitere Einstellungen vornehmen.
Zuletzt noch ein Tipp: Von der Startseite Ihres persönlichen Kontos aus erreichen Sie auch die »Kontoeinstellungen« mit dem Unterpunkt »Konto oder Dienste löschen«. Wenn Sie beispielsweise Google+ überhaupt nicht nutzen, können Sie dieses unter »Produkte löschen« entfernen. Gleiches ist auch mit Gmail möglich, falls Sie ohnehin einen anderen E-Mail-Dienst verwenden. Ihr Nutzername für das Google-Konto bleibt erhalten, Sie haben nur keinen Zugriff mehr auf die Gmail-Postfächer. Achten Sie aber darauf, dass Sie bei den persönlichen Daten eine E-Mail-Adresse angeben, unter der Sie erreichbar sind, denn auf diesem Wege erhalten Sie z.B. auch Warnmeldungen, falls jemand Ihr Konto unberechtigt verwendet.

Mehr zum Thema

Bisher in KONSUMENT erschienen:

Browser	1/16
Browser-Eweiterungen	3/16
Flash-Cookies und Skripte	4/16
E-Mails	5/16
Opera und Thunderbird	6/16
App-Berechtigungen	7/16

gefährliche produkte

Warnhinweise, Infos zu Sicherheits- und Qualitätsmängeln sowie Rückrufaktionen

HP: Notebook-Akkus

HP ruft weltweit Lithium-Ionen-Akkus, die zwischen März 2013 und August 2015 verkauft wurden, wegen Brand- und Explosionsgefahr zurück. Betroffen sind Notebooks der Serien HP, Compaq, HP ProBook, HP ENVY, Compaq Presario und HP Pavilion, die Akkus können aber auch einzeln als Ersatzteil verkauft worden sein. (https://h30686.www3.hp.com).

IKEA: Patrull-Schutzgitter

IKEA hat das Treppenschutzgitter Patrull zurückgerufen, nachdem Kunden berichtet hatten, dass sich das Gitter geöffnet habe und Kinder die Treppen heruntergefallen seien. Eine Untersuchung hat ergeben, dass der Schließmechanismus nicht einwandfrei funktioniert.

Thule Fahrradträger

Fahrradträger der Bezeichnung Thule Sprint mit der Produktnummer 569000, Verkaufszeitraum März 2015 bis April 2016, wurden zurückgerufen. Der Gabelspanner lässt sich nicht fest genug anziehen, außerdem kann der Schiebeblock einreißen, was zum Versagen der Klemmvorrichtung führt.

„Jeden Tag" Nudeln

Die Zentrale Handelsgesellschaft (ZHG) hat wegen Salmonellengefahr Nudeln der Marke „Jeden Tag" zurückgerufen, und zwar Spiralen, 1000 g, MHD 30.11.2017 und Faden, 1000 g, MHD 31.12.2017. Verkauft wurden die Produkte bei MPreis, Nah&Frisch und Unimarkt.

Kfz-Rückrufaktionen

BMW X3 und X4: Die Bügel für die Isofix-Kindersitze könnten beim Schwingen brechen; 9/2010 bis 4/2016; 600.000 Fahrzeuge, in Österreich 15.000. (APA)
Harley Davidson: defekter Zündschalter könnte zum Absterben des Motors führen; Low-Rider-Modelle 1/2014 bis 4/2016; 14.000 Zweiräder weltweit. (bike business)
Mercedes: Verbindung zwischen Hochdruckleitung und -pumpe könnte sich lösen und Kraftstoff austreten lassen; C180 Bluetec und C200 Bluetec, 12/2013 bis 4/2016; 2.200 Fahrzeuge. (ÖAMTC)
Nissan: Airbags des Herstellers Takata könnten bei Auslösen reißen; Modelle Note (8/2005 bis 7/2013) und Tiida (11/2007 bis 1/2014); 5.800 Fahrzeuge in Österreich. (ÖAMTC)