

WEB
+APP
Besser surfen,
mehr erleben

01011001010100111011011101110
010101001110110111011101110
1001010100111011011101110110
01011001010100111011011101110
10101100101010011101101110110
00101100Goo00g0l0e1100110
11001011001100110110011111001
1v0e1r0f1o1l0g0t0101001010100
01110110101010010110010110010
0010100110010111j0e1d0e1n1101
11001011001100110110011111001
1001u0n1s1e0r1e1r011101010010
11001011001100110110011111001
100101010010S0c1h0r1i1t0t1e11
11001011001100110110011111001

Googles Dienste speichern Unmengen an Informationen über das Nutzerverhalten. Das ist Fluch und Segen zugleich. Auf den folgenden Seiten erklären wir, welche Daten auf welche Weise gespeichert werden, wozu das gut sein kann und wie Sie mehr Kontrolle über die Tentakel der Datenkrake erhalten.

FOTOS: HERSTELLER

Von **Valerie Hagmann**

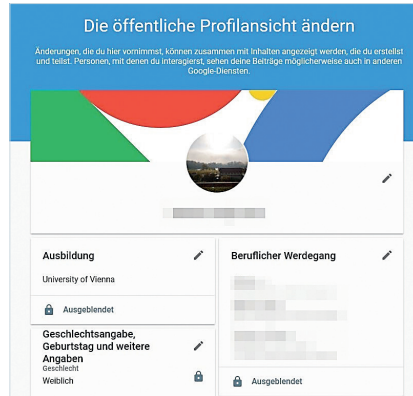
Google weiß, wo Sie arbeiten. Es weiß auch, wo Sie am liebsten essen gehen, welche Bekleidungsmarken Sie bevorzugen, welches Smartphone Sie nutzen und was Ihre Hobbys sind. Denn das Unternehmen lebt davon, aus unseren Nutzerdaten Schlüsse auf unsere Interessen zu ziehen, um punktgenau Anzeigen zu verkaufen und Werbung zu platzieren. Alles, was wir online tun, wenn wir beim Surfen mit unserem Google-Konto eingeloggt oder mit dem Android-Smartphone unterwegs sind, wird dafür verwendet. Und unter Umständen auch vieles, was wir offline tun. Der Vorteil ist, dass dadurch das Nutzererlebnis auf individuelle Bedürfnisse zugeschnitten und somit um ein Vielfaches verbessert wird. Ein Google-Konto ist enorm praktisch, um diese Informationen geräteunabhängig dabeizuhaben. Nutzer von Android-Smartphones kommen auch kaum daran vorbei, sobald sie sich mit Apps versorgen wollen.

Welche Arten von Daten Google tatsächlich sammelt, ist für den Einzelnen oft nur schwer zu durchschauen. Als Reaktion auf den immer lauter werdenden Ruf nach Datenschutz hat das Unternehmen im Vorjahr jedoch einige Tools veröffentlicht und Verbesserungen vorgenommen, um mehr Transparenz zu schaffen und den Nutzern ein gewisses Maß an Kontrolle über ihre Daten in die Hand zu geben. Wir zeigen, wie Sie diese Tools am besten verwenden.

Account-Übersicht: Persönliche Daten in der Konto-Schaltzentrale

Beim Anlegen eines neuen Google-Accounts werden Basisinformationen abgefragt. Dazu gehören Name, Geschlecht, alternative E-Mail-Adresse und Telefonnummer zur Kontoverifizierung und Wiederherstellung des Accounts sowie das Geburtsdatum. Wer jemals das soziale Netzwerk Google+ genutzt hat, hat seine persönlichen Daten vielleicht durch Profil- und Headerbild, Wohnort, Arbeitsplatz und Ausbildung ergänzt.

Einige dieser Angaben sind auch von vornherein öffentlich für andere



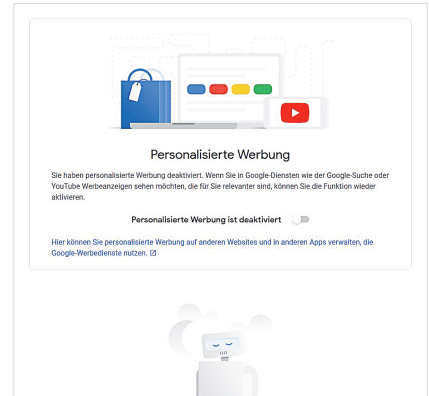
einschbar. Der Link myaccount.google.com führt ohne Umwege zur Konto-Übersichtsseite. Das ist quasi die persönliche Google-Schaltzentrale, um alle Datenschutz- und Sicherheitseinstellungen zu treffen, Abos und Zahlungsinformationen zu verwalten und von Google gesammelte Informationen einzusehen.

Im Reiter **Persönliche Daten** können die oben genannten Angaben eingesehen und gegebenenfalls geändert sowie teilweise entfernt werden. Ein Klick auf den Pfeil neben jeder Angabe lässt Änderungen vornehmen und informiert über deren Sichtbarkeit.

Weiter unten zeigt das Menü **Über mich** (aboutme.google.com) die öffentliche Profilsicht. Die Sichtbarkeit der Angaben kann einzeln eingestellt werden. Einträge mit einem kleinen Schloss-Symbol sind für andere nicht zu sehen. Eine Option, den Account als Ganzes auf privat zu schalten, gibt es derzeit noch nicht, zumindest lassen sich aber alle persönlichen Informationen entfernen oder verbergen.

Anzeigeneinstellungen: Welche Interessen Google Ihnen zuschreibt

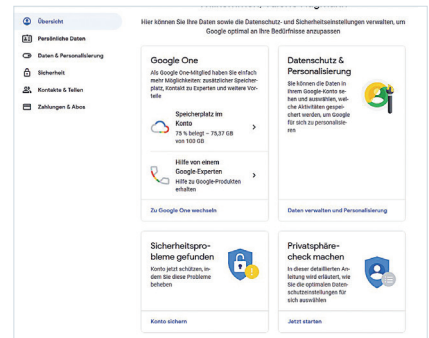
Die im Profil angegebenen Daten genügen bereits, um den Nutzer zu „kategorisieren“ und Werbeanzeigen nach möglichen Interessen zu schalten. Wichtig für diese Einschätzung sind außerdem eingegebene Begriffe aus der Google-Suche. Somit bekommt der Nutzer idealerweise die Produkte und Dienstleistungen angeboten, die besonders viel Relevanz für ihn haben. Dabei werden Daten von sämtlichen Geräten miteinbezogen, auf denen der User mit dem entsprechenden Google-Konto angemeldet ist.



In der Konto-Schaltzentrale lässt sich unter adssettings.google.com einsehen, anhand welcher Informationen die personalisierte Werbung ausgewählt wird. Anzeigen von bestimmten Werbetreibenden lassen sich gezielt ausblenden. Um die grundsätzliche Verwendung der Suchbegriffe zu unterbinden, kann die personalisierte Werbung via Schieberegler deaktiviert werden.

Da die Videostreaming-Plattform YouTube zu Google gehört, fließen auch die dort gesammelten Nutzerdaten mit ins Werbeprofil ein. Dazu gehören der Video-Verlauf sowie zu Videos verfasste Kommentare und Likes. Auf der YouTube-Startseite werden somit Videos vorgeschlagen, die basierend auf den gesammelten Suchverläufen zu den Interessen des Nutzers passen könnten.

Aktivitätenverlauf: Was treiben Sie so im Internet?



Egal, ob Surfen im Chrome-Browser, Google-Kalendereinträge oder App-Suche im Play Store: Google merkt sich jeden Eintrag und jede Eingabe. Mittels dieser Daten werden dann etwa die Vorschläge bei Sucheingaben präziser auf den Nutzer zugeschnitten.

myactivity.google.com ist der Schlüssel, um all diese Daten einzuse-

FOTOS: HERSTELLER

hen. Die Aktivitäten sind nach Datum und Uhrzeit geordnet aufgelistet.

Durch das Suchfeld lassen sich gezielt Eingaben in diesem Datenschatz finden. Ein Klick auf das Dreipunkt-Menü neben jedem Eintrag zeigt weitere Details oder ermöglicht es, den Eintrag zu löschen. Der YouTube-Suchverlauf hat unter *myactivity.google.com/activitycontrols/youtube* sogar eine eigene Übersichtsseite mit denselben Möglichkeiten. Hier lässt sich auch festlegen, ob Suchanfragen und Wiedergabeverlauf überhaupt gespeichert werden.

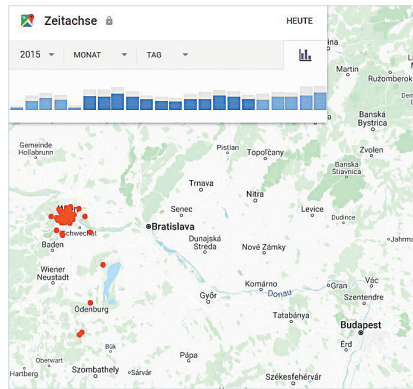
Wer sich nicht durch seitenweise Sucheinträge klicken will, kann eine automatische Löschung festlegen. Auf Wunsch werden die Einträge dann nach drei oder 18 Monaten gelöscht. Voreingestellt ist allerdings das Speichern bis zur manuellen Löschung.

Wer der Speicherung von Web- und App-Aktivitäten in größerem Umfang einen Riegel verschieben möchte, kann dies unter *myaccount.google.com/activitycontrols* tun. Hier kann nicht nur festgelegt werden, ob Sprach- und Videoaufnahmen in die Personalisierung miteinbezogen werden sollen, sondern es lässt sich mit einem simplen Klick auf den Schieberegler auch die Nachverfolgung komplett deaktivieren.

Standort: Google rekonstruiert unseren Tagesablauf

Sobald die Ortungsfunktion am Smartphone oder am Computer aktiviert ist, weiß Google, wo sich der Nutzer wann und wie lange aufgehalten hat. Wird über Google Maps navigiert, dann sogar, wie lange die Fahrt gedauert hat und wo Zwischenstopps eingelegt wurden. Der Dienst fasst all diese Infos im Standortverlauf – einsehbar unter *maps.google.com/locationhistory* – zusammen und zeichnet sogar für einzelne Tage Bewegungsmuster auf. So lässt sich für Jahre zurückverfolgen, wo man sich zu einem bestimmten Zeitpunkt aufgehalten hat.

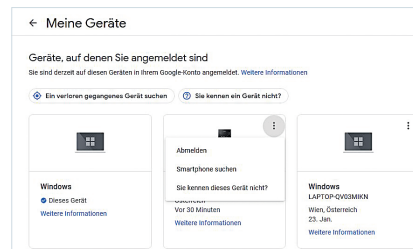
In der Zeitachse lassen sich Jahr, Monat und Tag einstellen. Mit einem Klick werden weitere Details zu den vermeintlich oder tatsächlich besuchten Orten angezeigt. Die Einträge können korrigiert oder einzeln über das Dreipunktmenü gelöscht werden. Für



andere Nutzer sind diese Informationen nicht einsehbar. Grundsätzlich kann der Standortverlauf pausiert werden. Das bedeutet aber nicht, dass die bisher gesammelten Daten verschwinden. Außerdem wird der Nutzer weiterhin über andere genutzte Apps und Dienste getrackt, selbst dann, wenn die Ortungsfunktion der verwendeten Geräte inaktiv ist. Das lässt sich nur durch die pauschale Deaktivierung der Web- & App-Aktivitäten (siehe *Aktivitätenverlauf*) einschränken. Leider ist, im Gegensatz zu gespeicherten Suchanfragen, eine automatische Löschung nach einem festgelegten Zeitraum bis dato nicht möglich. Die gesammelten Standortdaten können nur als Ganzes gelöscht werden.

Seit November 2019 wird für die mobile App-Version von Maps ein Inkognito-Modus ausgerollt, der eine Nutzung der App ohne Standort-Speicherung erlaubt. Allerdings verhindert er immer noch nicht die Speicherung der Nutzeraktivitäten durch andere Apps oder Google-Services.

Google weiß, welche Geräte Sie nutzen

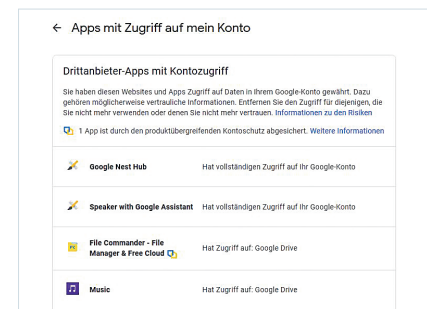


Google führt über Smartphones, Tablets oder Computer Buch, auf denen Sie sich mit Ihrem Google-Konto einloggen. Unter *myaccount.google.com/device-activity* sind alle Logins ersicht- lich. Unter dem Gerätenamen erfahren

Sie, zu welchem Datum, von welchem Standort aus und mit welchem Browser das Gerät zuletzt genutzt wurde. Kommt Ihnen ein Gerät in der Liste spanisch vor, haben möglicherweise Dritte Kontozugriff – dann empfiehlt es sich, das Google-Passwort zu ändern.

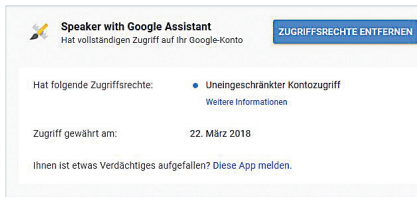
Haben Sie ein älteres Smartphone verloren oder verkauft, ist es hier möglich, das entsprechende Gerät aus der Liste zu entfernen, sollten Sie noch darauf angemeldet sein – dadurch wird das Konto von allen Google-Apps auf dem Gerät ausgeloggt. Haben Sie Ihr Smartphone verloren, kann das Menü auch helfen, es aufzuspüren. Entweder auf *Ein verlorengegangenes Gerät suchen* klicken oder *myaccount.google.com/find-your-phone-guide* aufrufen. Hier können Sie verschiedene Schritte unternehmen, um die Daten auch aus der Ferne zu schützen. Das geht allerdings nur, wenn das entsprechende Device auch eingeschaltet ist.

Diese Apps haben Zugriff auf Ihre Daten



Wird eine neue Applikation am Android-Smartphone installiert, zeigt das System an, welche Zugriffsrechte die App benötigt. *myaccount.google.com/permissions* listet alle Geräte und Services auf, denen Zugriffsrechte erteilt wurden. Mit einem Klick auf einen der Dienste können Sie Details zum Kontozugriff einsehen, die Zugriffsrechte entfernen und die App im Zweifelsfall als verdächtig an Google melden.

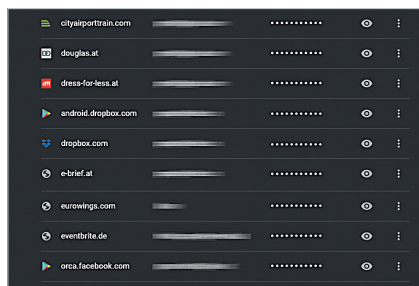
Verwenden Sie das Google-Konto, um sich bei Apps und Online-Services anzumelden? Auch die so verknüpften Dienste sind hier aufgelistet, mitsamt Details, welche Informationen für sie einsehbar sind und wann sie zuletzt genutzt wurden. Google weiß somit, wann, wie lang und wie oft Sie bestimmte Dienste verwenden.



In den Einstellungen des Android-Smartphones können App-Berechtigungen differenzierter eingeschränkt werden. Das System listet in den Berechtigungseinstellungen Zugriffspunkte wie Kamera, Mikrofon oder Kalender auf und zeigt alle damit verbundenen Apps. Entzieht man einer App einzelne Berechtigungen, kann es sein, dass diese nicht mehr wie vorgesehen funktioniert.

Ein Sonderfall sind die Google-Apps. Google selbst gibt an, dass etwa Inhalte von Mails auf Gmail nicht gelesen werden. Technisch gesehen hat Google aber durchaus Zugriff auf jede empfangene oder geschickte E-Mail und kann diese auf werberelevante Informationen scannen. In der Datenschutzerklärung heißt es, dass „Inhalte erhoben“ werden – was genau das bedeutet, ist unklar. Man kann davon ausgehen, dass Absender, Betreff und Links in Mails immer noch von Algorithmen auf relevante Stichworte analysiert werden. Das ist aber auch bei anderen E-Mail-Diensten der Fall.

Chrome ist kein guter Passwort-Safe

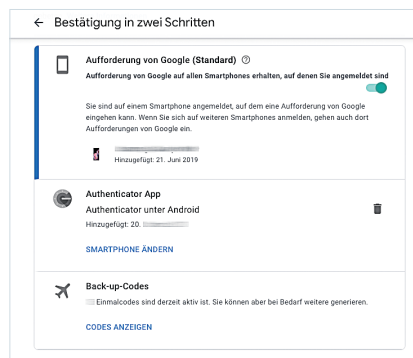


Googles Browser Chrome speichert auf Wunsch Nutzernamen und Passwörter, diese werden dann auch geräteübergreifend synchronisiert. Die meisten Nutzer sind permanent mit ihrem Google-Konto auf den von ihnen genutzten Geräten eingeloggt. Hat eine dritte Person Zugriff auf Smartphone oder PC, kann sie theoretisch in den Browser-Einstellungen die Login-Daten sehen. Für Einfachzugänge bei

Online-Gewinnspielen oder öffentliche Foren ist es sicherlich bequem, das Passwort zu speichern. Grundsätzlich raten wir aber davon ab. Bei Bedarf ist der Griff zum Passwort-Safe besser, dafür gibt es gute Open-Source-Programme wie KeePass, 1Password oder LastPass.

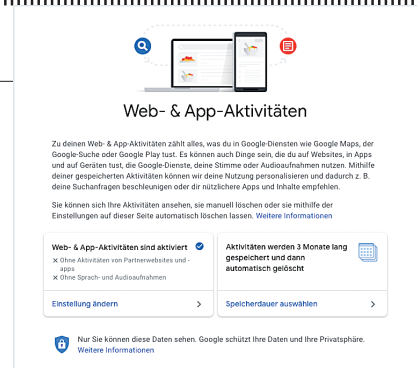
Auch Lesezeichen werden geräteübergreifend synchronisiert. Man muss sich darüber im Klaren sein, dass Google sehr wahrscheinlich daraus Interessen ableitet und diese Daten nutzt, um spezifisch Werbung zu schalten.

Konto zweifach absichern



Die im Google-Account gespeicherten Daten sind nicht nur für den Betreiber interessant. Denn selbst wenn man Anzeigeeinstellungen, Standort- und Aktivitätenverlauf abdreh, bleiben noch immer jede Menge Informationen, die nicht nur für Hacker lohnenswert sind, sondern unter anderem auch für Kollegen im Büro von Interesse sein können. Um Schnüffeleien jedweder Art zu verhindern, sollten die Kontozugangsdaten nie im Browser gespeichert, sondern immer manuell eingegeben werden. Wichtig ist auch, sich nach der Nutzung wieder abzumelden.

Zusätzlich empfehlen wir, das Sicherheitsfeature *Bestätigung in zwei Schritten* zu aktivieren (**Account-Einstellungen > Sicherheit > Bei Google anmelden**). Sie bekommen dann bei jedem Konto-Login via Browser von Google eine Aufforderung ans Smartphone geschickt, in der der Anmeldevorgang bestätigt werden muss. Dadurch erhält selbst jemand, der ihr Google-Passwort kennt oder errät, keinen Zugriff aufs Konto und die damit verbundenen Dienste.



Fazit: Wer unsichtbar sein will, muss Google entsagen

Wer ein mit dem Internet verbundenes Gerät nutzt, muss sich darüber im Klaren sein, dass es völlige Anonymität nicht gibt. Dienste nutzen unsere Daten schon allein, um so zu funktionieren, wie sie sollen. Dabei ist es aber ein Unterschied, ob eine App den aktuellen Standort liest und wieder löscht oder Login-Daten speichert und private Fotos scannt. Letztendlich sollte man immer das Kleingedruckte lesen. Googles Apps können enorm nützlich sein, und durch die vielen neuen Tools kann sich jeder Anwender einen recht genauen Überblick darüber verschaffen, welche Daten er oder sie zur Verfügung stellt. Für den Anfang lohnt sich ein Privatsphärecheck unter *myaccount.google.com/privacycheckup*, in dem Google Schritt für Schritt durch alle im Artikel genannten Einstellungen führt.

Das Unternehmen bietet darüber hinaus die Möglichkeit, eine manuelle Löschung der Daten über einen beliebigen Zeitraum hinweg zu beantragen. Dafür gibt es den Menüpunkt **Aktivitäten löschen** in den Aktivitätseinstellungen unter *myactivity.google.com*. Zuvor – oder eigentlich generell – empfiehlt sich eine Sicherung der Google-Daten: Unter *google.com/takeout* können Sie sämtliche über Ihr Nutzungsverhalten gespeicherten Daten herunterladen. <<

