Die Privacy-Checklisten

Mehr Datenschutz mit wenig Aufwand

Moderne Software verlockt ihre Nutzer dazu, private Daten auszulagern und damit überall im Zugriff zu haben. Die Hersteller machen per Voreinstellung alle Datenschleusen auf – und profitieren von der Fülle an persönlichen Nutzerdaten. An vielen Stellen können Sie ohne großen Aufwand und Komfortverlust gegensteuern. Unsere Privacy-Checklisten zeigen, wie es geht.

Von Holger Bleich

Für Google oder Facebook sind unsere Daten ein Rohstoff, mit dem sich personalisierte Angebote schmieden lassen – aber auch kleinere Unternehmen mischen mit. Viele von ihnen erfassen Informationen wo immer es geht. Diese Berge von Daten wecken auch Begehrlichkeiten von Strafverfolgern und Geheimdiensten. Dass einige Konzerne allzu bereitwillig mit derlei Behörden kooperieren, ist spätestens seit den Snowden-Enthüllungen bekannt.

Nicht nur die Betriebssysteme von Desktop-PCs und Smartphones, sondern auch jede mit dem Internet sprechende Software ist in der Lage, die Privatsphäre des Nutzers zu unterminieren. Jeder nutzt immer mehr dieser potenziellen Datensensoren. Weil es im Interesse der Hersteller liegt, möglichst alle Nutzer- und Nutzungs-Informationen zu sammeln, sind oft viel zu viele Datensammel-Schnittstellen erst einmal scharfgestellt. Per Opt-out sollten Sie sich selbst darum kümmern, einige Schotten dicht zu machen.

Dabei unterstützt Sie c't mit den folgenden Checklisten. Redakteure aus den jeweiligen Fachgebieten haben zusammengestellt, wie Sie mit geringem Aufwand das Datenschutz-Niveau auf dem jeweiligen Gerät oder in der Software deutlich erhöhen können. Dabei sind Beobachtungen aus Kontakten mit Lesern ebenso eingeflossen wie persönliche Erfahrungen und Vorlieben.

Wohlgemerkt steht hinter keiner der Listen der Anspruch, den absoluten Schutz der Privatsphäre zu gewährleisten. Vielmehr stellen sie einen möglichen Kompromiss vor: Leicht umzusetzende Maßnahmen helfen, den Datenabfluss zu dämmen, ohne allzuviel Nutzungskomfort einzubüßen.

Graduell statt radikal

Dieses Unterfangen ist nicht immer leicht – zum Beispiel Android: Ein Smartphone-Betriebssystem, das de facto dazu konzipiert wurde, Nutzerdaten in die Hersteller-Cloud zu pumpen, lässt sich nur in Teilen bändigen. Hinzu kommt in diesem Fall, dass nicht nur mehrere Versionsstände von Android auf dem Markt sind, sondern auch noch jeder Handy-Hersteller sein eigenes Süppchen kocht: Selbst, wenn Sie die Kommunikation Ihres Android-Smartphones mit Googles Servern minimieren, lauschen vielleicht noch Samsung, LG oder Huawei mit.

In c't 4/17 haben wir deshalb ausführlich erläutert, welche Maßnahmen nötig sind, um Android komplett zum Schweigen zu bringen [1]. In letzter Konsequenz klappt das tatsächlich nur, wenn Sie Android vom Smartphone verbannen und durch eines der alternativen Custom-ROMs ersetzen – mit allem damit einhergehenden Funktionsverlust. Denn dann ist es eben kein ganz vollwertiges Android-Smartphone mehr. In der Privacy-Checkliste dagegen geht es um eine graduelle Verbesserung der Situation, die auch Nicht-Experten problemlos erreichen können.

Mithörende Betriebssysteme

Eine besondere Bedeutung für den Schutz der Privatsphäre kommt den Desktop-Betriebssystemen zu. Sie landen mittlerweile mit einer großen Ausstattung eigener Software auf den Geräten. Konzerne wie Microsoft, Google und auch Apple locken die Anwender mit vielen nützlichen Funktionen in ihre Clouds – weil sie großes Interesse an deren persönlichen Daten haben. Die Privacy-Checkliste zu Windows 10 etwa belegt drastisch, an wie vielen Stellen Microsoft versucht, Informationen abzugreifen.

Weil die Hersteller dabei bisweilen schlampig arbeiten, ist es ratsam, aufmerksam zu sein und die Nachrichtenlage zu verfolgen. Zum Beispiel Apple: Wer im Webbrowser Safari in macOS seinen Surf-Verlauf löscht, sollte sich nicht sicher sein, dass die eventuell sensible Historie auch wirklich entfernt ist. Apple synchronisiert den Verlauf nämlich permanent in die iCloud, sofern der Mac daran angebunden ist. Die vom Nutzer entfernten Einträge verschwinden zwar lokal von allen synchronisierten Geräten, eine Rekonstruktion aus der iCloud ist aber auch rund ein Jahr später noch möglich, wie der Forensik-Software-Hersteller Elcomsoft herausfand. Er rekonstruierte erfolgreich exakte Zeitpunkte und die URLs von gelöschten Verläufen. Apple reagierte und behob das Problem – ein mulmiges Gefühl bleibt.

Selbst das an und für sich Privacy-freundliche Linux ist nicht ganz von Datenschutz-Problemen frei. So war die Distribution Ubuntu Desktop bereits 2012 ins Gerede gekommen, weil das Betriebssystem selbst bei lokalen Datei-Suchen die Such-Strings an den Ubuntu-Sponsor

Canonical schickte. Diese Informationen landeten teilweise bei Amazon, das sie Medienberichten zufolge für personalisierte Werbung nutzte. Richard Stallman, Präsident der Free Software Foundation, brandmarkte deshalb Ubuntu gar als „Spyware“. Erst 2016 hat Distributor Canonical das umstrittene „Feature“ endgültig aus Ubuntu entfernt.

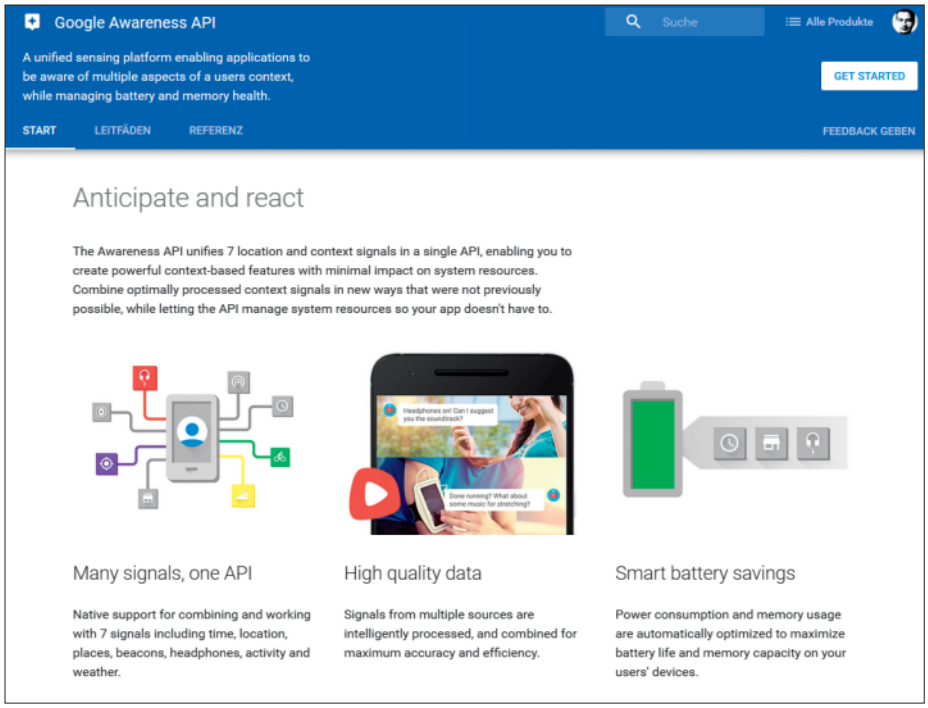
Datengrundschutz

Die folgenden Privacy-Checklisten liefern konkrete Empfehlungen, sollten Sie aber nicht dazu verleiten, grundsätzliche Dinge außer Acht zu lassen. Dazu gehört etwa, die vielen Online-Accounts bei den Web-Diensten vor fremden Zugriff zu schützen. Einen größeren Eingriff in die Privatsphäre als den böswilligen Abzug persönlicher Daten aus womöglich kriminellen Motiven gibt es nicht. Wählen Sie also sichere Passwörter und nutzen Sie wo immer möglich die Zwei-Faktor-Authentifizierung. Verzichten Sie auf das allzu bequeme Single-Sign-In, wie es etwa Facebook bietet – wer Ihren Facebook-Account kapert, bekäme dann nämlich den Generalschlüssel zu Ihrer Online-Identität in die Finger.

Vermeiden Sie die Konzentration all Ihrer persönlichen Informationen in einer oder wenigen Händen. Nutzen Sie eben nicht nur Google, so komfortabel die kostenlosen Services des Megakonzerns auch sein mögen. Denken Sie über einen alternativen E-Mail-Provider nach, speichern Sie Ihre Kontakte woanders, und legen Sie Ihre Fotos bei wieder einem anderen Cloud-Anbieter ab. So erschweren Sie es den Datensammlern, sich ein vollständiges Bild Ihrer Persönlichkeit zusammenzupuzzlen [2].

Awareness-API

Zu selten wird Smartphone-Nutzern vor Augen geführt, wer alles Zugriff auf die Daten erhält, die ihr Handy unablässig sammelt. Wenn ein Fall öffentlich wird, dann meist in unverdächtigem Kontext. Anfang Februar etwa erklärte Ivyrevel, eine Tochterfirma des schwedischen Bekleidungskonzerns H&M, dass sie eine mobile App entwickelt, mit der Kunden Kleidung passend zu ihren Interessen und Gewohnheiten zusammenstellen, gestalten lassen und kaufen können. Dabei helfe der gigantische Datenpool von Google.



Über das Awareness-API gewährt Google fremden Herstellern Zugriff auf Informationen zum Android-Nutzer, die es aus den vielen Smartphone-Sensoren generiert.

Google? Wie das? Nun, seit einigen Monaten gewährt Google über das sogenannte „Awareness-API“ Fremd-Apps Zugriff auf Informationen zum aktuellen Gerätekontext. Die Apps dürfen – nachdem das der Nutzer per Häkchen abgenickt hat – beispielsweise das Wetter zum Standort, Nutzeraktivitäten, besuchte Lokalitäten und Beacons in der Nähe abgreifen. Und genau darüber will die Ivyrevel-App für Android dem jeweiligen Kunden zu via API ermittelten Lebensumständen und Anlässen das passende Outfit automatisiert anbieten.

Das Awareness-API verrät einige der Berechnungen, die Google mit den vielen abgegriffenen Daten der Android-Telefone anstellt. Die Nutzeraktivität etwa lässt sich als „DetectedActivity“-Objekt abfragen, das Werte wie RUNNING für Laufbewegungen, WALKING für Spaziergänge oder ON_BICYCLE für eine vermutete Bewegung mit dem Fahrrad rückmeldet. Google weiß also anhand der Standortdaten nicht nur, *das*, sondern auch *wie* Sie sich bewegen.

Separate Identität

Zu guter Letzt: Lassen Sie sich nicht von Rabatt-Systemen wie Payback, Gutschein-Aktionen oder Gewinnspielen verleiten. Denken Sie stets daran, dass der Deal dort „Goodie gegen persönliche Daten“ lautet. Nutzen Sie das Internet of Things und Geräte wie Wearables, Smartwatches und Fitness-Tracker achtsam. Diese Geräte pumpen kontinuierlich Ihr Verhalten in die Cloud – ebenso wie vernetzte Kühlschränke oder Zahnbürsten. Wer sich für derlei Gadgets eine von den sonstigen Informationen abgekoppelte Fantasie-Identität mit separater Mail-Adresse zulegt, hat schon wieder etwas Privatsphäre hinzugewonnen.

Und nun wünschen wir viel Spaß beim Umsetzen unserer Tipp-Sammlung. Vielleicht helfen die Checklisten ja nicht nur Ihnen, sondern auch Ihrer Familie oder Freunden, denen ansonsten die c’t-Lektüre „etwas zu hoch“ erscheint.

(hob@ct.de) c't

Literatur

[1] Christian Wölbert, Schwerpunkt: Android ohne Google, c’t 4/17, S. 68
[2] Markus Morgenroth, Digital gebrandmarkt, Wie Konsumentendaten gesammelt, gehandelt und genutzt werden, c’t 1/17, S. 64