TIPPS GEGEN DATENKLAU VOM SMARTPHONE/TABLET

1. Manuelle Einrichtung nutzen

Vom Start weg mehr Kontrolle bietet die sorgfältige, manuelle Einrichtung. Das fängt bei der Erstkonfiguration des Betriebssystems an. Unerwünschte, vorinstallierte Apps sollten - sofern möglich - entfernt oder zumindest deaktiviert und gegebenenfalls durch seriöse Alternativen ersetzt werden. Wer seine Apps nur von vertrauenswürdigen Quellen wie den App-Shops der Plattformanbieter herunterlädt, verringert Sicherheitsrisiken.

2. GPS deaktivieren

Klar: Ohne GPS-Koordinaten führt die Navigations-App nicht zum Ziel. Und auch die Datentransfers via WLAN oder Bluetooth sind de facto unverzichtbar. Wer mehr für seine Sicherheit tun und zudem Strom sparen möchte, sollte Ortung und Netzwerkverbindungen nur aktivieren, wenn diese benötigt werden. In der Regel ist das Ein- oder Ausschalten dieser Features im System schnell erledigt.

3. Apps vor Installation ausführlich prüfen

Erst prüfen, dann installieren. Vor dem Herunterladen sollten Sie sich über die App und den Anbieter informieren. Dabei helfen Bewertungen und Kommentare anderer Nutzer. Fordert eine Anwendung nur die Berechtigungen ein, die für die gewünschte Funktion notwendig sind, weckt das mehr Vertrauen, als eine Wetter-App, die unnötigerweise Zugriff auf die Kontakte verlangt. Zudem sollte man Kleingedrucktes wie Datenschutzbestimmungen nicht ungelesen "abhaken".

4. Updates (aufmerksam) installieren

Updates schließen unter anderem Sicherheitslücken und sind daher Pflicht. Doch auch hier sollten Sie genauer hinsehen und deren Installation gegebenenfalls manuell durchführen. Im Zuge einer Aktualisierung können sich "schwarze Schafe" unter den Apps auch gleich noch erweiterte Zugriffsrechte auf Ihre Daten genehmigen.

5. Vorsicht bei In-App-Käufen

Achtsamkeit ist auch bei In-App-Käufen geboten. Die kostenpflichtigen Zusatzangebote werden von den App-Stores teils nicht so genau kontrolliert und gelten mitunter als Hintertür für Malware und Schnüffel-Apps.

6. Mobile Seiten nutzen

Es muss nicht immer eine App sein. Viele Dienste sind auch über mobile Webseiten erreichbar. Die Nutzung ist dann zwar nicht so komfortabel. Vorteil ist aber: Beim Aufruf über den Browser muss sich die Webseite beim Zugriff auf Daten das Einverständnis des Besuchers holen. Bei den Apps läuft der Datenaustausch im Rahmen der einmalig akzeptierten Berechtigungen automatisch im Hintergrund ab.

7. Facebook-Login & Co. Meiden

Als Alternative zu der klassischen, App-basierten Anmeldung erlauben einige Anbieter auch das Login mit den Zugangsdaten beliebter Anwendungen wie Facebook. Wer diesen zugegebenermaßen komfortablen Weg wählt, riskiert, dass die App als zusätzlicher Datensammler für den Login-

Partner fungiert.

8. Inkognito browsen

Beim Internetsurfen speichern die Browser im Privatmodus weniger Daten. Zudem können der Verlauf der besuchten Webseiten und die Cookies in den Einstellungen auch separat gelöscht werden. Allerdings schützen diese Maßnahmen die Privatsphäre nur bedingt.

9. VPN-Dienst nutzen

Wer anonymer surfen möchte, muss seine IP-Adresse verschleiern. Dazu kann der Datenverkehr im Web über zwischengeschaltete Server (Proxy) umgeleitet werden. Oder Sie versuchen eine verschlüsselte VPN (Virtual Private Network)-Verbindung einzurichten. Letztere empfiehlt sich für die Nutzung offener WLAN-Hotspots ohnehin. Allerdings erfordern diese Maßnahmen Kenntnisse in der Einrichtung der benötigten Tools und Dienste.

10. Verschiedene Dienste nutzen

Mehrgleisig fahren. Wer mehr Privatsphäre wahren möchte, sollte häufig genutzte Anwendungen wie Maildienst, Browser und Suchmaschine von verschiedenen Anbietern verwenden. Das erschwert Datensammlern die Erstellung detaillierter Profile. Zum Beispiel bieten die Browsereinstellungen oft mehrere Suchmaschinen zur Wahl. Anbieter wie DuckDuckGo versprechen, keine anwenderbezogenen Daten zu speichern.