Smartphones & Tablets – Von Werbeschleudern und Taschenspionen

In diesem Fachartikel werden Maßnahmen und Applikationen beschrieben, die unerwünschte Werbung, das Nachverfolgen des Benutzerverhaltens und seiner Präferenzen (Tracking) durch Social Media, Werbeanbieter, Internethändler und Mobilgerät-Apps verhindern.

Einleitung

Haben Sie sich auch schon gewundert, dass Sie im Netz nach bestimmten Produkten gesucht oder diese gekauft haben und Sie danach über Wochen von Werbung für diese Kategorie verfolgt werden? Dann ist es großen Werbeanbietern wie Google, Facebook oder Amazon mit Hilfe ihrer Werbenetzwerke erfolgreich gelungen, Sie zu tracken und Ihr Endgerät wieder zu identifizieren. Im Folgenden werden Gegenmaßnahmen am Endgerät selbst oder im Netzwerk beschrieben.

Gegenmaßnahmen am Endgerät

Im Web-Browser (Firefox / Chrome) sind zwei wichtige Browser Add-on-Applikationen empfehlenswert:

1. **uBlock Origin** (der dzt. beste Adblocker, ACHTUNG: es gibt in den App-Stores viele ähnlich klingende Apps, die wirkungslos oder sogar gefährlich sind) und der
2. **EFF Privacy Badger** (ein automatisch lernender Werbe- und Tracking-Blocker)

Auf der Ebene des Web-Browsers werden so die schlimmsten Umtriebe von Social Media und der Werbeindustrie verhindert.

Auf dem Smartphone/Tablet installierte Apps können aber weiterhin unbemerkt im Hintergrund Trackingdaten übermitteln. Dies ist aus zwei Gründen ärgerlich:

1. In manchen Apps sind zwischen 5 und 27 (!) verschiedene Tracking-Mechanismen enthalten, die an Social-Media-Firmen, Internethändler und Werbenetzwerke unkontrolliert Daten übermitteln. Es findet aus Datenschutzsicht ein permanenter, weitgehend unbekannter und selten eingewilligter Datenfluss über das Verhalten des Smartphones/Tablet-Benutzers statt.

   Bei der Erstellung dieser meist kostenlosen Smartphone/Tablet Apps greifen die Programmierer auf vorgefertigte Programmteile der Social Media und Werbeanbieter zurück, kopieren diesen Code zusätzlich in ihre Programme und erhalten für die Einbindung und die anschließend übermittelten Daten Geld.

2. Der zweite Effekt ist, dass diese Datenübertragungen große Datenvolumina (insbesondere eingespielte Werbevideos) erzeugen. Das verlangsamt die Datenübertragung, verbraucht kostenpflichtiges Datenvolumen und auch die Akkulaufzeit wird massiv verkürzt, da ja das Mobilgerät immer wieder Funkverbindungen zur Datenübermittlung aufbauen muss.

Um ungewünschtes Tracking durch Apps zu vermeiden, wird die kostenlose Android App **Blokada** empfohlen. Die App verhindert zuverlässig ungewünschtes Tracking, schont das Datenvolumen und den Akku.

Da die App diametral den Interessen von Google zuwiderläuft, ist sie nicht im App-Store zu finden. Sie muss separat unter

https://blokada.org/index.html

herunterladen und manuell installiert werden. Alle notwendigen Schritte sind gut beschrieben. Eventuell müssen Sie in den Einstellungen Bildschirmsperre & Sicherheit die Option „Installation von Apps aus unbekannten Quellen zulassen" aktivieren.

Für Apple-Smartphones / Tablets ist uns noch keine vergleichbare App bekannt. Apple legt aber auf die Privatsphäre der Benutzer großen Wert und bewirbt dies explizit.

Unter folgendem Link

https://reports.exodus-privacy.eu.org/en/search/

können Trackingmechanismen einer bestimmten App identifiziert werden. Die App kann auch installiert werden und analysiert dann alle installierten Apps.

Gegenmaßnahmen im Netzwerk

Zum Schutz gegen Angriffe, Werbung und Trackingmaßnahmen im Firmen- oder auch Heim-Netzwerk wird eine Firewall empfohlen.

Es handelt sich hierbei nicht um die von den Anbietern zur Verfügung gestellten Modems oder WLAN-Router. Diese bieten nur einen Netzwerkzugriff und keinen Schutz. Die günstigsten performanten Systeme ab ca. EUR 300 basieren auf quelloffenen Firewall-Lösungen wie pfSense oder OPNSense. Auf diesen Firewalls können Werbeblocker und ein sog. Intrusion Detection / Intrusion Prevention System (IDS/IPS) laufen, die auf Basis täglich aktualisierter Listen unwillkommene Websites, Werbung, Tracking und andere gefährliche Angriffe bzw. Datentransfers aus dem Netz erkennen und blockieren. Gleichzeitig werden auch unerwünschte Datentransfers (zB Windows 10 Nutzungsdaten etc.) durch Programme und Apps aus dem internen Netz verhindert.

Wo vorher Werbung, Pop-up Fenster, unaufgeforderte Videos stören, kehrt nun eine herrliche Ruhe ein und ein ungestörtes Surferlebnis wird möglich. Die gleichen vorgenannten Systeme schützen auch die Kinder zu Hause bei ihren ersten Schritten im wilden Internet. Diese Lösung im professionellen Umfeld ist aber mit Aufwand beim Aufsetzen und der Wartung verbunden.

Oben genannte Anwendungen führen auch detaillierte Statistiken über blockierte Verbindungen. Ca. 27% aller DNS-Adressenanfragen werden vom System blockiert und Inhalte nicht heruntergeladen. Innerhalb der blockierten Verbindungen werden wiederum 65% durch von im lokalen WLAN-Netz befindlichen Smartphones/Tablets/IoT-Geräte verursacht. Diese Zahlen basieren auf eigenen Auswertungen der Firmen-Firewall über ein Jahr.

Verlässt man nun mit seinem Smartphone/Tablet diesen „Cordon sanitaire", so verhindern die vorgenannten Anwendungen uBlock Origin / Privacy Badger / Blokada das Einspielen von unerwünschter Werbung und Tracking. Es wird allerdings nicht das gleiche Schutzniveau wie im eigenen Netz hinter der Firewall erreicht.

Zusammenfassung / Empfehlungen

Zwischen 70-90% aller Apps verwenden nicht DSGVO-konforme Tracking-Mechanismen. Das heißt die Daten werden ohne Einwilligung des Benutzers erhoben und an Social Media / Internethändler / Werbenetzwerke übermittelt. Das Blockieren von Cookies reicht nicht mehr aus. Die Social Media / Werbeanbieter verfügen über sehr ausgefeilte sog. Fingerprinting-Methoden, mit denen sie genaue Profile des Nutzers erheben. (zB das OCEAN 5 Modell).

Prüfen Sie regelmäßig, welche App oder Programme Sie auf Ihrem Tablet/Smartphone wirklich benötigen.

Durch die vorgenannten Maßnahmen sind Sie zukünftig ein weniger gläserner Nutzer des Internets. Die verringerte Preisgabe von Information erhöht auch die Sicherheit ggü. Pishing- und Malware-Angriffen.

Mag. Markus Lenotti, Sept. 2019

Geschäftsführer
Lenotti Advisors GmbH