KEEPER | Pressemitteilung

Phone-Tracking: Wertvoll, aber manchmal auch riskant

So lässt sich die Standortverfolgung im Bedarfsfall blockieren

Von Anne Cutler, Senior Director of Global Communications, Keeper

Smartphones sind aus dem Alltag nicht mehr wegzudenken, denn sie sorgen an vielen Stellen für Erleichterungen – sowohl privat als auch im Business. Allerdings sammeln sie auch jede Menge Informationen, u.a. über die Orte an denen man sich aufhält. Das mag vielfach sinnvoll sein, etwa wenn man navigiert oder von einem Uber-Fahrer angeholt werden möchte. Doch außerhalb derartiger Situationen ist es ratsam, die Trackingfunktion abzuschalten, damit das eigene Bewegungsprofil nicht von Apps, Werbeanbietern oder sogar Hackern missbraucht werden kann.

Mit ein paar Tricks lässt sich das Phone-Tracking auf ein Minimum beschränken.

App-Berechtigungen

Über die Systemsteuerung des Mobilgeräts lassen sich die Berechtigungen überprüfen und ändern. iPhone-Nutzer können beispielsweise auf die Registerkarte „Datenschutz & Sicherheit“ klicken und dann auf die Ortungsdienste gehen. Hier sind die Ortungseinstellungen der einzelnen Apps hinterlegt. Am besten ist es die Apps so zu konfigurieren, dass diese zuerst fragen müssen, bevor sie einen Standort verwenden dürfen oder dass der Standort nur verwendet werden darf, während die App geöffnet ist.
Bei Android-Handys verhält es sich etwas anders. In der Regel kann jedoch in den Einstellungen das Standortsymbol angetippt und für alle oder einzelne Apps ein- oder ausgeschaltet werden. Die Auswahlmöglichkeiten sind bei den verschiedenen Herstellern ähnlich wie bei iOS.

iPhone-Datenschutz

Apple hat darüber hinaus weitere Optionen, um das Tracking durch Drittanbieter zu reduzieren. In der Einstellung "Datenschutz & Sicherheit" gibt es auf der Registerkarte "Tracking" einen Schalter, mit dem man die Anforderung der Nachverfolgung zulassen oder ablehnen kann. Ist diese Option deaktiviert, werden neue App-Anfragen automatisch abgelehnt.

Personalisierte Werbung

Datenschutzexperten empfehlen, die interne Anzeigenkennung von Google- oder Apple-Geräten zu blockieren. Auf dem iPhone kann man dies unter der Datenschutzeinstellung. Hier scrollt man zum Apple Advertising und deaktiviert personalisierte Werbung. Auf neueren Android-Smartphones geht man ebenfalls auf die Datenschutzeinstellungen und dann zu Werbeanzeigen, wo man die Werbe-ID löschen sollte.

Punktgenaue Ortsangabe

Unabhängig davon, ob es sich um ein Android- oder Apple-Gerät handelt, verfügen beide über die Möglichkeit, den Standort des Geräts genau bestimmen zu können. Das funktioniert über die Signale und Daten integrierter Sensoren wie etwa dem Barometer oder

Beschleunigungsmesser. So kann das Mobilgerät den Standort präzise bestimmen – auch dann, wenn beispielsweise innerhalb eines Gebäudes kein GPS-Signal vorhanden ist. Wer nicht möchte, dass eine App auf diese Informationen zugreifen kann, sollte nur die allgemeinen Standortangaben freigeben. Dafür deaktiviert man auf Android-Smartphones die Einstellung "Standortgenauigkeit" und auf dem iPhone schaltet man dieses Feature für jede einzelne Apps ein- oder aus.

Google-Konto
Neben den App-Berechtigungen sollten auch die Berechtigungen für das Google-Konto überprüft werden. Auf dem Google-Account geht man auf den Abschnitt „Daten & Datenschutz“, wo sich die Steuerelemente für den Standortverlauf befinden. Bei den letzten Änderungen wird der Verlauf nach drei Monaten gelöscht – das kann man jedoch individuell in den Standardeinstellungen ändern.

Browser
Auch beliebte Smartphone-Browser wie Safari oder Chrome können den Standort eines Mobiltelefons verraten. Das lässt sich vermeiden, indem man andere Browser verwendet wie etwa DuckDuckGo, Firefox Focus oder Ecosia. Diese datenschutzorientierten Browser werden für den Fall, dass sie über eine IP-Adresse auf den Standort zugreifen müssen, eine Standortfreigabe anfragen und nicht unautorisiert darauf zurückgreifen.

Mein Gerät suchen
Telefone oder Tablets können mit den Funktionen "Find My" von Apple oder "Find My Device" von Google gesucht werden. Auch diese Funktion lässt sich bei Bedarf deaktivieren, evtl. wenn der Verdacht besteht, dass sich jemand Zugriff auf das eigene Apple- oder Google-Konto verschafft hat.

###

Über Keeper Security:
Keeper Security verändert die Cybersicherheit für Millionen von Einzelpersonen und Tausende von Unternehmen weltweit. Die intuitive Cybersicherheitsplattform von Keeper ist mit einer End-to-End-Verschlüsselung ausgestattet und genießt das Vertrauen von Fortune-100-Unternehmen, um jeden Benutzer auf jedem Gerät und an jedem Standort zu schützen. Unsere patentierte Zero-Trust- und Zero-Knowledge-Lösung für das Privileged Access Management vereint die Verwaltung von Unternehmenspasswörtern, Geheimnissen und Verbindungen mit Zero-Trust-Netzwerkzugriffen und Remote-Browser-Isolation. Durch die Kombination dieser wichtigen Identitäts- und Zugriffsverwaltungskomponenten in einer einzigen cloudbasierten Lösung bietet Keeper beispiellose Transparenz, Sicherheit und Kontrolle und gewährleistet gleichzeitig die Einhaltung von Compliance- und Audit-Anforderungen. Erfahren Sie unter KeeperSecurity.com, wie Keeper Ihr Unternehmen vor den heutigen Cyberbedrohungen schützen kann.

Folgen Sie Keeper auf Facebook Instagram LinkedIn X YouTube TikTok

Pressekontakt für Keeper in DACH:
Alexandra Schmidt, +49 170 387 10 64
Thilo Christ, +49 171 622 06 10
keeper@tc-communications.de