

Beunruhigungsspiele

Missbrauch von Apples AirTags für Stalking und Überwachung

„Datenschutz serienmäßig“ verspricht Apple für seine AirTags. Doch in der Praxis lassen sich Personen und Fahrzeuge wochenlang orten, weil Apples AirTags anders als zugesichert nicht vor unerwünschtem Tracking warnen.

Von Mirko Dölle

Ein simpler Lautsprecher ist bei Apples AirTags das wichtigste Bauteil, um Personen vor unerwünschtem Tracking durch aufdringliche Verehrer, gewalttätige Ehepartner oder extremistische politische Gegner zu schützen. Denn die von Apple beworbene optische Warnung vor unerwünschtem Tracking gibt es nur bei iPhones, deren Marktanteil unter 30 Prozent liegt. Somit ist der größte Teil der Bevölkerung darauf angewiesen, dass sich ein AirTag per Tonfolge selbst zu erkennen gibt, was aber frühestens nach etlichen Stunden oder Tagen passiert und was sich leicht dauerhaft unterbinden lässt, wie c't herausfand.

Das AirTag ist kein neues Produkt. Ortungs-Tags etwa für Schlüsselbund oder Koffer gibt es längst von verschiedenen Herstellern, wobei Apple die Nahbereichssuche um UWB (Ultra Wide Band) ergänzt und auch NFC in die AirTags integriert hat, damit der Besitzer dem Finder eine Nachricht zukommen lassen kann. Auf größere Distanz ist die Funktionsweise der Tags verschiedener Hersteller ähnlich, sie arbeiten als Funkbaken und senden via Bluetooth in regelmäßigen Abständen eine Kennung (Beacon, Leuchtfrequenz) aus, anhand derer sie identifiziert werden können. Empfängt ein Smartphone in der Nähe die Aussendung, verknüpft es die Daten mit seiner eigenen aktuellen Position und leitet sie an den Hersteller weiter. Die in der Cloud gespeicherten Positions-

daten kann der Besitzer mit einer speziellen App abrufen, um sein Tag zu finden.

Doch während andere Hersteller darauf angewiesen sind, dass möglichst viele Smartphone-Besitzer ihre proprietäre App installieren, hat Apple die Funktion direkt in iOS integriert: Jedes Apple-Mobilgerät, das selbst über die „Wo ist?“-App auffindbar ist, leitet die Aussendungen der AirTags an Apple weiter. Diese Funktion ist standardmäßig auf allen Apple-Mobilgeräten aktiviert und setzt iOS 14.5 voraus. So verfügt Apple über ein dichtes Netzwerk aus rund einer Milliarde Geräten weltweit, um die Position von AirTags zu ermitteln, während andere Hersteller selbst in Großstädten nur wenige hundert aktive Teilnehmer verzeichnen – das sind meist Besitzer solcher Tags.

Damit AirTag-Nutzer nicht von fremden Personen verfolgt werden können, wechseln AirTags ihre individuellen Merkmale wie die Bluetooth-MAC-Adresse ständig und verschlüsseln ihre Daten, so dass sie letztlich nur der Eigentümer identifizieren kann. Selbst Apple weiß nicht, welches AirTag wem gehört. Doch das macht es unmöglich, im Missbrauchsfall den Täter zu identifizieren.

Unsichtbar

Aufgrund der geringen Größe und der langen Laufzeit von bis zu einem Jahr lassen sich AirTags sehr leicht etwa im Innenfutter einer Jacke, eines Rucksacks oder einer Handtasche verstecken, um damit Personen unbemerkt zu überwachen: Solange das AirTag immer wieder in der Nähe seines Eigentümers auftaucht, etwa weil man im gleichen Haushalt wohnt oder sich an der Arbeit regelmäßig über den Weg läuft, erscheint keine Meldung im iPhone der überwachten Person. Auch bleibt das AirTag stumm.

Erst, wenn es für längere Zeit vom Eigentümer getrennt ist, bei Redaktionschluss betrug die Frist mindestens drei Tage, alarmiert das AirTag akustisch. Allerdings erst, wenn man es anfasst oder stark beschleunigt – die Bewegungen einer

normalen Autofahrt reichen in unseren Tests nicht aus, um den Alarm zu triggern.

Von der versprochenen iPhone-Warnung vor einem unbemerkten Begleiter sollte man nicht viel erwarten: In einem unserer Versuche dauerte es über 8 Stunden, bis uns das iPhone ein fremdes AirTag meldete, in mehreren anderen Fällen erhielten wir selbst nach Wochen keine einzige Warnung. Welche iPhones unter welchen Umständen und nach welcher Zeit überhaupt eine Warnung anzeigen, verrät Apple auch auf Nachfrage nicht. Es ist also davon auszugehen, dass neben den Android-Besitzern auch eine ganze Menge iPhone-Besitzer keine Warnung vor fremden AirTags erhalten.

Apple braucht Google

Apple hat in einer Stellungnahme gegenüber c't angekündigt, im Laufe des Jahres eine Android-App bereitstellen zu wollen, mit der man AirTags und andere „Wo ist?“-kompatible Geräte auffinden können soll, die eine andere Person fernab des Eigentümers begleiten. Damit hätten Android-Nutzer immerhin eine Chance, ein AirTag frühzeitig zu entdecken. Außerdem soll sich das AirTag künftig schon nach 8 bis 24 Stunden akustisch bemerkbar machen und nicht erst nach drei Tagen. Das ist ein Schritt in die richtige Richtung, genügt aber nicht: Es vergeht immer noch zu viel Zeit, in der man das AirTag unbemerkt etwa bis nach Hause tragen könnte.

Um sein Datenschutzversprechen effektiv einzulösen, braucht Apple Unterstützung von Google: Android sollte genau wie iOS ohne eine spezielle App automatisch vor Ortungsgeräten in der Nähe warnen. Für die Corona-Kontakt-Warnungen, bei denen ebenfalls Bluetooth zum Einsatz kommt, kooperieren beide Hersteller bereits seit einem Jahr. Wie wäre es mit einer weiteren Kooperation, damit künftig alle Android- und iOS-Anwender über fremde Tracker informiert werden? Datenschutz und Privatsphäre mögen auf anderen Märkten keine Rolle spielen, in Europa

und insbesondere in Deutschland sind sie gute Verkaufsargumente.

Eine Funktion zur aktiven Suche nach fremden Ortungsgeräten ist weder für iOS noch für Android vorgesehen, man kann AirTags also auch künftig erst entdecken, wenn man sie über Stunden mit sich herumgetragen hat. Damit bleibt der Lautsprecher des AirTags die wichtigste Warneinrichtung, um ein fremdes AirTag zu bemerken. Doch ausgerechnet der Lautsprecher lässt sich leicht zum Schweigen bringen.

Unerhört

Um ein AirTag für immer verstummen zu lassen, benötigt man weder viel Geschick noch besonderes Werkzeug: An der richtigen Stelle angesetzt genügen ein Akkuschrauber und ein Bohrer, um in wenigen Minuten mit einem einzelnen Bohrloch die im AirTag verbaute Lautsprecherspule zu durchtrennen. Mit den Details konfrontiert kam Apple Deutschland in der offiziellen Stellungnahme gegenüber c't zu der Einschätzung, dass man „das Aufbohren nicht als eine sehr einfache Deaktivierungsmöglichkeit sehen“ würde. Dabei erleichtert der Aufbau des AirTags diese Modifikation; hätte Apple die Lautsprecheranschlüsse auf der Rückseite der Platine verlötet, würde man das AirTag beim Aufbohren zwangsläufig zerstören.

Ein stummes AirTag meldet aber weiterhin seine Anwesenheit an alle Apple-Geräte in seiner Nähe und lässt sich somit weiter aus der Ferne orten. Apple hat es versäumt, Manipulationen zu erkennen und das AirTag daraufhin abzuschalten. Dabei ist das keine Raketenwissenschaft, eine einfache Durchgangsprüfung oder die Beobachtung der Stromaufnahme des Verstärkers würden eine durchtrennte Lautsprecherspule sofort entlarven. Ohne solche Schutzmaßnahmen ist Stalking Tür und Tor geöffnet – und der Täter muss nicht einmal strafrechtliche Schritte befürchten.

Gesetzeslücke

Ungeachtet möglicher zivilrechtlicher Ansprüche bestehen nach unseren Recherchen Zweifel an der Strafbarkeit, wenn etwa der eifersüchtige Mann den Aufenthaltsort seiner Partnerin mit einem AirTag überwacht: Der Stalking-Paragraf 238 des Strafgesetzbuchs erfasst beispielsweise nur Kontaktaufnahme, Datendiebstahl oder Bestellungen auf fremden Namen – den Aufenthaltsort zu überwachen und Bewegungsprofile zu erstellen ist jedoch nicht mit Strafe bedroht.

Diese Lücke hat das Bundesjustizministerium bereits erkannt und in der geplanten Novelle des § 238 das Ziel formuliert, sie zu stopfen. Jedoch sieht der aktuelle Gesetzesentwurf vom 24. März 2021 dafür aber weiterhin kein Verbot vor. Auch die DSGVO bietet keine konkrete Handhabe, denn der eifersüchtige Mann könnte versuchen, sich auf die „Haushaltsausnahme“ zu berufen. Sie erlaubt explizit die Verarbeitung personenbezogener Daten zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten. Zudem müsste der Mann in Schädigungsabsicht handeln, um den Tatbestand der infrage kommenden datenschutzrechtlichen Strafnorm zu verwirklichen.

Damit zeichnet sich das Missbrauchspotenzial der AirTags deutlich ab: Wer die Wohnung etwa infolge häuslicher Gewalt verlässt und Zuflucht sucht, muss künftig damit rechnen, vom Lebenspartner binnen Stunden aufgespürt zu werden – dank eines im Koffer, in der Handtasche oder in der Jacke versteckten AirTags. Und zwar auch dann, wenn es sich um ein unmodifiziertes Exemplar handelt, da die akustische Warnung und eine etwaige Anzeige auf dem iPhone erst nach vielen Stunden ausgelöst wird, wenn man seinen neuen Aufenthaltsort längst verraten hat.

Auch dürfte das AirTag zum Lieblingsspielzeug für politische Extremisten avan-

cieren, mit dem sie billig und extrem effizient den Aufenthaltsort missliebiger Lokalpolitiker überwachen können. Einfach hinter die Stoßstange geklebt weiß man immer, wo man das Opfer abpassen kann. Und selbst wenn das AirTag etwa vom Staatsschutz entdeckt wird: Sofern er nicht seine Fingerabdrücke darauf hinterlassen hat, führt keine Spur zum Täter.

Fazit

Apple hat mit dem AirTag eine leistungsfähige, hoch entwickelte Ortungstechnik auf den Markt geworfen, die sich leicht modifizieren und missbrauchen lässt. Der vom Hersteller versprochene serienmäßige Datenschutz existiert faktisch nicht: Der Lautsprecher als wichtigstes Schutzmerkmal lässt sich leicht lahmlegen und Apple hat es verschlafen, Vorkehrungen gegen Manipulationen zu treffen und das AirTag dann unschädlich zu machen.

Nicht einmal die versprochene iPhone-Warnung vor fremden AirTags funktioniert zuverlässig, und wer ein anderes Smartphone verwendet, hat noch weniger Chancen, ein untergeschobenes AirTag zu entdecken. Doch selbst wenn man zufällig ein fremdes AirTag bei sich entdeckt, kann man kaum mehr tun, als es abzuschalten: Nicht einmal Apple kennt den Besitzer. (mid@ct.de) 



Die Lautsprecherspule in der Mitte ist auf der Oberseite der Platine verlötet und lässt sich daher leicht anbohren. Damit verstummt das AirTag für immer, ohne seine Ortungsfunktion einzubüßen.

Bild: iFixit.com