Achtung, Handy hört mit!

Ausprobiert: Wie Smartphone-Apps Gespräche belauschen können

Onlinewerbung bezieht sich häufig auf Themen, über die man kurz zuvor gesprochen hat. Das weckt seit jeher den Verdacht, dass Smartphones permanent mitlauschen und Gesprächsinhalte an Facebook, Google & Co. weitergeben. Aber ist das realistisch? Ein Team des Bayerischen Rundfunks hat es ausprobiert – und kam ziemlich weit.

Von Ronald Eikenberg

Kaffeepause: Sie unterhalten sich mit einem Kollegen über ein bestimmtes Thema und kurz darauf erscheinen bei Facebook, Google oder Instagram Werbeanzeigen, die erstaunlich gut dazu passen. Bei c't melden sich immer wieder Leser, die Ähnliches beobachtet haben.

Häufig steht der Verdacht im Raum, dass Smartphone-Apps ungefragt die Mikrofone einschalten, um heimlich Gespräche und Telefonate zu belauschen. Das junge „AI + Automation Lab" des Bayerischen Rundfunks (BR) ist dem Verdacht nachgegangen. Für das YouTube-Format „PULS Reportage" (siehe ct.de/ycmg) versuchten die Journalisten, unter anderem die Apps von Instagram, TikTok & Co. mit fingierten Gesprächen aus der Reserve zu locken: Während mehrere Smartphones mit einschlägigen Social-Media-Apps in Hörweite lagen, unterhielten sich die BR-Mitarbeiter zum Beispiel über Hundefutter und Legosteine.

Anschließend wurde überprüft, ob in den beteiligten Social-Media-Accounts Werbung zu den besprochenen Themen erscheint. Tatsächlich tauchte in einem Fall Lego-Werbung bei Instagram auf, allerdings erst vier Tage später. Da Lego allgemein viel Onlinewerbung in sozialen Netzwerken schaltet, ist die Wahrscheinlichkeit hoch, dass es sich um einen Zufallstreffer handelt.

Das BR-Team prüfte zudem, ob eine App technisch überhaupt dazu in der Lage sein kann, das Mikrofon des Smartphones unbemerkt anzuzapfen. Dazu entwickelte das Team eine Test-App für Android und iOS, die heimlich Gespräche im Hintergrund aufzeichnen sollte. Diese wurde auf einem iPhone 12 (iOS 14.7.1) und auf einem Samsung Galaxy A22 5G mit Android 11 installiert.

Katzen als Spionagehelfer

Die App forderte vom Nutzer über die jeweiligen Betriebssystem-APIs das Recht ein, aufs Mikrofon zuzugreifen. Hierfür lieferte sie sogar einen plausiblen Grund: Die App war einem Social Network nachempfunden und bot die Möglichkeit, Katzenfotos per Sprachaufzeichnung zu kommentieren. Ihre eigentliche Aufgabe war es jedoch, möglichst lange Audiomitschnitte an einen Server im Netz zu übertragen, ohne dass der Nutzer etwas davon mitbekommt.

Als die App auf dem iPhone aktiv war und die Aufzeichnung lief, signalisierte ein gelber Punkt in der Statusleiste den Zugriff aufs Mikro. Es handelt sich um den mit iOS 14 eingeführten Privacy Indicator. Beim Wechsel zu einer anderen App lief die Aufnahme zwar im Hintergrund weiter, das Betriebssystem verstärkte jedoch seine Warnung und machte durch ein rot hinterlegtes Mikrofonsymbol auf den Zugriff aufmerksam. Wurde das Handy gesperrt, stoppte die Aufzeichnung. Ein heimliches Mitlauschen war nicht möglich.

Display aus, Mikro an

Bei dem Android-11-Smartphone kam das BR-Team ein gutes Stück weiter: Die Test-App zeichnete sogar dann noch Gespräche auf, als das Display ausgeschaltet war. Dazu war ein Kniff nötig, wie Rebecca Ciesielski gegenüber c't berichtet: „Wir sind darauf gekommen, dass App-Entwickler bei Android einen einfachen Trick verwenden können, um sehr lange – mindestens eine Stunde lang – unbemerkt zuzuhören. Dafür müssen sie nur eine Benachrichtigung einblenden."

Durch eine solche Benachrichtigung würde der Lauschangriff mit hoher Wahrscheinlichkeit auffliegen. Doch auch dafür fand das Team eine Lösung: „Die Benachrichtigung kann problemlos so programmiert werden, dass sie nur angezeigt wird, wenn der Bildschirm aus ist, die Nutzer sie also nicht sehen können. Sobald jemand den Bildschirm anschaltet, verschwindet auch die Nachricht", erklärt Ciesielski. Dann lauscht die App zwar nur, wenn das Smartphone nicht genutzt wird, aber dann entstehen ja ohnehin die interessantesten Gespräche.

Während die Android-App genutzt wird, sind solche Tricks nicht nötig: Hat der Nutzer den Zugriff aufs Mikrofon gewährt, kann es die aktive App jederzeit benutzen. Einen visuellen Indikator gibt es bis einschließlich Android 11 nicht. Erst mit Android 12 zieht Google mit Apple

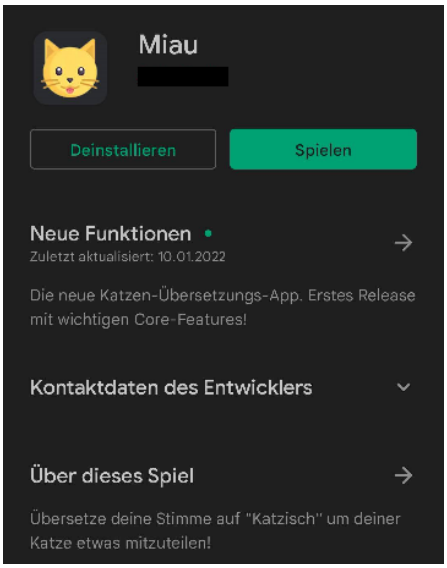

Bild: BR

Das BR-Team entwickelte eine Test-App, die Gespräche bei ausgeschaltetem Display belauschen kann. Die App schafft es sogar in den Play Store.

© Copyright by Heise Medien.
Persönliches PDF für alle Leser der c't aus 30625 Hannover

gleich und zeigt einen farbigen Punkt in der oberen rechten Bildschirmecke an.

Auf Nachfrage des BR erklärte Google, wer sensible Daten missbraucht und gegen die App-Richtlinien verstößt, werde blockiert. Doch verhindern Googles Kontrollen, dass Lausch-Apps im Play Store landen? Um das herauszufinden, probierte das BR-Team, die zu Versuchszwecken erstellte Spionage-App bei Google Play einzustellen. Das gelang auf Anhieb, woraufhin die Journalisten die App sofort wieder entfernten.

Bild: BR / PULS Reportage

Eine weitere Test-App zeigte, dass sich Gesprächsinhalte prinzipiell auch über den Beschleunigungssensor erfassen lassen.

Verräterische Schwingungen

Gesprächsinhalte lassen sich jedoch nicht nur über die Mikrofone belauschen. Beispielsweise demonstrierten US-Forscher, dass auch die in Smartphones verbauten Beschleunigungssensoren (Accelerometer) mitunter so sensibel sind, dass sie auch akustische Schwingungen erfassen, ähnlich wie ein Mikro (siehe ct.de/ycmg).

Tests des BR-Teams zeigten, dass Gespräche im Raum zwar nicht zu nennenswerten Schwingungen führen, sehr wohl aber Telefonate, die über die Freisprechfunktion des Android-Smartphones geführt wurden.

Die US-Forscher gingen noch weiter: Mit einem KI-Modell gelang es ihnen, einzelne Wörter und Ziffern in den Sensordaten zu identifizieren. Solche Angriffe bezeichnet man als Seitenkanalattacken (Sidechannel attack). Sie sind besonders problematisch, weil sie vorhandene Schutzkonzepte häufig umgehen: Während der Zugriff aufs Mikro durch das Betriebssystem geschützt ist, können Apps meist uneingeschränkt auf Sensoren zugreifen.

Vertraulichkeit des Wortes

Doch die Apps der großen Internetkonzerne sind weltweit milliardenfach installiert – und stehen somit unter enorm großer Beobachtung. Sollte nur einer der Nutzer eine App nachweisbar auf frischer Tat beim Mithören ertappen, dann hätte der App-Anbieter große Schwierigkeiten.

Dies hätte auch juristische Konsequenzen. Zum Beispiel ist das gesprochene Wort laut § 201 StGB hierzulande besonders geschützt („Verletzung der Vertraulichkeit des Wortes“). Wer unbefugt das nichtöffentlich gesprochene Wort aufnimmt, kann mit bis zu drei Jahren Haft oder einer Geldstrafe rechnen.

Unbestritten ist jedoch, dass Werbeanzeigen und News-Vorschläge bei Google, Facebook & Co. schon mal Themen treffen, über die man sich Minuten zuvor noch unter vier Augen unterhalten hat. Wie wäre das möglich, ohne den Nutzer dauerhaft zu belauschen?

Das BR-Team liefert hierzu Theorien: Eine davon sind „Ad Targeting Groups“, also Werbezielgruppen mit Nutzern, die ähnliche Interessen haben. Wenn ein Gruppenmitglied nach einem bestimmten Produkt sucht, ist die Wahrscheinlichkeit hoch, dass sich auch die anderen Mitglieder dafür interessieren.

Daten, überall Daten

Eine weitere Theorie ist die Auswertung standortbezogener Daten wie GPS-Koordinaten oder WLAN- und Bluetooth-Geräten in Reichweite. Halten sich zwei Nutzer längere Zeit am gleichen Ort auf, kann es für Unternehmen sinnvoll sein, Nutzer B die Produkte anzuzeigen, nach denen Nutzer A zu dieser Zeit gesucht hat. Durch weitere Metadaten, etwa Verbindungsdaten von WhatsApp-Calls, ließe sich dieses Prinzip ausbauen.

Nicht zu unterschätzen sind auch die Datenschätze, die man Facebook, Google & Co. frei Haus liefert: Wer sich nicht schützt, dem schauen die Werbefirmen beim Surfen fast kontinuierlich durch Third-Party-Tracking über die Schulter. Mit all diesen Daten entsteht ein digitaler Zwilling auf den Servern der Werbeindustrie, der ein paar Tage in der Zukunft lebt und schon heute weiß, wofür sich der Nutzer übermorgen interessieren könnte.

Kognitive Verzerrung

Einen Beitrag zur Erklärung des Phänomens könnte auch ein psychologischer Effekt leisten: Sobald man sich für eine bestimmte Sache interessiert, begegnet man ihr plötzlich überall. Ein simples Beispiel: Wer beschließt, ein rotes Fahrrad zu kaufen, dem fallen plötzlich an jeder Straßenecke rote Fahrräder auf.

Diese kognitive Verzerrung wird als Frequenzillusion bezeichnet. Übertragen auf Onlinewerbung würde das bedeuten, dass man Werbung, die gerade nicht interessant ist, kaum zur Kenntnis nimmt, Werbung zu Themen, mit denen man sich jüngst beschäftigt hat, dafür umso mehr.

Fazit

Die BR-Experimente zeigen, dass es technisch durchaus möglich ist, dass Smartphone-Apps unter bestimmten Voraussetzungen Gespräche belauschen – und das sogar heimlich. Dass die Internetriesen tatsächlich davon Gebrauch machen, um passende Werbung auszuspielen, ist allerdings weiterhin nicht belegt. Es ist auch nicht wahrscheinlich, denn auf Gesprächsmitschnitte sind die Konzerne nicht angewiesen. Nutzer liefern eh schon allerhand Daten an, die auf die individuellen Interessen schließen lassen.

Wer verhindern möchte, dass Werbefirmen zielsicher die persönlichen Vorlieben erraten, muss seinen digitalen Fußabdruck reduzieren: Dazu zählt nicht nur, die von Apps eingeforderten Zugriffsrechte skeptisch zu hinterfragen und nur gezielt zuzustimmen, sondern auch Metadaten und Tracking-Surfspuren möglichst zu vermeiden. *(rei@ct.de)* c't

BR-Bericht: ***ct.de/ycmg***

© Copyright by Heise Medien.
Persönliches PDF für alle Leser der c't aus 30625 Hannover