Manche App zur Kindersicherung gefährdet die Privatsphäre der Kinder

geschrieben von Redakteur | März 14, 2025

Bis zu 80 Prozent der Eltern verwenden Apps, um die Sicherheit und Privatsphäre ihrer Kinder zu schützen

Bis zu 80 Prozent der Eltern verwenden Apps, um die Sicherheit und Privatsphäre ihrer Kinder zu schützen. Die Apps bieten verschiedene Funktionen: von der Beschränkung der Online-Zeit der Kinder und der Inhalte, die sie sehen können, bis hin zur Aktivitätsüberwachung und Standortverfolgung.

Eine Studie hat nun „offizielle“ Apps zur Kindersicherung, die im Google Play Store verfügbar sind, mit „sideloaded“ oder „inoffiziellen“ Apps zur Kindersicherung verglichen, die aus anderen Quellen erhältlich sind.

Die Studie verglich 20 sideloaded Apps zur Kindersicherung mit 20 aus dem Google Play Store und untersuchte dabei Datenschutzrichtlinien, Android-Package-Kit-Dateien (die zum Verteilen und Installieren von Android-Apps verwendet werden),

Anwendungsverhalten, Netzwerkverkehr und Funktionen.

Heimliches Ausspionieren

Das Team stellte fest, dass sideloaded Apps ihre Präsenz vor den Telefonbenutzer*innen eher verbergen – eine Vorgehensweise, die bei offiziellen Store-Apps verboten ist. Sie erforderten auch übermäßige Berechtigungen – Regeln, die festlegen, worauf Apps auf dem Telefon zugreifen können, darunter „gefährliche“ Berechtigungen wie den jederzeitigen Zugriff auf persönliche Daten, wie zum Beispiel den genauen Standort.

Darüber hinaus übertrugen drei sideloaded Apps vertrauliche Daten unverschlüsselt. Die Hälfte hatte keine Datenschutzrichtlinie. Acht von 20 Apps wurden als potenzielle Stalkerware identifiziert.

Schmaler Grad zwischen Schutz und Überwachung

Leonie Tanczer, leitende Autorin der Studie von der UCL: „Apps zur Kindersicherung sind ein beliebtes Mittel, um die Sicherheit von Kindern online und persönlich zu gewährleisten, und können nützliche Werkzeuge für Eltern sein, um die Gefahren zu meistern, denen Kinder in der heutigen Welt ausgesetzt sind. Aber die Ergebnisse unserer Studie zeigen, dass viele sideloaded Apps ernsthafte Probleme in Bezug auf Datenschutz, Zustimmung und sogar Sicherheit haben. Wenn eine App beispielsweise versucht, ihre Präsenz auf dem Gerät zu verbergen, ist das nichts anderes als Stalkerware. Sobald man beginnt, die Sicherheitsvorkehrungen zu entfernen, die offizielle Store-Apps haben müssen, ist es ein schmaler Grat zwischen legitimer Nutzung und unethischer Überwachung oder in extremen Fällen häuslicher Gewalt.“

Heimliche Screenshots und Abhören von Anrufen

Die Forscher*innen beobachteten mehrere besorgniserregende Verhaltensweisen von sideloaded Apps zur Kindersicherung, die ihrer Meinung nach für Apps, die als Kindersicherheitstools vermarktet werden, ungeeignet sind. Beispielsweise enthielten die Apps Funktionen zum Abfangen von Nachrichten von Dating-Apps wie Tinder.

Viele sideloaded Apps enthielten auch die Möglichkeit, Screenshots aus der Ferne zu machen, Anrufprotokolle anzuzeigen, Nachrichten zu lesen und sogar Anrufe abzuhören.

Die Forscher*innen stellten fest, dass Entwickler*innen aufgrund einer Gegenreaktion auf Apps, die beispielsweise zum Erwischen untreuer Ehepartner*innen vermarktet werden, stattdessen dazu übergegangen sind, Apps als Tools zur Kindersicherung zu vermarkten.

Fehlende Einwilligung der Kinder

Eva-Maria Maier, Erstautorin der Studie, die die Arbeiten im Rahmen ihrer Abschlussarbeit im Studiengang IT Security an der FH St. Pölten verfasst hat, sagt dazu: „Das Hauptproblem bei der umfangreichen Funktionalität dieser inoffiziellen Apps ist die Einwilligung. Wenn Eltern eine offene, transparente Beziehung zu ihrem Kind haben, sollten sie diese Apps nicht auf dem Telefon ihres Kindes verstecken oder auf so viele private Informationen zugreifen müssen. Das wirft ernsthafte Fragen darüber auf, ob Kinder wissen, wie sie verfolgt werden und wie sich dies auf ihre Privatsphäre und Rechte auswirkt. Auch wenn Eltern glauben, dass ihnen das Wohl ihres Kindes am Herzen liegt, birgt das Sammeln so vieler persönlicher Informationen Risiken, da es häufig zu Massendatenlecks kommt.“

Datenleak von Überwachungsapp

Im Jahr 2015 wurde der Entwickler der mSpy-App gehackt und zehntausende Kundendatensätze wurden online geleakt, darunter auch die persönlichen Daten von Kindern. Im Jahr 2024 wurden Kundendienstunterlagen von mSpy online geleakt, was Aufschluss darüber gab, wie Kund*innen die Apps nutzten, darunter das Ausspionieren von Partner*innen, die des Fremdgehens verdächtigt wurden. mSpy ist eine sideloaded App und wird derzeit als Überwachungssoftware für Eltern vermarktet.

Lukas Daniel Klausner, Forscher am Institut für IT-Sicherheitsforschung der FH St. Pölten: „Die Rechte von Kindern sind von Land zu Land unterschiedlich, aber in der Europäischen Union müssen Kinder unter 16 Jahren nicht ihre Zustimmung geben, wenn ein Elternteil eine Kindersicherungs-App auf ihrem Gerät installiert. Obwohl Kinder über 16 Jahren ihre Zustimmung geben müssen, sind es in Wirklichkeit oft die Eltern, die Geräte und Apps kaufen und einrichten. Daher vermute ich, dass die Zustimmung nicht immer erteilt wird. Diese Situation bedeutet auch, dass Kinder häufig keinen Zugriff auf ihre von Überwachungs-Apps gesammelten Daten und keine Autonomie darüber haben. Diese Apps und viele Aspekte der Online-Kultur sind relativ neu – es sind keine Probleme, mit denen sich Eltern vor einer Generation herumschlagen mussten. Ich denke, es besteht dringender Bedarf an einer öffentlichen Diskussion über die Verfügbarkeit dieser Apps, wie sie verwendet werden und wie sie aus ethischer Sicht verwendet werden sollten.“

Studie zum Thema

Eva-Maria Maier et al. „Surveillance Disguised as Protection: A Comparative Analysis of Sideloaded and In-Store Parental Control Apps“, Proceedings on Privacy Enhancing Technologies.

https://petsymposium.org/popets/2025/popets-2025-0052.php

https://doi.org/10.56553/popets-2025-0052

Über die FH St. Pölten – University of Applied Sciences

Die Fachhochschule St. Pölten steht für angewandte Forschung und internationale Vernetzung. Knapp 4.000 Studierende erhalten in zahlreichen Bachelor- und Master-Studiengängen sowie berufsbegleitenden Weiterbildungsprogrammen eine praxisorientierte Ausbildung in den Themenbereichen Medien, Kommunikation, Management, Digitale Technologien, Informatik & KI, Security, Bahntechnologie, Gesundheit und Soziales. Lehre und Forschung sind dabei eng verzahnt: Als forschungsstarke Hochschule kooperiert die FH St. Pölten mit nationalen und internationalen Partner*innen in anwendungsbezogenen Projekten. Zudem leitet sie die europäische Hochschulallianz E³UDRES² (Engaged and Entrepreneurial European University as Driver for European Smart and Sustainable Regions) und entwickelt zusammen mit Hochschulen aus neun Partnerländern zukunftsweisende Konzepte für die Hochschule der Zukunft sowie für smarte und nachhaltige europäische Regionen.

Mag. Mark Hammer, Fachhochschule St. Pölten