Einige Kita-Apps können Eltern und Kinder ausspionieren

geschrieben von Redakteur | Juli 10, 2022

Studie der Ruhr-Universität-Bochum: Einige Apps weisen gravierende Sicherheitsmängel auf

Kita-Apps sollen den Alltag in Kindertagesstätten erleichtern. Eltern können darüber beispielsweise Berichte über die Entwicklung ihres Kindes abrufen oder mit Erzieherinnen und Erziehern kommunizieren. Einige von diesen Anwendungen weisen jedoch gravierende Sicherheitsmängel auf. Zu diesem Schluss kommen Forschende der Ruhr-Universität Bochum (RUB), der Westfälischen Hochschule und des Bochumer Max-Planck-Instituts für Sicherheit und Privatsphäre gemeinsam mit einem Industriepartner. Sie analysierten 42 Kita-Apps aus Europa und den USA im Hinblick auf Sicherheit und Datenschutz.

Bei einigen Apps konnten sie auf private Fotos der Kinder zugreifen; mehrere Anwendungen griffen ohne Einverständnis persönliche Daten von Nutzern ab und teilten diese mit Drittanbietern.

Die Ergebnisse stellt das Team um Dr. Matteo Große-Kampmann,

der am Horst-Görtz-Institut für IT-Sicherheit der RUB promovierte, und Dr. Maximilian Golla vom Max-Planck-Institut für Sicherheit und Privatsphäre im Juli 2022 in Sydney auf dem „22nd Privacy Enhancing Technologies Symposium“ vor, welche als wichtigste Konferenz im Bereich der Privacy-Forschung gilt. Die Ergebnisse sind vorab online veröffentlicht.

„Laut der europäischen Datenschutzgrundverordnung und dem US-amerikanischen Children’s Online Privacy Protection Act unterliegen Daten von Kindern einem besonderen Schutz“, sagt Maximilian Golla. „Leider mussten wir feststellen, dass viele Apps diesen Schutz nicht gewährleisten können.“

Die Analysen erfolgten in Kooperation mit der AWARE7 GmbH. Das Team kontaktierte alle App-Hersteller vor der Veröffentlichung und machte sie auf die Schwachstellen aufmerksam.

Millionenfache Nutzung

Für die Studie analysierten die Forscher Android-Kita-Apps, die sie im Google Play Store finden konnten und die mindestens folgende Funktionen besitzen: Die Entwicklung der Kinder sowie besondere Aktivitäten können in Form von Notizen, Fotos und Videos in der App festgehalten werden; die App besitzt eine Messenger-Funktion, über die das Kita-Personal mit den Eltern kommunizieren kann; die App unterstützt das Kita-Management bei administrativen Prozessen wie der Rechnungsstellung, dem Erstellen von Zeitplänen oder der Gruppenorganisation. Die am weitesten verbreiteten Apps „Bloomz“ und „brightwheel“ wurden bereits mehr als eine Million Mal aus dem Google Play Store heruntergeladen. Alle Apps zusammengenommen kamen auf etwa drei Millionen Downloads.

Originalpublikation:

> *Moritz Gruber, Christian Höfig, Maximilian Golla, Tobias Urban, Matteo Große-Kampmann. "We may share the number of diaper changes": A privacy and security analysis of mobile child care applications, 22nd Privacy Enhancing Technologies Symposium, 2022, Sydney, Australien, Online-Veröffentlichung: https://petsymposium.org/2022/files/papers/issue3/popets-2022-0078.pdf*
>
> *Auf den Seiten 402 und 405 steht dann auch,*
> *um welche Apps es sich handelt.*

Persönliche Daten werden teils verkauft

Von den untersuchten Apps wiesen acht gravierende Sicherheitsprobleme auf, die es Angreiferinnen und Angreifern beispielsweise ermöglichen würden, private Fotos der Kinder einzusehen. Bei 40 Apps stellten die Forscher fest, dass sie die Eltern sowie Erzieherinnen und Erzieher beobachten: Sie sammeln die Telefonnummer und E-Mail-Adresse der Nutzerin oder des Nutzers sowie Informationen zum verwendeten Gerät und zur Verwendung der App, etwa wann auf welchen Button geklickt wurde. Diese und andere Informationen teilen und verkaufen die Hersteller an Drittanbieter. So schreibt ein App-Entwickler: „… Daten zu Geschäftszwecken an Partner weitergeben, z. B. die durchschnittliche Anzahl der Windelwechsel pro Tag …". Häufig werden die Daten an Amazon, Facebook, Google oder Microsoft für gezielte Werbekampagnen weitergegeben.

Mangelhafte Datenschutzerklärungen

„Wir haben uns auch die Datenschutzerklärungen der Anbieter angesehen“, erklärt Maximilian Golla. „Dabei ergab sich ein erschreckendes Bild. Viele der Erklärungen haben noch nicht einmal erwähnt, dass sie Daten von Kindern verarbeiten, geschweige denn, dass sie Daten sammeln und verkaufen, obwohl sie das nach den gesetzlichen Vorschriften Europas und der USA müssten.“

Dahinter müssen jedoch nicht unbedingt böse Absichten stecken. „Wir vermuten, dass es sich um technische und organisatorische Probleme handelt“, so Matteo Große-Kampmann. Laut Angaben der Forscher handeln manche Anbieter fahrlässig, weil die verlinkte Datenschutzerklärung nicht konform ist, unter anderem weil sie keine Angaben über die Datenverarbeitung in der App oder über die angebotenen Dienstleistungen enthält und häufig seit vielen Jahren nicht mehr angepasst wurde.

Gerade weil es um die Daten von Kindern geht, erhoffen sich die Forschenden mit ihrer Arbeit auf dieses sensible Thema aufmerksam machen zu können. „Kita-Verantwortliche, Kita-Träger und Eltern können natürlich nicht selbst jede App analysieren“, sagt Matteo Große-Kampmann. „Aber am Ende des Tages müssen sie die die Verantwortung für die Entscheidung tragen, welche App eingeführt wird.“

Richtlinien und Checklisten wären sinnvoll

Sich Kita-Apps grundsätzlich zu verweigern, stellt laut Maximilian Golla keine praktikable Lösung dar, gerade weil es auch Anbieter ohne Sicherheitsprobleme gibt, die datenschutzkonform agieren. „Wenn es keine offizielle App gibt, dann nutzen die Eltern eben Messenger-Dienste wie WhatsApp, was gerade aus Datenschutzsicht die schlechteste

aller Lösungen darstellt”, sagt er. Sinnvoll wäre es laut den IT-Experten daher, wenn Fachleute Richtlinien und Checklisten erstellen würden. So könnten beispielsweise staatlich verantwortliche Stellen Empfehlungen aussprechen und an die Trägervereine der Kitas weitergeben.

Förderung

Die Arbeiten fanden im Rahmen des Exzellenzcluster CASA – Cyber-Sicherheit im Zeitalter großskaliger Angreifer statt, gefördert von der Deutschen Forschungsgemeinschaft (EXC 2092 – 390781972).

Dr. Julia Weiler/Dezernat Hochschulkommunikation/Ruhr Universität Bochum