Stopp Corona App

Eine Ersteinschätzung
Wien, 27.03.2020

Stopp Corona App checked by security researchers

Experten von SBA Research analysieren mittels Reverse Engineering die Android Version der Stopp Corona-App des Roten Kreuzes auf Datensicherheit.

Technisches Statement

Bei dem nachfolgenden Statement handelt es sich um eine Ersteinschätzung der Stopp Corona App (Stand 25. März 2020, Version 1.0.0.6-QA_205, Play Store Link) des Roten Kreuzes, welche im Rahmen eines Quick-Checks von den Sicherheitsforschern Christian Kudera, Manuel Leithner und Georg Merzdovnik (SBA Research) analysiert wurde. Eine Analyse in so einem kurzen Zeitraum ersetzt keine vollständige Sicherheitsanalyse und die angeführten Resultate sind als vorläufig zu betrachten. Des Weiteren wurde nur die Funktionalität betrachtet, die in der analysierten Version für den Anwender zur Verfügung stand. Auf etwaige geplante Änderungen in der Funktionalität (z.B. automatisierter digitaler Handshake bei Begegnungen) wird nicht eingegangen.

Aus Sicht des Benutzers stellt sich vor allem die Frage, welche persönliche Daten die App weitergibt, und ob die Aussagen des Roten Kreuzes in den FAQ zur Apps mit den technischen Gegebenheiten übereinstimmen. Die App beinhaltet in der betrachteten Version die Funktionalitäten "Digitaler Handshake", "Gespeicherte Begegnungen", "Corona-Infektion melden" und "Benachrichtigung im Krankheitsfall".

Im Rahmen des digitalen Handshakes werden unmittelbar keine kritischen persönlichen Daten an das Rote Kreuz, Google oder einen Drittanbieter gesendet. Allerdings wird eine Benutzerkennung (UUID - anonyme Nummer die bei der ersten Inbetriebnahme der App erstellt wird und keinen Rückschluss auf den Benutzer zulässt) an den Server des Roten Kreuzes übermittelt. Solange diese UUID nicht mit persönlichen Daten verknüpft werden kann, stellt dies kein Problem dar und der digitale Handshake erfolgt, wie vom Roten Kreuz beschrieben, anonym. Allerdings wird zusätzlich zum Handshake auch von jedem Partner dessen eigene UUID mit einem Timestamp versehen an das Rote Kreuz übermittelt. Während dies technisch gesehen zwar nicht im direkten Widerspruch mit der Datenschutzvereinbarung zu stehen scheint, könnten so trotzdem im Hintergrund die Daten anhand der Zeitstempel korreliert, und so Handshake-Partner miteinander verknüpft werden. Dies sollte weiter kritisch beobachtet werden, da diese Funktionalität zur Erbringung der Leistung der App aus gegenwärtiger Sicht nicht notwendig erscheint. Die Sinnhaftigkeit des manuellen digitalen Handshakes ist außerhalb des Scopes dieser technischen Einschätzung und wird aus diesem Grund nicht näher betrachtet. Die Funktion "Gespeicherte Begegnungen" ist aus technischer Sicht unbedenklich.

Die Funktion "Corona-Infektion melden" ist aus Datenschutzperspektive nicht unbedenklich, da im Rahmen der Meldung die Mobilnummer des Benutzers an den Server des Roten Kreuzes übermittelt wird. Die Benutzerkennung (UUID) wird dabei zwar nicht übertragen; die Benachrichtigung im Rahmen der Funktion "Digitaler Handshake" beinhaltet jedoch potentiell Informationen über den Zeitpunkt einer solchen Meldung. Somit können theoretisch die Benutzerkennung (UUID) und die Mobilnummer miteinander verknüpft werden. Ob das Rote Kreuz die Mobilnummer serverseitig weiterverarbeitet (z.B. längerfristig

speichert) kann aus technischer Sicht nicht eingeschätzt werden. Laut der vom Roten Kreuz veröffentlichten Mobilnummer serverseitig weiterverarbeitet (z.B. längerfristig speichert) kann aus technischer Sicht nicht eingeschätzt werden. Laut der vom Roten Kreuz veröffentlichten Datenschutzinformation (Kapitel 2.3, Version 1.1 vom 24.03.2020) wird die Mobilnummer einerseits für die Kontaktierung bei allfälligen notwendigen Hilfeleistungen und andererseits für die Aufklärung einer rechtswidrigen bzw. bei einer missbräuchlichen Nutzung der App oder für die Rechtsverfolgung gespeichert. Die Analyse hat gezeigt, dass Mobilnummern an andere Nutzer und Nutzerinnen der App nicht weitergeleitet werden. Es kann keine allgemein gültige Empfehlung gegeben werden, ob ein Anwender es billigen soll, dass seine Mobilnummer übermittelt wird und jeder Anwender muss selbst entscheiden ob er diese Übermittlung in Kauf nimmt. Bei der "Benachrichtigung im Krankheitsfall" Funktionalität werden, wie vom Roten Kreuz versichert, nur anonyme Daten versendet bzw. empfangen.

Zusammenfassend kann mit dem derzeitigen Wissensstand gesagt werden, dass das Rote Kreuz bei der Entwicklung der App einen Fokus auf das Recht der Privatsphäre gelegt hat und die App keine Datenkrake darstellt, wenn auch die Sammlung der Handshakes aus momentaner Sicht eine für die Funktionalität unnötige Datensammlung darzustellen scheint. Benötigte Berechtigungen und übermittelte personenbezogene Daten (z.B. Mobilnummer) werden offen in den Datenschutzinformation dargelegt. Die Übertragung der personenbezogenen Daten birgt zwar grundsätzlich das Potential für weitergehende Analysen (z.B. von sozialen Kontakten zwischen anonymen Benutzern), ist aber im Rahmen der beschriebenen Verarbeitung gerechtfertigt.

Nachfolgend werden die vier Funktionalitäten detailliert erläutert. Zusätzlich wird die Weitergabe von persönlichen Daten analysiert.

Digitaler Handshake

Für den digitalen Handshake müssen mindestens zwei Benutzer die Funktion "Digitaler Handshake" auswählen. Sobald diese Funktion aktiviert ist, sendet das Smartphone einerseits Informationen aus, damit es gefunden werden kann, und sucht andererseits aktiv nach solchen ausgesendeten Informationen von anderen Smartphones. Die App zeigt nach erfolgreicher Suche alle anderen Benutzer in der Nähe an, wobei jedem Benutzer eine vierstellige Nummer zugeteilt wird, welche keine Rückschlüsse auf die Identität zulässt. Die Benutzer müssen sich ihre zugeteilte Nummer abseits der App in einem Gespräch mitteilen und anschließend in der App auswählen, dass sie mit dieser Nummer Kontakt hatten und die Person hinter der Nummer in das persönliche Kontakttagebuch ("Gespeicherte Begegnungen") aufgenommen werden soll. Nach dem erfolgreichen digitalen Handshake wird eine Meldung an einen Server des Roten Kreuzes gesendet, welche die eigene Benutzerkennung (UUID - anonyme Nummer die bei der ersten Inbetriebnahme der App erstellt wird und keinen Rückschluss auf den Benutzer zulässt) und die Uhrzeit des digitalen Handshakes beinhaltet. Die Benutzerkennung des Gegenübers wird nicht vom eigenen Smartphone an einen Server des Roten Kreuzes gesendet. Im Rahmen des digitalen Handshakes wird ein sogenannter öffentlicher Schlüssel (public Key) jedes Benutzers erfasst mit dem ein digitaler Handshake durchgeführt wird. Dies ist aus technischer Sicht begrüßenswert und die technischen Gründe werden in der Sektion "Benachrichtigung im Krankheitsfall" erläutert. Die UUID des Gegenübers wird dabei nicht übertragen.

Technisch wurde der Handshake mit der Programmbibliothek Google Nearby Messages API umgesetzt, welche mittels Bluetooth, WLAN Informationen und dem Mikrofon (Töne im Ultraschallbereich, welche für den Menschen nicht hörbar sind) nach anderen Smartphones sucht und Nachrichten austauscht. Bei der ersten Verwendung des digitalen Handshakes benötigt die App die Freigabe zur Verwendung von "Nearby" und informiert den Benutzer mittels der Meldung "Nearby" verwendet den Standort, das Mikrofon und Bluetooth" über die Auswirkungen der Berechtigung. Im Rahmen der Analyse der App konnte keine

Aufzeichnung des Standorts durch das Rote Kreuz festgestellt werden. ~~Nearby benötigt für die Kommunikation zwischen Android-Geräten keine Internetverbindung und überträgt dabei keine Daten an Google. Für die Kommunikation mit einer (aktuell noch nicht verfügbaren) Version der App für iPhones wäre ein Datenaustausch mit Google als "Vermittler" notwendig~~. *Update 16. April 2020: Bei einer erneuten Überprüfung der Version 1.0 haben wir festgestellt, dass ein digitaler Handshake auch zwischen zwei Android-Geräten eine Internetverbindung erfordert.*

Gespeicherte Begegnungen

Die Begegnungen (siehe digitaler Handshake) werden in einer Datenbank gespeichert und können in der App eingesehen werden. Dabei ist das Datum, die Uhrzeit und die jedem Benutzer zugeteilte vierstellige Nummer ersichtlich. Nicht ersichtlich, aber in der Datenbank gespeichert, ist für jeden Benutzer, mit dem ein digitaler Handshake durchgeführt worden ist, ein sogenannter öffentlicher Schlüssel (public Key) des Benutzers. Dieser öffentliche Schlüssel lässt keine Rückschlüsse auf die Identität zu.

Corona-Infektion melden

Der Benutzer kann melden, dass bei ihm eine Corona-Infektion festgestellt wurde, wodurch seine Kontakte der letzten Begegnungen benachrichtigt werden. Dazu muss in einem ersten Schritt ein TAN über die persönliche Telefonnummer angefordert werden, welcher per SMS zugestellt wird. Das Rote Kreuz schreibt dazu, dass die Mobilnummer des Benutzers mittels TAN validiert wird, damit ein Missbrauch der Corona-Infektion melden Funktion vermieden werden kann. Nach der erfolgreichen Eingabe des TAN wird dem Benutzer ein Informationstext angezeigt. Einerseits wird der Benutzer informiert, dass im Fall der Zustimmung jene Kontakte, mit denen in den letzten 48 Stunden ein digitaler Handshake durchgeführt wurde, anonym benachrichtigt werden. Andererseits wird nochmals versichert, dass keine persönlichen Daten an Dritte weitergegeben werden. Der Benutzer muss bestätigen, dass er die Angaben wahrheitsgemäß tätigt und kann danach die Infektion melden.

Aus technischer Sicht kommt es im Rahmen der "Corona-Infektion melden" Funktionalität zu zwei Anfragen (Requests) an den Server des Roten Kreuzes. In der ersten Anfrage wird dem Server die vom Benutzer in einem Textfeld eingegebene Mobilnummer gesendet, wodurch vom Roten Kreuz eine SMS mit einem TAN an diese Nummer gesendet wird. Die zweite Anfrage erfolgt nach der Meldung der Infektion. In dieser Meldung ist der TAN, die Mobilnummer und eine Summe von Nachrichten enthalten. Die Summe von Nachrichten besteht aus je einer Nachricht für jede Person, mit der ein digitaler Handshake durchgeführt wurde. Die jeweilige Nachricht wird mit dem öffentlichen Schlüssel (public Key) des Empfängers verschlüsselt und kann somit nur vom Empfänger und von keinem Anderen gelesen werden. Aus Datenschutzperspektive betrachtet, handelt es sich bei einer Mobilnummer um personenbezogene Daten. Die Übermittlung an den Server des Roten Kreuzes im Zusammenhang mit der Meldung der Corona-Infektion erlaubt aus technischer Sicht eine Deanonymisierung, sofern die Mobilnummer öffentlich ist. Allerdings wird die Mobilnummer nicht an andere Benutzer der App weiterversendet (siehe Benachrichtigung im Krankheitsfall). Die Abwägung ob ein Anwender der App es billigt, dass seine Mobilnummer übermittelt wird, ist jedem selbst überlassen. Hier kann keine Empfehlung abgegeben werden.

Benachrichtigung im Krankheitsfall

Die App kommuniziert regelmäßig mit dem Server des Roten Kreuzes und fragt eine Liste der Meldungen von Corona-Infektionen ab. Die Liste der Meldungen enthält keine personenbezogenen Daten, sondern ausschließlich eine fortlaufende Nummer sowie eine Nachricht. Der Inhalt der Nachricht ist nicht gänzlich geklärt; der aktuelle Stand der Analyse legt jedoch nahe, dass es sich hierbei um eine verschlüsselte Meldung handelt, welche nur von den Kontakten der betroffenen Person entschlüsselt werden kann und Informationen über den Zeitpunkt des digitalen Handshakes beinhaltet. Somit werden bei der

Benachrichtigung im Krankheitsfall wie vom Roten Kreuz versichert nur anonyme Daten versendet bzw. empfangen, wobei jedoch durch den Zeitpunkt des Handshakes potentiell Rückschlüsse auf den individuellen Kontakt möglich sind.

Zusätzlich zu der bisher beschriebenen Funktionalität abonniert die App Push-Benachrichtigungen mittels des Dienstes Google Firebase. Dadurch können auf dem Smartphone Nachrichten empfangen werden, welche durch das Rote Kreuz veranlasst werden können. Dieser Dienst wird in vielen Apps verwendet und ist aus technischer Sicht unbedenklich. Allerdings konnte im Rahmen der Analyse keine Push-Benachrichtigung betrachtet werden und somit ist die Verwendung von Google Firebase momentan nicht vollständig geklärt. Naheliegend ist, dass Apps hiermit über neue Meldungen zu Corona-Infektionen informiert werden.