



CORONA WARN-APP

Eine Veranstaltung der DigitalBotschafter*innen
der Verbandsgemeinde Gau-Algesheim

Die Corona-Warn-App



Ziele der App

- Erkennen von Kontaktketten infizierter Menschen über einen „digitalen Handschlag“.
- Schnellere Unterbrechung von Infektionsketten zur Bekämpfung der COVID-19 Pandemie.
- Nutzung der weit verbreiteten mobilen Geräte zur automatischen Erkennung von Kontakten.

Die Corona-Warn-App ist kein Ersatz für die bestehenden Hygieneregeln wie Mund-Nasen-Schutz oder Abstandsgebote! Die App ist nur eine Ergänzung, ein Instrument, und kann nicht vor einer Infektion schützen.

Ansatz der Bundesregierung

- Freiwilligkeit.
- Datenschutzkonformität.
- Hohes Maß an IT-Sicherheit.
- Auch im Falle einer Infektion: Anonymität.
- Dezentral.
- Interoperabilität.
- Fachliche Beratung durch renommierte Institute für Datenschutz und Datensicherheit.

Funktionsweise

- Die App misst mit Hilfe von Bluetooth den Abstand zwischen Personen (über die Signalstärke) sowie die Dauer dieser Begegnung.
- Sie merkt sich diese Kontakte lokal, indem die Geräte untereinander temporäre, verschlüsselte und anonyme Identitäten austauschen.
- Werden Nutzer der App positiv auf das Coronavirus getestet und melden dies auf freiwilliger Basis über die App, werden ihre Kontakte durch die App informiert, indem die verschlüsselten IDs des Infizierten allen Geräten der App-Nutzer zur Verfügung gestellt werden.
- Die Geräte überprüfen lokal, ob sie mit übermittelten IDs von Infizierten in Kontakt waren. Bei einer Übereinstimmung wird der Nutzer über einen solchen kritischen Kontakt gewarnt.

Tracing statt Tracking

- Bluetooth statt GPS.
- Nutzung der energiefreundlichen BLE-Technik (Bluetooth Low Energy).
- Kein Standort-Tracking durch GPS oder das Funknetz.
- ➡ **Entscheidend ist, ob ein Kontakt stattgefunden hat, nicht wo.**
- So wird kein Bewegungsprofil erstellt.
- Es werden regelmäßig geänderte Zufallscodes als Kennungen (IDs) verwendet. Es gibt keine feste Geräte-Kennung.
- Die App ist sehr datensparsam und dennoch relativ genau.

Dezentral statt Zentral (1)

- Alle Daten (eigene Kennung und Kontakte) bleiben auf dem Gerät des Benutzers.
- Ein positiv getesteter Mensch gibt dies freiwillig in seiner App an. Erst dann findet eine Übertragung seiner Kennung (ID) an einen Zentralserver statt:
 - ohne Personalisierung,
 - ohne Lokalisation.
- Andere Benutzer können nachprüfen, ob sie Kontakt mit einer infizierten Person hatten. Dabei erfahren sie nur, **dass** ein relevanter Kontakt stattgefunden hat.

Dezentral statt Zentral (2)

- Schutz vor Missbrauch (Hacking).
Auf dem Zentralserver liegen nur IDs infizierter Personen vor, keine sonstigen Daten.
- Datenschutzfreundlich: eine Nachverfolgung und De-Anonymisierung wäre sehr aufwendig, wenn nicht unmöglich.
- Insgesamt verfügt die dezentrale Lösung über einen besseren Datenschutz als eine zentrale Lösung (z.B. Frankreich).

Freiwilligkeit statt Zwang

- Es ergeben sich keine Nachteile für Nicht-Nutzer der App.
- Ein Zwang zur Nutzung der App müsste **überwacht** werden.
Eine Nichtnutzung müsste **sanktioniert** werden (Bußgeld).
Das erscheint - auch **juristisch** - völlig unmöglich.
- Praktische Probleme in der Technik (Akku ist leer, die Aktivierung von Bluetooth wurde vergessen, ...) lassen eine Verpflichtung zur Nutzung einer App unmöglich erscheinen.
- Zwänge resultieren immer in Widerstand und damit in einer negativen Reaktion.
- Eine Freiwilligkeit schafft mehr Vertrauen.

Zur Entwicklung

- Der Programmcode der App wird offen gelegt - als „OpenSource“ auf der Plattform GitHub.
- Die Entwickler kommen von SAP und der Deutschen Telekom. Beide Firmen arbeiten im Auftrag der Bundesregierung.
- Google (Android) und Apple (iOS) unterstützen das Projekt durch eine eigene Schnittstelle. Diese ist bereits in den neuesten Updates vorhanden.
(Sonderfall: Huawei)

Technische Voraussetzungen

- Android (ca. 80,9% Marktanteil in D):
 - mindestens Android 6.0 (Marshmallow) (auf ca. 86% der Androids)
 - Google Play Dienste (Google Mobile Services GMS)
- Apple (ca. 18,9% Marktanteil in D):
 - mindestens iOS 13.5 (auf ca. 50% der iPhones und 33% der iPads)
- Huawei Geräte ohne Google Dienste (seit Mai 2019):
 - mindestens HMS Version 4.1 (Huawei Mobile Services)



Einsatz und Nutzen

- Nur eine hohe Zahl von Anwendern der App lässt eine Nutzung sinnvoll erscheinen.
- Nur eine gut gemachte, datenschutzkonforme und sichere App wird zur Erreichung des angestrebten Nutzungsgrades von 60% helfen.
(zum Vergleich: WhatsApp ist auf etwa 69% der deutschen Mobilgeräte installiert.)
- Eine epidemiologische Wirkung zeigt sich erst in der Zukunft (bei hohen Nutzungszahlen).

Offene Fragen

- Was passiert, wenn mit Hilfe der App ein Kontakt mit einem Infizierten festgestellt wird:
 - Hat die betroffene Kontaktperson Anspruch auf einen Test?
 - Muss die Person in Selbstisolation oder zum Arzt?
 - Darf die Person so weiter leben, als wäre nichts passiert?
- Kann ein Missbrauch der App ausgeschlossen werden?
(Prüfung auf Nutzung der App als Voraussetzung für eine Dienstleistung)
- Wie oft kommt es zu einem Fehllarm (in beide Richtungen)?
- ...

Fazit

Jede/r muss für sich selbst
entscheiden,
ob und wie er/sie die App nutzen
möchte.

Vorführung

- Android Dienst für Corona
 - Installation der App
 - Erster Eindruck
- iOS Dienst für Corona
 - Installation der App
 - Erster Eindruck



Ihre Fragen, bitte!



Danke für Ihre Aufmerksamkeit!

Quellennachweis und weiterführende Links

- [Verbraucherzentrale zur CORONA-Warn-App](#)
- [Web-Seminar der Verbraucherzentrale zur CORONA-Warn-App](#)
- [Homepage der CORONA-Warn-App](#)
- [Stellungnahme der Bundesregierung zur Corona-Warn-App](#)
- [Projektbeschreibung zur CORONA-Warn-App](#)
- [GitHub OpenSource Plattform](#)
- [YouTube Videos zur CoronaWarnApp](#)
- [TÜV-IT Prüfung der App](#)
- [Der Bundesbeauftragte für Datenschutz und Informationsfreiheit BfDI](#)
zum Datenschutz während der Pandemie

Alle Informationen dieser Präsentation wurden sorgfältig recherchiert.

Sollten Sie Fehler feststellen oder Sie Fragen zu den Quellen haben, wenden Sie sich bitte an den Autor per eMail unter webmaster@hillschmidt.de.