# Corona-App: "Ein eklatanter Betrug"

29.06.2020 | Originalartikel

*"Der Quellcode bleibt bei Microsoft, das Protokoll wird von Apple und Google implementiert und kontrolliert, der Server wird von Amazon gehostet. Die aktuelle Informationspolitik leidet unter unklaren oder falschen Angaben."*
*(Aus der Analyse von Professor Vaudenay)*

*Während Politik und Medien weiterhin nicht offen kommunizieren, veröffentlicht SPR Auszüge aus der vernichtenden Analyse von EPFL-Informatik-Professor Serge Vaudenay zur Intransparenz und den Sicherheitsrisiken der "dezentralen" Kontaktverfolgung. Die Analyse ist von weltweiter Bedeutung, da das Schweizer Protokoll durch Google und Apple zum globalen Standard wurde.*

***Vorbemerkung SPR**: Die WHO kam in einer Studie von 2019 zu Grippepandemien zum Ergebnis, dass Kontaktverfolgung "unter keinen Umständen zu empfehlen" ist, da epidemiologisch nicht sinnvoll. NSA-Whistleblower Edward Snowden warnte in diesem Zusammenhang, dass Corona als Vorwand benutzt wird, um die Massenüberwachung der Gesellschaft umfassend auszubauen.*

## Analyse von SwissCovid

Prof. Serge Vaudenay, Martin Vuagnoux
5. / 25. Juni 2020

### 1) Aus der Einleitung

*"Die Website des Nationalen Cyber-Security Centers NCSC listet viele Sicherheitsberichte auf, die SwissCovid recht positiv bewerten. Aber sie listet unseren Bericht nicht auf. Stattdessen enthält sie eine "detaillierte Analyse" des NCSC über unseren Bericht. Wir sind mit dieser Analyse nicht einverstanden. Da es ziemlich klar zu sein scheint, dass die Kommunikation nicht transparent ist, legen wir hier unsere Beobachtungen für die Öffentlichkeit dar."*

## 2) Zusammenfassung

"Zusammengefasst lauten unsere Beobachtungen wie folgt:

1. Obwohl der Quellcode der App zur Verfügung steht, können wir sie nicht kompilieren, ausführen und zum Laufen bringen, ohne eine Vereinbarung mit Apple oder Google zu unterzeichnen. Wir finden die App daher nicht kompatibel mit dem Begriff Open Source.
2. Ein grosser Teil des Kontaktverfolgungsprotokolls wird von Apple-Google in einem Teil des Systems namens GAEN implementiert. Dieser Teil hat keinen verfügbaren Quellcode, obwohl das Gesetz die Offenlegung des Quellcodes aller Komponenten des Systems verlangt.
3. Einige Server werden von Amazon als Teil eines externen Dienstes gehostet.
4. Die verfügbaren Informationen für potenzielle Benutzer sind unklar, unvollständig oder falsch.
5. Benutzer können bei der Benutzung von SwissCovid durch Überwachungssysteme Dritter aufgespürt oder identifiziert werden.
6. Diagnostizierte Benutzer, die einen Bericht absenden, haben ein Risiko, von einer Drittpartei identifiziert zu werden.
7. Dritte könnten auf einem Zieltelefon oder auf einer grossen Gruppe von Zieltelefonen falsche Warnungen vor einer möglichen Infizierung eingeben. Dies würde dazu führen, dass Menschen in Quarantäne gehen müssten, ohne wirklich gefährdet zu sein.

Um das Problem zu umgehen, dass GAEN (die Google-Apple-Schnittstelle) keinen verfügbaren Quellcode hat, obwohl das Gesetz für alle Komponenten einen Quellcode vorschreibt, erliess der Bundesrat eine Verordnung, die alle Komponenten aufzählt, aber in der GAEN **nicht** enthalten ist.

Um einen solchen Ausschluss zu rechtfertigen, argumentieren die Promotoren von SwissCovid, dass GAEN Teil des Betriebssystems des Telefons oder Teil der Bluetooth-Schnittstelle des Telefons sei und dass es nicht üblich sei, die Offenlegung des Quellcodes solcher Teile zu verlangen.

Wir bestreiten, dass GAEN ein solcher Teil des Telefons ist, zumindest auf Android-Telefonen. GAEN ist Teil der Google Play Services, die unabhängig vom Betriebssystem und von den Kommunikationsschnittstellen sind. ()

Darüber hinaus ist der grösste Teil des früheren DP3T-Protokolls (zur "dezentralen" Kontaktverfolgung), das in der ursprünglichen Version implementiert war, in der aktuellen Version der Anwendung verschwunden, da ein äquivalentes Protokoll jetzt in GAEN integriert ist.

Wir kommen zu dem Schluss, dass es **keine fundierte technische Rechtfertigung für den Ausschluss von GAEN aus den Komponenten des Systems gibt**. Wir sind der festen Überzeugung, dass die Verordnung ein juristischer Trick ist, um das Gesetz zu umgehen, was die Folge einer Meinungsverschiedenheit zwischen SwissCovid und Apple-Google ist.

Wir fordern Verfassungsexperten auf, eine Beurteilung der Gültigkeit der Verordnung vorzunehmen."

### 3) Zur intransparenten Kontrolle des Tracings durch Google und Apple

Alle Hervorhebungen durch SPR.

- "Wir stellen fest, dass SwissCovid weit davon entfernt ist, Open Source zu sein. **Der Quellcode bleibt bei Microsoft, das Protokoll wird von Apple und Google implementiert und kontrolliert. Der Server wird von Amazon gehostet.** Die aktuelle Informationspolitik leidet unter unklaren oder falschen Angaben."
- "Fast alles, was sensibel ist, wird von der GAEN-API [der Schnittstelle von Google und Apple] behandelt, **die keinen Quellcode zur Verfügung stellt und die wir niemals kompilieren oder analysieren können.**"
- "**Deshalb ist SwissCovid weit davon entfernt, Open Source zu sein.** Im besten Fall ist der Quellcode der grafischen Benutzeroberfläche verfügbar, aber er kann weder die laufende Anwendung reproduzieren noch modifiziert werden."
- "Es gibt einige seltsame Anzeichen in der Beziehung zu Google-Apple. Das DP3T-Projekt [für "dezentrales" Contact-Tracing] bittet seinen Partner Google-Apple in einer Mitteilung, die Schnittstelle wenigstens für externe Audits zu öffnen und ihre Implementierung zu aktualisieren. **Dies lässt uns vermuten, dass DP3T die Kontrolle über SwissCovid verloren hat.**"
- "Die aktuelle Beziehung mit Google-Apple bringt SwissCovid in eine seltsame Situation. () **Die Benutzer müssen zustimmen, ihre persönlichen Informationen an Google-Apple weiterzugeben**, während SwissCovid diese nicht verwenden darf. Ebenso ist es der SwissCovid-Applikation verboten, den Standort zu verwenden. Die Google-Play-Services verwenden jedoch Zugriff auf Geräte, Fotos, Standort, Lesezeichen, Kalender, Speicherplatz, Telefon, Mikrofon, Geräte-ID, Kamera, Kontakte, Wi-Fi, Gerätestatus und -verlauf, Identität, SMS und viele andere Privilegien. Da iOS geschlossen ist, könnten wir nichts sagen, aber es wird wohl dasselbe sein."

- "Es gab eine Kontroverse über die Einführung zentralisierter oder dezentralisierter Systeme. Wir können nun sehen, **dass das dezentralisierte DP3T-System zu einem undurchsichtigen System wurde, das bei Google-Apple-Services zentralisiert ist.**"
- "Unabhängig von SwissCovid wird die gleiche Bluetooth-Technologie bereits von Apple und Google zur Ortung von Bluetooth-Geräten verwendet. **Die Nichtverwendung von GPS bedeutet nicht, dass es unmöglich ist, ein Telefon zu orten.**"
- "Da der grösste Teil des Systems von der Google-Apple-Schnittstelle implementiert wird, bleibt von DP3T nicht viel übrig."

**4) Zu den Sicherheitsrisiken**

Auflistung der einzelnen Sicherheitsrisiken im Originalbericht.

- "**Wir haben gezeigt, dass SwissCovid kritische Bedrohungen der Sicherheit und der Privatsphäre schafft.** Egal ob sie reduziert werden oder nicht, so sind wir der Meinung, dass sie auf jeden Fall kommuniziert werden müssen."
- "Noch wichtiger ist, dass die verfügbaren Informationen unzureichend sind, dass es **Falschinformationen über Anonymität und Open Source gibt**, dass es keine öffentlichen Sicherheitstests zu geben scheint, und dass die Entwickler von SwissCovid **an Entscheidungen von Google-Apple gebunden sind**."
- "Uns ist bekannt, **dass bereits mehrere Angriffe empirisch getestet und gemeldet worden sind**. Unser Hauptpunkt ist, **dass freiwillige Nutzer sich dieser Angriffe bewusst sein sollten**. Sie mögen für die meisten von ihnen als geringfügig, für einige jedoch als von entscheidender Bedeutung angesehen werden. **Bislang schweigt die dem Benutzer zur Verfügung gestellte Dokumentation dazu.**"

**5) Zur Umgehung des Tracing-Gesetzes durch den Bundesrat**

- "Das Gesetz vom 19. Juni 2020 besagt, dass alle Komponenten des SwissCovid-Systems über einen öffentlich zugänglichen Quellcode verfügen müssen und überlässt es dem Bundesrat, sich mit den Einzelheiten des Einsatzes zu befassen. Die Verordnung des Bundesrates vom 24. Juni 2020 definiert die Komponenten so, dass sie *ausschliesst*, was von Google-Apple bereitgestellt wird und die DP3T-Funktionalitäten implementiert. **Die Umsetzung von DP3T hat somit das Gesetz umgangen.**"
- "Wir glauben, dass die Verordnung bereits in Vorbereitung war, als Ständerat und Nationalrat über die Notwendigkeit eines öffentlich zugänglichen Quellcodes diskutierten und *unsere Analyse zensiert wurde*.

**Die Bürgerinnen und Bürger und das Parlament sind getäuscht worden**. Mag es aus guten Gründen sein (z.B. um die zweite Welle zu verhindern), **es ist ein eklatanter Betrug**. Unserer Meinung nach hat sich das Gesetz, das geschaffen wurde, um die Menschen davor zu schützen, ein undurchsichtiges System benutzen zu müssen, **5 Tage nach seiner Verabschiedung als unzureichend erwiesen.**"

- "Auf Android ist GAEN Teil der Google Play Services, die die Google-spezifischen Dienste regulieren. () **Dies beweist, dass GAEN weder Teil der Kommunikationstreiber noch Teil des Betriebssystems ist, im Gegensatz zu der üblichen Ausrede für die Nicht-Offenlegung von GAEN, die immer wieder von der Presse verbreitet wird.**"
- "Wir sind überzeugt, dass die rechtliche Definition von "Komponenten" in einer Verordnung **ein Trick ist, um das Gesetz über die Verfügbarkeit von Quellcode zu umgehen."**
- **"Wir fordern unabhängige Rechtsexperten auf, sich zu dieser Kontroverse zu äussern,** um zu bestimmen, ob GAEN als Bestandteil von SwissCovid betrachtet werden soll und deshalb dem Gesetz unterstehen soll, das einen verfügbaren Quellcode verlangt.

*Zum vollständigen Vaudenay-Bericht auf Englisch*