

Überprüfung der Stopp Corona-App: “Unmittelbare Verbesserungen durch Experten-Bericht”

Experten von epicenter.works, noyb.eu und SBA Research evaluieren die Stopp Corona-App des Roten Kreuzes auf Datensicherheit und Datenschutz. Es wurden keine kritischen Sicherheitslücken gefunden, jedoch einiges Verbesserungspotential bei der Umsetzung des Datenschutzes identifiziert.

Viele empfohlene Verbesserungen wurden bereits vom ÖRK umgesetzt. Innerhalb des bestehenden Systems wurden einige dieser Punkte bereits heute implementiert, andere benötigen langfristige Änderungen - auch durch Apple und Google.

Hintergrund zur Prüfung. Das Österreichische Rote Kreuz (ÖRK) und Accenture GmbH haben den Quellcode der Stopp Corona-App (Version 1.1) epicenter.works, noyb.eu und SBA für eine Analyse zur Verfügung gestellt, um die Software im Hinblick auf IT-Security, Datenschutz und rechtliche Aspekte zu analysieren. Die Analyse erfolgte unentgeltlich.

25 Empfehlungen. Experten von epicenter.works, noyb.eu und SBA Research haben die Applikation sicherheitstechnisch und im Hinblick auf Datenschutz überprüft und ihre Erkenntnisse und 25 Empfehlungen in einem Bericht zusammengefasst. Die Ergebnisse wurden in einer Pressekonferenz am 22. April 2020 präsentiert, der vollständige Bericht ist auf den jeweiligen Webseiten der Organisationen abrufbar (epicenter.works, noyb.eu und sba-research.org).

Accenture (die die App für das ÖRK programmieren) hat bereits zugesagt 16 der Empfehlungen mit einem “Hotfix” heute, drei der Empfehlungen mit der nächsten Version der App und vier Empfehlung in etwa vier Wochen umzusetzen.

Dezentrales Konzept. Die App basiert zwar auf einer dezentralen Speicherung der Daten auf dem eigenen Handy - die Kommunikation zwischen den Telefonen passiert aber noch weitestgehend über zentrale Server, da das relevante Bluetooth-Protokoll zu wenig Daten zwischen den Mobiltelefonen übertragen kann.

Thomas Lohninger, Geschäftsführer epicenter.works: *“Inzwischen gibt es mit Konzepten wie DP-3T oder Co-Epi Lösungen, die auch den Großteil der Kommunikation direkt von Handy zu Handy ermöglichen und damit noch datenschutzfreundlicher sind. Wir empfehlen dem ÖRK, sobald das technisch möglich ist, auf dieses Konzept zu wechseln.”* Hierzu ist insbesondere auch eine angekündigte technische Umstellung von Apple und Google notwendig, damit die App auch auf iPhones reibungslos funktioniert.

Technische Prüfung. Grundsätzlich bescheinigen die Fachleute der App im Hinblick auf sicherheitstechnische Aspekte und Fragen des Datenschutzes ein gutes Ausgangsniveau, empfehlen jedoch eine Reihe von Nachbesserungen. Christian Kudera, IT-Sicherheitsexperte SBA Research: *“In der App war eine Statistikfunktion eingebaut, die den Kontaktaustausch über Bluetooth und den Empfang von Infektionsnachrichten an das Rote Kreuz übermittelt hat. Die Statistikfunktion wurde aufgrund unserer dringenden Empfehlung umgehend entfernt.”*

Ein weiteres Problem ist das Offline-Tracking von Geräten. Christian Kudera, IT-Sicherheitsexperte SBA Research: *“Es ist für Angreifer möglich, Smartphones über längere Zeiträume an bestimmten Orten wiederzuerkennen und im Extremfall Bewegungsprofile zu*

erstellen. Uns wurde zugesagt, dass dieses Problem mit einer neuen Version Ende nächster Woche behoben wird.“ Nutzer*innen können als Zwischenlösung den automatischen Handshake deaktivieren.

DSGVO. Das Konzept der App ist auch nach dem europäischen Datenschutzrecht zulässig. Max Schrems, Datenschutzjurist, noyb.eu: *“Das Konzept des Roten Kreuz ist jedenfalls datenschutzkonform. In der doch extrem schnellen Umsetzung kann man aber noch in Details nachbessern. Wir haben noch genauere Informationen empfohlen und mehr Gedanken, wie man sicherstellen kann, dass die Corona-Warnungen auch korrekt sind. Vieles davon wurde sofort umgesetzt.”*

Contact-Tracing-Apps. Contact-Tracing-Apps können im Idealfall Leben retten. Die österreichische “Stopp Corona“-App ist, soweit bekannt, mit 400.000 Installationen bisher Vorreiter in Europa. Gleichzeitig Max Schrems: *“In Europa sind wir jetzt sicher Vorreiter, aber der Stand der Technik ändert sich aktuell fast täglich und das Rote Kreuz muss da sicher weiter dran bleiben.”*

Die heutige Pressekonferenz wurde aufgezeichnet und ist auf den YouTube-Kanälen der Organisationen im Laufe des Vormittags verfügbar.

Rückfragehinweis:

Zum technischen Datenschutz

Thomas Lohninger
Datenschutzexperte

epicenter.works - Plattform
Grundrechtspolitik

team@epicenter.works
Mobil: +43 680 1238611
<https://epicenter.works/>

Zur IT-Security

Christian Kudera
IT-Sicherheitsexperte

SBA Research gGmbH

ckudera@sba-research.org
Mobil: +43 664 4625333
<https://www.sba-research.org/>

Zu rechtlichen Aspekten

Max Schrems & Marco Blocher
Datenschutzexperten

noyb.eu - Europäisches
Zentrum für digitale Rechte

media@noyb.eu
Mobil: +43 660 2678622
<https://noyb.eu>