Bundesamt für Sicherheit in der Informationstechnik, 53175 Bonn

Frau Eva Christiansen (BKamt)
Herr Staatssekretär Dr. Markus Richter (BMI)
Herr Gottfried Ludewig (BMG)

nachrichtlich Herr Andreas Könen (BMI CI)

[redacted]
Bundesamt für Sicherheit in der Informationstechnik

Godesberger Allee 185-189
53175 Bonn

Postanschrift:
Postfach 20 03 63
53133 Bonn

[redacted]

www.bsi.bund.de

DE-Mail-Adresse:
poststelle@bsi-bund.de-mail.de

Betreff: Stellungnahme zur Luca-App

Datum: 12.04.2021

Sehr geehrte Damen und Herren,

das BSI hatte von November 2020 bis Januar 2021 Kontakt zur Entwicklerfirma der Luca-App und in diesem Zusammenhang eine kursorische Bewertung der zur Verfügung gestellten Sicherheitskonzeption der Gesamtanwendung vorgenommen. Entsprechende Verbesserungsvorschläge sind zuletzt im Januar 2021 durch das BSI übermittelt worden.

In den letzten Wochen wurden in unterschiedlichen Medienberichten Zweifel an der IT-Sicherheit der Luca-App geäußert. Neben den Untersuchungen der Eidgenössischen Technischen Hochschule Lausanne und der Radboud-Universität Nijmegen[1] waren dies zuletzt Twitter-Meldungen[2] und Veröffentlichungen des Chaos Computerclubs Freiburg e.V.[3] zum Missbrauch der mTAN-Funktion der Luca-App.

Eine finale Bewertung des Sicherheitsniveaus ist erst nach einem Review der aktuellen Version möglich. Zurzeit wird die Luca-App einem Pentesting durch das BSI unterzogen.

Grundsätzlich unterscheidet sich der zentrale und personalisierte Ansatz der Luca-App aus Sicht des Datenschutzes und der Datensicherheit jedoch deutlich von der in Version 2.0 der Corona-Warn-App implementierten Event-Registration-Funktion.

Stellungnahme

Das BSI möchte aus diesem Grund zu der jetzt für den Einsatz vorgesehenen Version der Luca-App einige grundsätzliche Hinweise geben:

Im Gegensatz zur Corona-Warn-App erhalten Gesundheitsämter im Infektionsfall von einem Event-Ausrichter, der die Luca-App nutzt, den Zugriff auf die Teilnehmerdaten seiner Veranstaltung. Damit wird die bisher geführte schriftliche Kontaktnachverfolgung

[1] Preliminary Analysis of Potential Harms in the Luca TracingSystem, verfügbar unter: https://arxiv.org/pdf/2103.11958.pdf
[2] Tweet von Fr. MdB Domscheit-Berg, verfügbar unter https://twitter.com/anked/status/1380836300199198722
[3] Meldung des CCCFB verfügbar unter: https://wiki.cccfr.de/luca_app_sms-tan

digitalisiert und zu Teilen automatisiert. Dabei muss allerdings beachtet werden, dass die bei der Erst-Nutzung der Luca-App angegebenen personenbezogenen Daten (Name, Vorname, Adresse) nicht verifiziert werden. Die Angabe beliebiger Datensätze ist möglich und die verwendete Telefonnummer ist der einzige Vertrauensanker. Dies ist in der Analogie zu den bisher verwendeten Papierlisten, bei denen ebenfalls in der Praxis keine Überprüfung der gemachten Angaben stattfand, evtl. noch tragbar.

Es muss darauf hingewiesen werden, dass gerade in Kaufhäusern beziehungsweise bei großen Veranstaltungen in Konzerthallen oder Fußballstadien oder weitläufigen Geländen wie bspw. Tierparks[4] ein einziger QR-Code nur bedingt Rückschlüsse auf konkrete Ansteckungsrisiken darstellen kann. Betrachtet man weiterhin, dass ein Check-Out aus einem Kaufhaus oder von einer Veranstaltung über das sogenannte Geo-Fencing, also das Verlassen eines vom Veranstalter festgelegten Gebietes, stattfinden soll und dies die aktive Freigabe der Ortungsfunktion durch den Nutzer bedingt, erscheint die Luca-App bereits aus rein prozessualer Sicht nur bedingt zur Kontaktnachverfolgung geeignet.

Konkreter: Die Infektionsmeldung eines Teilnehmers einer Großveranstaltung mit nur wenigen oder evtl. nur einem QR-Code für die gesamte Veranstaltung in Kombination mit einem nicht vollständig funktionalen Check-Out-Prozess könnte eine unangemessen hohe Anzahl von Quarantäne- und Test-Anordnungen nach sich ziehen, welche das Gesundheitssystem unnötig belasten würden. Die Konzeption der Corona-Warn-App sieht aus diesem Grund vor, die App nur für Veranstaltungen in geschlossenen Räumen einzusetzen. Halten sich die Besucher in unterschiedlichen Räumen auf, sollte für jeden Raum ein eigener QR-Code erstellt werden. Jeder Besucher scannt dann nur den QR-Code für die Räume, in denen er sich aufgehalten hat. Nur so kann sichergestellt werden, dass nur die Personen gewarnt werden, die auch tatsächlich einem erhöhten Infektionsrisiko ausgesetzt waren.

Neben diesen funktionalen Aspekten sollte bei der Entscheidung für einen Einsatz der Luca-App in Betracht gezogen werden, dass bei der Veröffentlichung von Teilen des Quellcodes der Anwendung bekannt geworden ist, dass die Entwickler der Luca-App teilweise gegen gültiges Lizenzrecht in Deutschland verstoßen haben (unerlaubte Verwendung von Programmzeilen anderer Entwickler). Dadurch ergeben sich unbekannte Risiken für den Einsatz der Luca-App durch die öffentliche Hand, da nicht bekannt ist, ob nicht ggf. weitere Lizenzverstöße in noch nicht veröffentlichten Teilen des Quellcodes vorliegen.

Nutzung der Corona-Warn-App für Zwecke der Event-Registrierung

Grundsätzlich ist es ab Version 2.0 (nach derzeitiger Planung verfügbar ab 16.04.2021) auch mit der Corona-Warn-App möglich, eine Event-Registrierung durchzuführen. Die verwendeten QR-Codes sind dabei kompatibel mit denjenigen des Luca-Systems. Im Gegensatz zur Luca-App sind alle Quellcodes der Corona-Warn-App offengelegt, Lizenzprobleme existieren nicht. Da die Verwendung von QR-Codes lediglich eine funktionale Erweiterung der Exposure-Notification-Funktion darstellt, ergeben sich für den Nutzer im Bereich der Warnung sowie dem Umgang mit Warnungen keine Änderungen.

[4] Siehe dazu auch: https://twitter.com/anked/status/1379689231149326336

Fazit

Der Einsatz der Luca-App erscheint funktional noch nicht empfehlenswert. Insbesondere die nicht verifizierte Eingabe von personenbezogenen Daten lässt an der Korrektheit der ermittelten Kontaktinformationen zweifeln. Ein Missbrauch solcher Eingaben kann zu einer Überlastung des Gesundheitswesens führen.

Mit freundlichen Grüßen
Im Auftrag

[redacted]
Abteilungspräsidentin