Berlin, 14. April 2021

Stellungnahme zum Schreiben des CCC vom 13. April 2021

Wir haben die Stellungnahme des CCC gesehen, geprüft und möchten gerne darauf reagieren. Wir empfinden die Vorwürfe des CCC als überzogen. luca ist ein Hilfsmittel zur Eindämmung der Pandemie - auf keinen Fall der alleinige Heilsbringer. Es ist außerdem ein freiwilliges Angebot für Bürger:innen. Die luca App kann ausgetrickst werden - wie viele andere Hilfsmittel gegen Corona auch.

Eine teils polemische Auseinandersetzung oder ein Wettrennen, wer Systeme am besten täuschen oder missbrauchen kann, ist in der Pandemie aus unserer Sicht nicht hilfreich. Sicherheitsrelevante Fragen sollten unbedingt gestellt werden - hier ist allerdings keine Lücke im luca-System bekannt, durch die hinterlegte Daten der Nutzer:innen gefährdet sind. Um den hohen Sicherheitsstandard zu gewährleisten und das System weiterzuentwickeln ist der Quellcode in einer sehr liberalen Lizenz verfügbar. Hier hoffen wir auf die konstruktive Zusammenarbeit mit der netzpolitischen Community.

Das luca-System befindet sich momentan im Roll-Out in 13 Bundesländern. Innerhalb weniger Wochen werden aktuell circa 300 von 375 Gesundheitsämtern angeschlossen. Vier Millionen Bürger:innen sind bereits bei luca registriert. 81.000 Standorte in Deutschland nutzen luca. Schnelles und konsequentes sowie gleichzeitig rechtsstaatliches und datenschutzkonformes Handeln ist inmitten einer pandemischen Lage erforderlich. Das luca-System ist einsatzfähig.

Ein Lernprozess wird den Einsatz in der Praxis begleiten. Hieran arbeiten in vielen Gemeinden und Landkreisen engagierte Mitarbeiter:innen in Gesundheitsämtern, Stadtverwaltungen, Handelskammern und vielen anderen Institutionen sowie Bürger:innen und Betreiber:innen mit. Und auch wir werden das luca-System immer weiter entwickeln und verfeinern. Epidemiolog:innen, Virolog:innen und Vertreter:innen des Gesundheitsdienstes haben sich mehrfach für eine schnelle und flächendeckende Einführung des luca-Systems ausgesprochen und auf die Wichtigkeit der Verfügbarkeit von Daten im Gesundheitsamt hingewiesen.

Mit der luca App und der Corona-Warn-App des Bundes liegen zwei datenschutzkonforme, digitale Helfer für unsere Gesellschaft vor, um die Pandemie zu bekämpfen. Beide Systeme ergänzen sich in ihrer Zielrichtung und Wirkungsweise und sollten möglichst breitflächig und von vielen Mitbürger:innen eingesetzt werden. Sie sollten nicht gegeneinander ausgespielt werden. Vielmehr

sollten wir als verantwortungsvoll handelnde Bürger:innen und als Gesellschaft jedes Mittel nutzen, um die Pandemie in den Griff zu kriegen.

Wir möchten hier zu den erhobenen Vorwürfen Stellung nehmen:

CCC-Vorwurf: Zweifelhaftes Geschäftsmodell
luca: Transparentes Geschäftsmodell

Das luca-“Geschäftsmodell” ist klar und transparent: Die Bundesländer erwerben eine Lizenz für ihre Gesundheitsämter für die Nutzung des luca-Systems zur Ende-zu-Ende verschlüsselten Datenübermittlung von Nutzer:innen und Betreiber:innen an die Gesundheitsämter. Dieses dient der personifizierten Kontaktnachverfolgung, die die Aufgabe der Ärzt:innen des Öffentlichen Gesundheitsdienstes ist.

Darüber hinaus werden damit verbundene Services, wie z.B. das Hinterlegen von negativen Schnelltests und möglicherweise perspektivisch auch Einlasstickets eingebunden. Diese Daten können Nutzer:innen jeweils nur lokal auf ihrem Smartphone hinterlegen. Wir reagieren damit auf Nachfragen von Kommunen und Landkreisen, die sich diese Kombination für Modellregionen wünschen.

Hieraus ein “unseriöses Geschäftsmodell” abzuleiten halten wir für unsachlich: Eine einfache Nachfrage bei uns oder den beteiligten Partnern hätte gezeigt: Die Anbindung erfolgt für alle Beteiligten kostenlos und unentgeltlich und dient lediglich der Vereinfachung von digitalen Anforderungen im Rahmen von smarten Öffnungsstrategien bei entsprechend niedrigen Inzidenzzahlen. Darüber hinaus erfolgt die Erfassung von Check-in-Daten zweckgebunden. Diese Zweckgebundenheit wird im übrigen auch von den Datenschutzbehörden kontinuierlich beurteilt und überwacht.

CCC-Vorwurf: Unregelmäßigkeiten bei der Auftragsvergabe
luca: Vergabeverfahren gemäß Verordnung

Für die Vergabe öffentlicher Aufträge gibt es klare gesetzliche Regeln. Diese müssen umfänglich von den zuständigen Behörden geprüft werden und sind rechtlich überprüfbar. Die Vergabeverordnung sieht Verhandlungsverfahren ohne Teilnahmewettbewerb gemäß § 14 Absatz 4 Nummer 2b und Nummer 3 vor. Im besonderen Verfahren der digitalen Kontaktnachverfolgung wurden umfangreiche Anwendungserfordernisse formuliert, die mehrere Bundesländer unabhängig voneinander geprüft haben. Offensichtlich erfüllte nur das luca-System alle Standards und Anforderungen.

Insgesamt zehn Länder haben das luca-System in einem gemeinsamen Verhandlungsverfahren ohne Teilnahmewettbewerb beauftragt, erläuterte ein Sprecher des Sozialministeriums Baden-Württemberg unter Leitung von Sozialminister Manne Lucha (Grüne): "Die Vergabestelle, die das Verfahren für die zehn Länder durchgeführt hat, hat diese Form der Vergabe umfassend geprüft und für rechtlich zulässig erachtet. Ein Markterkundungsverfahren hat stattgefunden." Der Vertrag läuft über ein Jahr.
(https://www.sueddeutsche.de/gesundheit/gesundheit-stuttgart-ministerium-empfiehlt-luca-app-trotz-kritik-dpa.urn-newsml-dpa-com-20090101-210414-99-195710)

Zum selben Ergebnis kamen auch die in Bayern erfolgte Vergabe und die damit verbundenen Prüfungen, an der mehrere Bieter teilgenommen haben.

In allen Leistungsanforderungen war beispielsweise die Ende-Zu-Ende Verschlüsselung als MUSS-Kriterium aufgeführt, damit Betreiber:innen nicht Kontaktdaten der Nutzer:innen einsehen und verwenden können. Dies ist nur über eine Fachanwendung möglich, die ein entsprechendes Schlüsselmanagement mitbringt. Weitere Anforderungen waren beispielsweise die Übertragung von Kontakthistorien, die von Nutzer:innen durch Check-ins erstellt werden sowie die Möglichkeit der direkten Benachrichtigung von Gästen bei einer Datenabfrage eines Gesundheitsamtes.

Eine Sprecherin des Ministerium für Energie, Infrastruktur und Digitalisierung in Mecklenburg-Vorpommern betont: "*...dass es uns bei der Beschaffung eines Systems zur Kontaktnachverfolgung um eine möglichst schnelle Lösung ging, die aber insbesondere unsere hohen Anforderungen an den Datenschutz erfüllen musste. Eine Ausschreibung, die in der Regel mehrere Monate dauert, kam für uns in diesem Fall ausnahmsweise nicht in Frage: Die Pandemie hat uns jetzt im Griff und wir brauchten jetzt eine Lösung. Diese Begründung rechtfertigt aus unserer Sicht den Verzicht auf eine zeitintensive Ausschreibung.*" und ergänzt bezüglich der stattgefundenen Markterkundung: *"Unsere Digitalisierungsabteilung hat zunächst mittels einer intensiven Internetrecherche ermittelt, welche Lösungen zum damaligen Zeitpunkt am deutschen Markt überhaupt verfügbar waren und wie diese aussahen. Aus dieser Auswahl ergaben sich zehn Alternativen, die jede für sich weiter geprüft wurden. Dazu wurden die Webseiten der Anbieter, Nutzerbewertungen, vor allem aber auch online verfügbare fachliche Analysen herangezogen. Auf dieser Datenbasis stellte sich heraus, dass das luca-System zu diesem Zeitpunkt die beste verfügbare technische Lösung war und die einzige, die sofort und offenkundig unsere strengen Datenschutzvorgaben sowie die zügige Anbindung an die Software unserer Gesundheitsämter erfüllte. Aus diesem Grund nahmen wir dann persönlich Kontakt zu deren Entwicklern auf.*
Gern möchte ich hinzufügen, dass sich unsere Entscheidung fürs luca-System in jeder Hinsicht bewährt hat. Die Anbindung aller acht Gesundheitsämter sowie der sicheren Server von Telekom und Bundesdruckerei erfolgte binnen acht

Tagen nach Vertragsunterzeichnung und das System fand große Zustimmung bei den Datenschützern, insbesondere dem Landesdatenschutzbeauftragen.”

CCC-Vorwurf: Handwerklich fehlerhafte Validierung
luca: SMS-Verifizierung stark verbessert

Um sich zu bei luca zu registrieren, geben Nutzer:innen ihre Telefonnummer an, die per SMS oder Anruf verifiziert wird.

Bei allen Systemen, die keine Authentifizierung über Benutzername/Passwort (Benutzerkonten) oder beispielsweise ein Google Captcha vornehmen, bleibt ein Missbrauchspotential. Google Captcha kommt im luca-System aus datenschutzrechtlichen Gründen aktuell nicht zum Einsatz.

Welcher Schaden kann hieraus entstehen? Ein missbräuchliches Skript kann SMS und Anrufe zur Verifikation beim luca-System anfordern. Der Schaden ist überschaubar, wenn auch ärgerlich: Die betroffene Telefonnummer bekommt eine SMS oder einen Anruf. Dies ist bereits bekannt aus allen anderen Systemen, die eine Telefonnummer-Verifikation in einer frei zugänglichen App umsetzen.

Um diesen Missbrauch zu begrenzen wurde im luca-System bereits im Rahmen des Penetration Test ein „Rate Limit“ eingebaut, damit ein Missbrauchs-Skript nicht beliebig viele Anrufe absetzen kann. Zusätzlich haben wir alle IP-Adressen von Bot-Netzwerken und dem TOR-Netzwerk auf unsere Blacklist gestellt.

CCC-Vorwurf: luca-Backend ist potenziell jederzeit in der Lage, einzelne Geräte eindeutig zu identifizieren und ihnen alle Check-ins zuzuordnen
luca: Das ist Fundamentalkritik an zentralen Datenspeicherungssystemen

Die luca App kommuniziert mit dem Backend des Servers, um beispielsweise einen Check-in durchzuführen oder Anfragen der Gesundheitsämter zu beantworten. Eine missbräuchliche Nutzung des luca-Backendsystems ist im übrigen strafbewährt und wird von den Aufsichtsbehörden überwacht.

Aus unserer Sicht ist das Fundamentalkritik an zentralen Datenspeicherungssystemen, die im übrigen aber an vielen Stellen des gesellschaftlichen Lebens wie bei Telekommunikationsanbietern, Kreditkartenunternehmen und auch im Gesundheitswesen vielerorts zum Einsatz kommen. Entsprechend müssen diese Systeme gegen Missbrauch abgesichert werden. Dies ist beim luca-System der Fall.

CCC-Vorwurf: Bis heute ist nur ein Teil des Quellcodes des Gesamtsystems öffentlich

luca: Verfügbarer Open Source-Code heute veröffentlicht

Der verfügbare Source Code der luca App wurde am heutigen Mittwoch vollständig unter einer Open Source-Lizenz veröffentlicht. Die Code Repository sind auf GitLab unter luca · GitLab für jeden einsehbar.
Damit ermöglicht Culture4life GmbH, das Unternehmen hinter dem luca-System, eine transparente Analyse und Weiterentwicklung der Software.

Dazu Patrick Hennig, CEO: “Das luca-System soll transparent entwickelt werden - auch um ein hohes Vertrauen in die Sicherheit bei allen Beteiligten und interessierten Nutzer:innen zu erzeugen. Die Standards und Peer-Reviews sorgen außerdem dafür, dass der Quellcode oft getestet und mögliche Issues schnell identifiziert werden können und ein unabhängiger Feedback Prozess ermöglicht wird.”

Die Veröffentlichung des letzten noch fehlenden Elements des Quellcodes erfolgt zwei Wochen später als geplant. Patrick Hennig dazu: “Wir hatten das Projekt luca als private Initiative gestartet und Open Source zunächst nicht eingeplant. Open Source ist soweit auch keine Pflicht. Wir verstehen das Interesse aber und wollten dies nachholen. Es handelt sich aber um sicherheitskritische Software, die wir nicht vorschnell veröffentlichen wollten. Uns ist kein vergleichbares Projekt bekannt, das während eines großen Rollouts seinen ganzen Quellcode offen gelegt hat. Daher haben wir uns die Zeit genommen. Wir möchten aber die geforderte Transparenz herstellen und freuen uns auf den Austausch.”

CCC-Vorwurf: Luca-Schlüsselanhänger verraten bei jedem Scan die vollständige zentral gespeicherte Location-Historie

luca: Missbrauch mit Historie bei Schlüsselanhänger nicht mehr möglich. Schutz der Kontaktdaten war immer gewährleistet

Die persönlichen Schlüsselanhänger im luca-System dienen dazu, auch Mitbürger:innen ohne Smartphone am luca-System und damit an der schnelleren und effizienteren Kontaktnachverfolgung teilhaben zu lassen.
Für luca ist eine möglichst breite Teilnahmemöglichkeit wichtig, um alle Mitbürger:innen im Falle einer erforderlichen Kontaktnachverfolgung schnell und zuverlässig informieren zu können.

Jeder Schlüsselanhänger ist – wie die eigene Telefonnummer – statisch. Der Schlüssel selbst ist auf dem Schlüsselanhänger im QR Code und der Seriennummer hinterlegt. Durch die Schlüssel auf dem Anhänger werden Historie und Kontaktdaten der Nutzer:innen gegenüber dem System vor unerwünschten Zugriffen verschlüsselt. Daher empfehlen wir, den

Schlüsselanhänger vertraulich aufzubewahren. Die Daten der Nutzer:innen sind weiterhin nur vom Gesundheitsamt entschlüsselbar. Im vorgeworfenen Beispiel hat ein Dritter sich Besitz über ein Schlüsselanhänger verschafft. Daher konnte der Angreifer die Historie dieses einen Schlüsselanhängers herausfinden, jedoch nicht die Kontaktdaten. Wir haben zur Sicherheit diese Möglichkeit abgeschaltet.

CCC-Vorwurf: Die App erfüllt Mindeststandards der Barrierefreiheit nicht
luca: Barrierefreiheit wird implementiert

Die Barrierefreiheit werden wir selbstverständlich herstellen. Wir sind mit entsprechenden Verbänden und Berater:innen im Gespräch, um hier die Anforderungen und Bedürfnisse zu erfüllen. Die ersten Verbesserungen, wie zum Beispiel Voice Over, sind bereits fertig entwickelt und sind Bestandteile der nächsten Releases.

CCC-Vorwurf: Die Gesundheitsämter sind bisher jedoch weder durch besonders schnelle Kontaktnachverfolgung noch durch besonderes Interesse an Besuchslisten aufgefallen
luca: Unser System entlastet die Mitarbeiter:innen der Gesundheitsämter und beschleunigt Prozesse durch digitale Kontaktnachverfolgung

Die Gesundheitsämter durch digitalen Prozesse und vollständige Daten zu entlasten, ist in der Bekämpfung der Pandemie bereits viel diskutiert. luca digitalisiert den Nachverfolgungsprozess in den Gesundheitsämtern. Die Information über Risikobegegnungen erfolgt nach individuelle Risikobewertung durch das Gesundheitsamt. luca ist dabei die verlängerte Werkbank der Ärzt:innen der Gesundheitsämter und sorgt dafür, dass nur die relevanten Daten im Gesundheitsamt ankommen und gelesen werden können..

Dr. Ute Teichert, Direktorin der Akademie für Öffentliches Gesundheitswesen, Düsseldorf und Vorsitzende des Bundesverbandes der Ärztinnen und Ärzte des Öffentlichen Gesundheitsdienstes e.V. sagt dazu: *„Die vergangenen Monate haben gezeigt, dass Vollständigkeit der Daten und Geschwindigkeit die beiden entscheidenden Parameter im Kampf gegen die Pandemie sind. Wenn ein Gesundheitsamt das Kontaktpersonen-Management-System SORMAS nutzt, erscheint der Fall direkt in der Datenbank. Das ist fantastisch. Aber auch Gesundheitsämter, die SORMAS noch nicht nutzen, können ihre Systeme schnell und unkompliziert direkt an die Luca-App anbinden. luca funktioniert schon jetzt, es muss nichts mehr neu programmiert werden, und die App kann als Tool zur Pandemiebekämpfung sofort eingesetzt werden.“*

Die schnelle und lückenlose Kontaktnachverfolgung sei ein wesentlicher Faktor beim Eindämmen der Pandemie, sagte Gesundheitsministerin Ursula

Nonnemacher (Grüne/ Brandenburg). Nur so könnten Infektionsketten unterbrochen werden. "Die digitale Kontaktnachverfolgung durch Luca ist ein wichtiger Baustein bei Öffnungsschritten, sobald die Infektionszahlen nachhaltig sinken", so Nonnemacher weiter.
(https://www.rbb24.de/politik/thema/corona/beitraege/2021/04/brandenburg-erste-gesundheitsaemter-luca-app.html)

Der Hauptgeschäftsführer des Landkreistags Baden-Württemberg, Alexis von Komorowski, sagte am Mittwoch: *"Das Land sollte jetzt rasch ein breites Bündnis aus Handel, Gastronomie, Tourismus und Kultur initiieren, damit gemeinsam mit den Kommunen die Voraussetzungen für eine breite Nutzung der App durch die Bürgerinnen und Bürger geschaffen werden können."* Die flächendeckende Nutzung wäre für die digitale Kontaktpersonennachverfolgung "*ein echter Meilenstein*". "*Deswegen unterstützen die Gesundheitsämter dieses Vorgehen auch auf breiter Front*", sagte von Komorowski laut Mitteilung.
(https://www.sueddeutsche.de/gesundheit/gesundheit-stuttgart-ministerium-empfiehlt-luca-app-trotz-kritik-dpa.urn-newsml-dpa-com-20090101-210414-99-195710)

CCC-Vorwurf: Mecklenburg-Vorpommern will die Installation sogar zur Voraussetzung der Teilhabe am öffentlichen Leben machen.
luca: Die Nutzung der luca-App ist freiwillig

Die Nutzung der luca App ist freiwillig. Auch Betreiber:innen bleibt die Wahl der Mittel, mit denen sie der Verpflichtung der Anwesenheitsdokumentation im Rahmen der Kontaktnachverfolgung gemäß der jeweiligen Corona Verordnung nachkommen.

Dies gilt auch für Mecklenburg-Vorpommern. Die Sprecherin des Ministerium für Energie, Infrastruktur und Digitalisierung Mecklenburg-Vorpommern sagt dazu: "*Die Händlerinnen und Händler haben teilweise nach den einschlägigen Bestimmungen Anwesenheitslisten zu führen, deren genaue Inhalte die Corona-Schutz-Rechtsverordnung vorsieht. Diese kann durch eine digitale Lösung ersetzt werden. Insoweit ist die Nutzung der Luca-App also freiwillig. Wir appellieren jedoch an alle, die App zu nutzen, um die Kontaktnachverfolgung zu erleichtern und somit am Ende zu einer Lockerung der Corona-Beschränkungen beizutragen."*

CCC-Vorwurf: Eklatante Mängel in Spezifikation
luca: Wir haben uns für den Referenzierungsfehler entschuldigt

Der Beginn der Veröffentlichung des Source Code war für den 31.3. geplant. Bereits am 30.3 wurde mit der Android App die erste Komponente auf GitLab veröffentlicht. Erste Personen haben sich schon vor Bekanntgabe in das Projekt eingelesen. Die gesamte Veröffentlichung - auch der folgenden Bausteine wie

Frontend und Backend - unterliegt einer freien Lizenz. An einer Stelle wurde ein Open Source Code-Baustein verwendet, der zur freien Verfügung steht. Dieser wurde nicht nach gängiger Praxis referenziert, das wurde aber umgehend behoben. Durch die starke Verteilung von Code in verschiedenen öffentlichen Projekten unter diversen Lizenzen und durch automatische Refactoring Tools können solche Lizenzkommentare in der Praxis verloren gehen.

Um es klar zu sagen: Wir haben einen Referenzierungsfehler gemacht, für den wir uns beim Autor sofort persönlich entschuldigt haben und auch bei der Open Source Community entschuldigen!