#luca App zu EPLF Studie

Ein Team aus Forscher:innen rund um Carmela Troncoso, EPLF, die das dezentrale System CrowdNotifer entwickelt haben, veröffentlichten am 22. März 2021 eine Analyse zum Sicherheitskonzept von luca Link: https://arxiv.org/abs/2103.11958. Das uns vorliegende Papier dreht sich in der Analyse im Kernpunkt um die Frage, ob eine zentrale Kontaktnachverfolgung durch die Gesundheitsämter oder eine dezentrale Lösung, die auf das Einspeisen von Testergebnissen der Nutzer:innen angewiesen ist, die “bessere” Lösung ist.
Hierzu müssen sowohl datenschutztechnische und -rechtliche als auch epidemiologische Argumente zusammengeführt werden. Hierauf verweisen im übrigen auch die Publisher der Studie.

In der Folgeabschätzung basiert die Studie scheinbar auf der irrigen Annahme, dass im luca Backendsystem Postiv-Testergebnisse hinterlegt sind, der luca Back End Server also weiß, ob eine Person positiv getestet ist. Dies ist nicht der Fall. Im luca Backend Server sind keine positiven Testergebnisse hinterlegt. Auch das freiwillige Teilen der Kontakthistorie oder eine Anfrage des Gesundheitsamts bedeutet nicht, dass Nutzer:innen infiziert sind.

Das luca System verfügt über keine zentrale Stelle, die Daten alleine entschlüsseln kann. Dies reduziert signifikant die Wahrscheinlichkeit sowohl für erfolgreiche Angriffe durch Innentäter als auch von erfolgreichen Angriffen durch Schadsoftware oder sonstige externe Angreifer wie Hacker. Selbst für den Fall, dass diese Zugriff auf die Daten bekommen, sollten sie für diese nicht lesbar sein. Dies bestätigt auch das Gutachten des Landesdatenschutzbeauftragten Baden-Württemberg, dessen Veröffentlichung wir ausdrücklich zugestimmt haben.

Das Backend und Frontend der Gesundheitsämter läuft auf Servern des Bundes, die insgesamt ein besonders sensibler Bereich der digitalen Infrastruktur sind und daher generell einem besonderen Schutz unterliegen. Einen Angriff auf das luca System aus dieser Richtung kann unserer Meinung nach ausgeschlossen werden.

Zur Frage, ob zentrale oder dezentrale Systeme (an denen es im übrigen ebenfalls Kritik gibt) wirkungsvoller in der Pandemiebekämpfung sind, zeigt die bisherige Erfahrung, dass in den dezentralen Systemen zu wenige Nutzer:innen ihr Testergebnis teilen, Verzögerungen auftreten und insgesamt leider zu wenig Infektionsketten unterbrochen werden. Darüber hinaus kann eine wissenschaftliche Begleitung, wo und wieso besondere Clusterinfektionen entstehen (Superspreading Events) nicht stattfinden, da keine entsprechende Datenbasis vorliegt.

Von circa 2,6 Millionen Infizierten in Deutschland warnten leider nur 302.000 ihre Mitbürger:innen (circa 11%) durch die Einspeisung ihrer Testergebnisse in der Corona-Warn-App. Dies sind 302.000 Infektionsketten, die unterbrochen werden konnten, aber eben 2,3 Millionen Infektionsketten, die nicht durch die Corona-Warn-App unterbrochen wurden. Aus Sicht des BMG und aus unserer Sicht ergänzen sich beide Anwendungen perfekt, weswegen eine entsprechende Zusammenarbeit in den letzten Tagen angekündigt wurde, die im luca System ab Mitte April umgesetzt wird.

Hierzu sagt Prof. Dr. Maximiliane Wilkesmann, Professorin für Arbeits- und Organisationssoziologie, Fakultät Sozialwissenschaften, Technische Universität Dortmund

„Die Luca-App kann vor allem für Schnelligkeit in der Kontaktverfolgung durch die Gesundheitsämter sorgen, welche essenziell für die Identifizierung von Superspreadern bei der Bekämpfung der Covid-19-Pandemie ist. Einher geht dies mit einem weiteren erforderlichen Digitalisierungsschub in den Gesundheitsämtern. Aus meiner eigenen Forschung und der Beschäftigung mit Wissen und Nichtwissen im Gesundheitswesen weiß ich, dass gerade im medizinischen Bereich nach wie vor Faxgeräte eine zentrale Rolle bei der Übermittlung von Gesundheitsinformationen spielen."

luca stellt dem Gesundheitsamt nicht nur Daten im Infektionsfall zur Verfügung, sondern informiert auch besuchte Locations und mögliche Kontaktpersonen und reduziert dadurch den Aufwand der Kontaktnachverfolgung in den Gesundheitsämtern und gibt möglichen Betroffenen einen entscheidenden zeitlichen Vorteil im Umgang mit dem Virus.

Das luca System nutzt eine dezentrale Schlüsselspeicherung, gleichwohl nimmt das luca Backend eine zentrale Rolle in der Speicherung und Verwaltung der Datensätze ein. Im Bewusstsein der Herausforderungen eines zentralen Systems nutzt luca nicht nur die marktüblichen Sicherungsmaßnahmen und vertrauenswürdige Cloudanbieter, sondern arbeitet intensiv mit Sicherheitsforschern wie z.B. Prof. Dr. Marian Margraf, Fraunhofer AISEC zusammen, um das System kontinuierlich weiter zu entwickeln.
Penetration Tests wurden von ERNW durchgeführt, die Ergebnisse sind öffentlich einsehbar und zeigen keine kritischen Risiken.

Zu weiteren Kritikpunkten.

Die Forscher:innen EPLF kritisieren eine fehlende Third Party Zertifizierung der Schlüssel in den Gesundheitsämtern.
Dieser Punkt ist uns bewusst, weswegen wir sehr deutlich an politische Entscheider appellieren, dass luca System auf Länderebene einzuführen. Denn dann übernimmt die Bundesdruckerei als Third Party die Ausstellung und Verteilung der Zertifikate der Gesundheitsämter. Dies ist ein gelerntes Verfahren z.B. aus dem Prozess der digitalen Einreisemeldung und räumt einen zentralen Kritikpunkt aus.

(Im übrigen verhindert auch das aktuelle Verfahren, dass neXenio oder Mitarbeiter von neXenio die vergebenen Schlüsselzertifikate entschlüsseln oder nutzen können.)

Technischer ausgedrückt:
Das in der Analyse diskutierte Thema des Vertrauens-Dienstanbieters (CA, certification authority) ist uns bewusst und sehr wichtig. Die Erstellung vertrauenswürdiger CA Zertifikate wird durch die Einbindung der D-Trust GmbH (Tochter der Bundesdruckerei) gelöst. Voraussetzung hierfür sind entsprechende Verträge auf Länderebene.
Daher unser Appell für eine Implementierung des Systems auf Bundes- oder Landesebene.

Ein Dauerbetrieb der aktuellen Modelllösung ist von uns nicht gewollt.

Darüber hinaus wird kritisiert, dass die Authentizität von Entschlüsselungsanfragen an beispielsweise Venue Owner/Betreiber oder Nutzer unklar wäre. Deren Authentizität wird jedoch gerade durch die HDSKP (Health Department Signing Key Pair) Signatur in Zukunft sichergestellt. Darüber hinaus ist dieser Schlüsselsatz immer nur einen Tag gültig und wird täglich erneuert. Alle Daten werden nach 30 Tagen gelöscht. Es findet kein Datenabfluss an Dritte statt.

Die Forscher:innen der EPFL weisen darauf hin, dass sich das Versprechen, dass nur das Gesundheitsamt im Infektionsfall mit dem derzeitigen Aufbau des Systems nicht halten lasse: “Weil Nutzer:innen bei einem Check-in mit Luca nicht nur verschlüsselte Daten an den Server schicken, sondern auch ihre IP-Adresse und andere Informationen über ihr Handy übermitteln, lasse sich mit großer Wahrscheinlichkeit rekonstruieren, welches Gerät und letztlich und letztlich welche Person sich hinter einer pseudonymen Nutzer-ID verbirgt.”

Hier möchten wir darauf hinweisen, dass dies bei quasi jeder Browser oder App Nutzung theoretisch möglich ist. Missbrauch durch den Anbieter ist gesetzlich geregelt und im Fall eines Verstoßes auch strafbar.

Das luca System nutzt solche Meta-Daten nicht zur De-anonymisierung der Nutzer, dies würde dem kryptografischen Konzept, das mit Prof. Dr. Marian Margraf, Fraunhofer AISEC entwickelt wurde, widersprechen.

Bezüglich eines möglichen Zugriffs von anderen Staatsorganen außerhalb des Gesundheitsamts und dem Einsatz von luca zum Beispiel bei politischen Treffen, in Glaubensgemeinschaften, Kirchen und Moscheen möchten wir zum einen darauf hinweisen, dass eine Nutzung von luca freiwillig ist und lediglich dem Hausrecht des Veranstalters unterliegt. Papierzettel werden nicht abgeschafft, luca ist ein ergänzendes, digitales System, was genutzt werden kann, aber nicht genutzt werden muss. Zusätzlich stellt der Austausch des involvierten Schlüsselmaterials eine sehr große Hürde. Diese müssten Staatsorgane an allen dezentralen Stellen abgreifen.

Darüber hinaus hat Dr. Anne Riechert dazu wie folgt Stellung genommen und verweist an die Möglichkeit des Gesetzgebers hier ausdrückliche Regelungen vornehmen zu können: „Eine Strafverfolgungsbehörde hat sich in der Vergangenheit die Kontaktliste eines Restaurants zu Beweiszwecken aushändigen lassen]. Mit Blick auf digitale Informationen, die etwa auf einem Mobiltelefon gespeichert sind, soll die Sicherstellung gemäß § 94 Absatz 1 StPO gestattet sein. Bei einer installierten App müssten die Kontaktdaten allerdings zunächst entschlüsselt werden. Grundsätzlich ist in diesem Zusammenhang zu beachten, dass dezentral auf einem Mobiltelefon gespeicherte Kontaktdaten, die der Nachverfolgung von Infektionsrisiken dienen, nicht dem Fernmeldegeheimnis unterliegen und keine Gesundheitsdaten darstellen. Beschlagnahme- und Verwertungsverbote könnten daher ausdrücklich gesetzlich geregelt werden.“
Prof. Dr. Anne Riechert Professorin für Datenschutzrecht und Recht in der Informationsverarbeitung, Frankfurt University of Applied Sciences

Zur selben Frage äußert sich auch noch einmal *Prof. Dr. Maximiliane Wilkesmann*

Professorin für Arbeits- und Organisationssoziologie, Fakultät Sozialwissenschaften, Technische Universität Dortmund

„Das Problem sehe ich in der vorliegenden datentreuhänderischen Konstellation nicht. Anstatt diese Diskussion zu eröffnen beziehungsweise zu befeuern, sollten die Chancen der Nutzung und Freiheitsgewinne im Vordergrund stehen. Die Chance liegt vor allem in der Gewinnung epidemiologischer Zusammenhänge, sprich an welchen Orten, in welchen Zeiträumen ist ein besonders hohes Infektionsrisiko vorhanden. Nur so lassen sich gezielte, evidenzbasierte Maßnahmen – zum Beispiel Schließungen – zur Bekämpfung der Pandemie ableiten, die wiederum für eine höhere Akzeptanz in der breiten Bevölkerung sorgen können."

Ebenso erheben die Forscher:innen den Vorwurf, dass luca ermögliche Covid-19 infizierte Personen zu stigmatisieren bzw. einer potentiellen Erpressung auszusetzen:
ZItat: "Diese Schwäche in der zentralen Architektur von Luca betrifft auch jene, die eine Infektion melden. Denn letztlich wisse der Server von Luca über diese Verknüpfungen auch, welche Nutzer:innen sich in der App positiv für Covid-19 gemeldet haben und welche Personen vom Gesundheitsamt kontaktiert wurden. Werden diese Informationen öffentlich, könne das zu einer Stigmatisierung von Nutzer:innen führen, Betroffene könnten mit dem Wissen erpresst werden."

Hier unser Hinweis, dass diese Daten bereits jetzt in unterschiedlichen anderen Datenbanksystemen gespeichert sind, teilweise deutlich schlechter geschützt als im luca System. Und auch wieder: es gibt keine zentrale Stelle im luca System, die alleine die Daten entschlüsseln kann.
Gerne möchten wir hier ergänzen: Eine gesellschaftliche Stigmatisierung von Mitbürger:innen mit einer COVID-19 Infektion lehnen wir als Unternehmen und Mitarbeiter:innen schon von unseren Grundwerten her ab und sehen es als gesamtgesellschaftliche Aufgabe dem entgegenzuwirken.

Im übrigen möchten wir darauf verweisen, dass dieses Problem auch in Bluetooth basierten, dezentralen Lösungen scheinbar nicht zu verhindern wäre:
https://www.netzwoche.ch/news/2020-06-16/das-sind-die-schwachstellen-der-swiss-covid-app
Zitat zur Swiss Covid App: Die App berge auch Risiken in Bezug auf die Privatsphäre der Personen, bei denen ein Covid-19-Test positiv ausgefallen ist. Zwar erfolgt die Identifizierung der Benutzer mittels eines Pseudonyms. Gleiche man die Daten jedoch mit weiteren von Drittpersonen ab, lasse sich die Identität des Benutzers herausfinden, sagt der Experte. Diese Verwundbarkeit bestehe aufgrund des dezentralisierten Ansatzes, auf dem Swiss-Covid basiere, ergänzt der EPFL-Forscher."

Einige weitere Punkte, die in der Studie angesprochen werden, sind uns bekannt und in im Rahmen der kontinuierlichen Weiterentwicklung den nächsten Versionen verändert:

Wechselnde User-IDs,
luca verwaltet Nutzer:innen mithilfe von UserIDs. Mit jeder UserID sind auf dem luca-Server die verschlüsselten Daten der Nutzer:innen verknüpft. Jeder Checkin enthält die UserID

allerdings nur verschlüsselt, so dass die Checkins vom Luca System nicht einem Nutzer zugeordnet werden können.
Im Infektionsfall, kann ein Gesundheitsamt die verschlüsselte UserID beziehen, entschlüsseln und so die Person kontaktieren.

Zukünftig wird nicht nur der QR Code minütlich erneuert, um jeweils aktuelle TraceIDs zu erzeugen, sondern auch jeweils eine zufällige User-ID erzeugt. Dies erschwert, eine theoretisch mögliche Zuordnung von aufeinanderfolgenden Check-Ins mit demselben Endgerät noch einmal zusätzlich. Und verschleiert die Historie des Nutzers gegenüber dem System noch stärker. Dies ähnelt dem Mechanismus der sich jetzt schon ändernden traceIDs.

Ebenso werden künftig TraceIDs im Gesundheitsamt auf dem Front End berechnet, das auf Servern des Bundes läuft. Dies erschwert zusätzlich dem Luca Backend die Nachvollziehbarkeit von Nutzerhistorien.

Die Auslieferung von Desktop Apps bei Betreiber:innen anstatt wie jetzt gewählt per WebApp haben wir im Vorfeld geprüft, halten wir aber nicht für praktikabel in einer breiten Nutzung.
Hierzu gilt es auch zu betonen, dass insbesondere in Gesundheitsämtern der sichere Betrieb der IT Infrastruktur im Vordergrund steht, und somit auch keine ungesichteten Änderungen von Browsern oder Software vorgenommen werden. Auch dass Betreibe mehrere Smartphones nutzen, die dann alle Teile der Daten sammeln ist sehr unpraktikabel.

Das Ergänzen des Venue Public Key im QR Code des Gastgebers wird weitere dezentrale Merkmale in das Gesamtsystem hinzufügen. Aufgrund der Größe des Keys war dies bisher nicht einfach möglich, es gibt aber bereits Ansätze dazu.

Bezüglich einer datenschutzrechtlichen Einschätzung verweisen wir auf die Stellungnahmen der unterschiedlichen Landesdatenschutzbeauftragten und die damit beschäftigte Arbeitsgruppe sowie die entsprechenden Gutachten von ERNW.