LANDTAG NORDRHEIN-WESTFALEN
17. Wahlperiode

Drucksache **17/14576**

20.07.2021

Antwort

der Landesregierung

auf die Kleine Anfrage 5610 vom 21. Juni 2021
des Abgeordneten Matthi Bolte-Richter BÜNDNIS 90/DIE GRÜNEN
Drucksache 17/14251

Sicherheitslücken bei der Luca-App

Vorbemerkung der Kleinen Anfrage

Die Luca-App wurde in den vergangenen Wochen – auch durch das Werben von Ministerpräsident Laschet – in der öffentlichen Debatte regelmäßig als wichtiges Hilfsmittel zur Kontaktnachverfolgung und damit zur Bewältigung der Corona-Pandemie diskutiert. Zugleich nahmen die Sicherheitsbedenken durch IT-Fachleute stetig zu. So veröffentlichte der Chaos Computer Club (CCC) bereits am 13. April eine Stellungnahme, in der er das Ende der Luca-App insbesondere im öffentlichen Bereich forderte.

Wörtlich hieß es beim CCC: „In den vergangenen Wochen wurden eklatante Mängel in Spezifikation, Implementierung und korrekter Lizenzierung der Luca-App aufgedeckt. Die nicht abreißende Serie von Sicherheitsproblemen und die unbeholfenen Reaktionen des Herstellers zeugen von einem grundlegenden Mangel an Kompetenz und Sorgfalt.“[1] Kurz zuvor hatte auch die Berliner Datenschutzbeauftragte „beträchtliche Risiken“ beim Einsatz der Luca-App gesehen[2].

Ende April warnten mehr als 70 Forscherinnen und Forscher aus dem Feld der IT-Sicherheit, die Risiken beim Einsatz der Luca-App seien „völlig unverhältnismäßig“[3].

Am 28. Mai schließlich warnte auch das Bundesamt für Sicherheit in der Informationstechnik vor der Luca-App[4]. Es verwies dabei auf eine Sicherheitslücke, durch die eine sogenannte Code Injection die Übertragung einer Schadsoftware in die Systeme der Gesundheitsämter ermögliche.

Der Minister für Wirtschaft, Innovation, Digitalisierung und Energie hat die Kleine Anfrage 5610 mit Schreiben vom 19. Juli 2021 namens der Landesregierung beantwortet.

[1] https://www.ccc.de/de/updates/2021/luca-app-ccc-fordert-bundesnotbremse
[2] https://www.tagesspiegel.de/berlin/betraechtliche-risiken-bei-corona-software-berlins-datenschutzbeauftragte-warnt-vor-luca-app/27079224.html
[3] https://www.zeit.de/digital/datenschutz/2021-04/luca-app-sicherheitsluecken-datenschutz-kritik-corona
[4] https://www.zeit.de/2021-05/luca-app-it-sicherheit-bsi-corona-kontaktverfolgung-hackerangriff

Datum des Originals: 19.07.2021/Ausgegeben: 26.07.2021

Vorbemerkung der Landesregierung

Die Rückverfolgbarkeit von Kontakten spielt in der Corona-Pandemie eine wichtige Rolle. Sie ermöglicht es, gezielte Infektionsschutzmaßnahmen einzuleiten und das Infektionsgeschehen einzudämmen. Die Rückverfolgbarkeit ist in § 8 der CoronaSchVO geregelt. Auch die digitale Erfassung von Kontaktdaten ist möglich. Bezüglich der digitalen Kontaktnachvollziehung gibt es viele verschiedene technische Lösungen. Das Land Nordrhein-Westfalen setzt diesbezüglich auf Anbieter-Pluralität.

1. Seit wann verfügt die Landesregierung über jeweils welche Sicherheits- und Gefährdungsanalyse hinsichtlich der Luca-App und ihres Einsatzes?

2. Welche Konsequenzen hat die Landesregierung aus der jeweiligen Sicherheits- und Gefährdungsanalyse gezogen?

Die Fragen 1 und 2 werden aufgrund ihres Sachzusammenhanges gemeinsam beantwortet.

Das Land ist mit der neXenio GmbH bezüglich des Einsatzes der Luca-App keine vertragliche Bindung eingegangen. Seitens der Landesregierung wurde somit auch keine Sicherheits- und Gefährdungsanalyse durchgeführt. Die Landesregierung setzt bei der digitalen Kontaktnachvollziehung auf Anbieterpluralität, hat mit keinem Anbieter einer Kontaktnachvollziehungslösung einen Rahmenvertrag geschlossen und somit auch keine derartige Prüfung durchgeführt. Stattdessen setzt sie sich für den Einsatz der Gateway-Lösung IRIS connect ein, bei der Sicherheits- und Penetrationstests durchgeführt werden. Die Luca-App ist noch nicht an IRIS connect angeschlossen.

IRIS connect kann – eine entsprechende Kooperation mit dem Anbieter von Luca vorausgesetzt – auch von Luca verschlüsselte Daten an das jeweilige Gesundheitsamt übermitteln und diese dann im IRIS Client im Gesundheitsamt zur Verfügung stellen.

Da der IRIS Client durch das Gesundheitsamt eingesetzt wird, kann dieser auch entsprechend verschlüsselte Daten bei Bedarf entschlüsseln.

Wie im Luca-System erfolgt die Entschlüsselung dann erst im Gesundheitsamt.

Ein derartiger Austausch von verschlüsselten Informationen ist aber nur möglich, wenn der Anbieter von Luca mit IRIS connect in den technischen Austausch tritt, um hier im Sinne der Gesundheitsämter eine praxistaugliche, einfache, aber dennoch sichere Lösung zur Anbindung von Luca an IRIS connect zu finden.

Die einzelnen Kommunen entscheiden eigenständig, ob und welche digitalen Lösungen zur Kontaktnachvollziehung bereitgestellt werden. Wird die Lösung Luca eingesetzt, beruht dies auf einer lokalen Entscheidung.

3. Wie hat die Landesregierung die Landesbehörden, die nachgeordneten Bereiche und die Kommunen über die jeweils aktuelle Sicherheits- und Gefährdungsanalyse hinsichtlich der Luca-App und ihres Einsatzes informiert?

4. Wie hat die Landesregierung die Bürgerinnen und Bürger über die jeweils aktuelle Sicherheits- und Gefährdungsanalyse hinsichtlich der Luca-App und ihres Einsatzes informiert?

Die Fragen 3 und 4 werden aufgrund ihres Sachzusammenhanges gemeinsam beantwortet.

Das Land hat keine eigene Sicherheits- und Gefährdungsanalyse durchgeführt. Die Informationen bezüglich etwaiger Sicherheitslücken beim Einsatz der Luca-App sind in den freien Medien öffentlich zugänglich[5] und dementsprechend verbreitet. Das Land hat auf die bestehende Thematik und Informationen hingewiesen. Es besteht keine ergänzende Notwendigkeit zur gesonderten ausführlichen Verteilung der öffentlich zugänglichen und breit publizierten Informationen.

5. Sollten aus Sicht der Landesregierung öffentliche Stellen die Luca-App einsetzen, ihre Verwendung empfehlen oder bei Nutzung öffentlicher Infrastrukturen voraussetzen?

Das Land setzt bei den digitalen Lösungen zur Kontaktnachvollziehung auf Anbieterpluralität, deren Umsetzung nunmehr technisch durch die Gateway-Lösung IRIS connect erleichtert wird. Die verschiedenen am Markt befindlichen Apps können sich an IRIS connect, als digitale Schnittstelle zu den Gesundheitsämtern, anbinden. Welche Lösung eingesetzt wird, entscheiden die Akteure vor Ort. Die Landesregierung spricht keine Empfehlung aus. Ziel ist es, den Gesundheitsämtern mit IRIS connect einen einfachen und einheitlichen Weg zur Verfügung zu stellen, über den sie Gästelisten aus verschiedensten Quellen abfragen können.

Die Datenübertragung wird dabei in allen Fällen auf dem Transportweg verschlüsselt und gegenseitig mit Zertifikaten von D-Trust (Bundesdruckerei) zwischen den Akteuren im IRIS connect System abgesichert. IRIS connect ist dabei keine eigenständige App zur Kontaktdatenerfassung.

Die CoronaSchVO NRW verpflichtet bei der digitalen Kontaktnachvollziehung nicht dazu, eine bestimmte Lösung einzusetzen.

[5] U.a.: https://www.daserste.de/information/wirtschaft-boerse/plusminus/sendung/sr/sendung-vom-09-06-2021-luca-app-100.html; https://twitter.com/mame82/status/1406269269873201159?s=20%3E; https://twitter.com/mame82/status/1405855701830938627; https://vimeo.com/565012610; https://twitter.com/mame82/status/1405889593644363781?s=20%3E; https://www.ccc.de/de/updates/2021/luca-app-ccc-fordert-bundesnotbremse; https://www.tagesspiegel.de/berlin/betraechtliche-risiken-bei-corona-software-berlins-datenschutzbeauftragte-warnt-vor-luca-app/27079224.html; https://www.zeit.de/digital/datenschutz/2021-04/luca-app-sicherheitsluecken-datenschutz-kritik-corona; https://www.zeit.de/2021-05/luca-app-it-sicherheit-bsi-corona-kontaktverfolgung-hackerangriff; https://t3n.de/news/sicherheitsluecke-kriminelle-1380790/