Bayerischer Landtag

18. Wahlperiode 31.05.2021 **Drucksache** 18/**16049**

Dringlichkeitsantrag

der Abgeordneten **Katharina Schulze, Ludwig Hartmann, Benjamin Adjei, Gülseren Demirel, Thomas Gehring, Jürgen Mistol, Verena Osgyan, Tim Pargent, Stephanie Schuhknecht, Gisela Sengl, Florian Siekmann, Kerstin Celina, Barbara Fuchs, Tessa Ganserer, Christina Haubrich, Claudia Köhler, Andreas Krahl, Eva Lettenbauer** und **Fraktion (BÜNDNIS 90/DIE GRÜNEN)**

IT-Sicherheitsbedenken ernstnehmen – Umfangreiche und unabhängige Sicherheitsanalyse der Luca-App durchführen lassen

Der Landtag wolle beschließen:

Die Staatsregierung wird aufgefordert, die Kontaktnachverfolgungsapp „Luca“ schnellstmöglich einer umfangreichen und unabhängigen Sicherheitsanalyse zu unterziehen.

Die Sicherheitsanalyse soll mindestens folgende Punkte umfassen:

– Konzeptionelle Sicherheitsüberprüfung, bei der das Softwaresicherheitskonzept (inkl. Softwarearchitektur und Krypto-Konzept) umfassend auf konzeptionelle Schwachstellen untersucht wird. Hierbei sind sowohl Frontend (Mobile App) als auch Backend (Serverapplikation) zu betrachten.

– Source Code Audit, bei dem der Quellcode auf Programmierfehler und sicherheitskritische Schwachstellen im logischen Aufbau der Softwarekomponenten geprüft wird.

– Umfassende Penetrationstests mit hoher Prüftiefe, um mögliche Angriffsszenarios und -vektoren identifizieren zu können. Hierbei sind nicht nur mögliche Angriffe auf die Mobile App und die Serverapplikation zu prüfen, sondern auch potenzielle Risiken für die Gesundheitsämter, die sich durch Integration von Luca in die internen Prozesse ergeben, zu evaluieren.

– Anfertigung einer detaillierten Dokumentation der Sicherheitsanalyse sowie eines Lastenheftes, in dem alle offenen Sicherheitsanforderungen sachgemäß spezifiziert werden.

Diese Analyse soll durch ein unabhängiges Forschungsinstitut durchgeführt werden. Die Ergebnisse sind anschließend vollumfänglich zu veröffentlichen.

Begründung:

Anfang April hat die Staatsregierung eine landesweite Jahreslizenz der Software Luca für über 5,5 Mio. Euro erworben. Damit können bayernweit alle Personen, Unternehmen und Organisationen diese Software kostenfrei zur elektronischen Dokumentation von Kontaktdaten gemäß der bayerischen Infektionsschutzmaßnahmenverordnung nutzen.

Der Freistaat Bayern hat bei solch einem umfangreichen, staatlich finanzierten und behördlich angeordnetem Softwareprojekt aber auch die notwendige Sicherheit und Integrität der Anwendung zu garantieren. Dem ist die Staatsregierung bisher nicht nachgekommen.

Bereits vor der erfolgten Vergabe gab es massive Kritik bezüglich des Sicherheitskonzeptes der Luca-App, die jedoch aufgrund des geheim gehaltenen Quellcodes nicht bestätigt werden konnte. Die Staatsregierung hat im Ausschuss für Staatshaushalt und Finanzfragen auf Nachfrage mehrerer Abgeordneter die schnelle Beschaffung mit der Dringlichkeit aufgrund der Coronapandemie begründet und darauf verwiesen, dass die Einsicht in den Quellcode Teil des Vertrages sei und eine umfangreiche Sicherheitsprüfung durch die Staatsregierung erfolgen würde. Diese Prüfung ist offensichtlich bisher nicht vorgenommen worden.

Seit der mittlerweile erfolgten Veröffentlichung des Quellcodes werden nun regelmäßig Sicherheitslücken und Datenschutzmängel bekannt. Zudem äußerten hunderte namhafte IT-Sicherheitsexpertinnen und -experten (u a. der Chaos Computer Club, der ehem. Bundesdatenschutzbeauftragte Peter Schaar, sowie zahlreiche Professorinnen und Professoren und Wissenschaftlerinnen und Wissenschaftler von Universitäten, Forschungseinrichtungen und NGOs) regelmäßig Kritik an Luca.

Neben grundsätzlicher Kritik am Softwaredesign, der zentralen Speicherung der Daten und der Möglichkeit von Fake-Profilen, wurden auch schwerwiegende Sicherheitsmängel publik. So konnten beispielsweise personenbezogene Daten über die QR-Codes an Schlüsselanhängern ausgelesen und damit personalisierte Bewegungsprofile von den Personen angefertigt werden.

Anfang Mai wurde zudem von einem Team um den IT-Sicherheitsexperten Marcus Mengs ein Angriffsszenario entdeckt, bei dem über die Luca-App Schadcode auf den Systemen der Gesundheitsämter ausgeführt werden konnte. Die Möglichkeit der „Code Injection“ wurde bereits am 3. Mai an die Entwicklerinnen und Entwickler der Luca-App gemeldet, von diesen jedoch weder beachtet noch behoben.

Erst als die Lücke drei Wochen später publiziert wurde, haben die Entwicklerinnen und Entwickler mit einem Quick-Fix reagiert. Eine grundlegende Behebung der Problematik ist bisher noch nicht erfolgt – stattdessen verweisen die Entwicklerinnen und Entwickler auf die Verantwortlichkeit der Gesundheitsämter.

Am 28. Mai riefen die Entwicklerinnen und Entwickler die App-Nutzerinnen und -Nutzer zudem dazu auf, den geheimen Private-Key (der nur den Nutzerinnen und Nutzern selbst zugänglich sein darf) auf einen Server hochzuladen und damit anderen, nicht genauer definierten Personen, zugänglich zu machen. Dies stellt einen groben Verstoß gegen jegliches Verschlüsselungskonzept dar.

Nach den nun am 26. Mai 2021 veröffentlichten und am 28. Mai 2021 vom Bundesamt für Sicherheit in der Informationstechnologie (BSI) bestätigten erheblichen Sicherheitsmängel und dem unzureichenden Umgang der Entwicklerinnen und Entwickler mit der Meldung dieser Mängel, ist eine zeitnahe unabhängige Sicherheitsanalyse der Luca-App dringend geboten.