Sicherheitslücke LucaTrack – Mangelhafte Software für Millionen

Mit nur einem Bild eines beliebigen Schlüsselanhängers, der im «Luca App»-System verwendet wird, lässt sich mit einfachen Programmierkenntnissen unbemerkt das Bewegungsprofil der Nutzer:in des Anhängers auslesen.

In einem technischen Machbarkeitsnachweis weist eine Gruppe verschiedener IT- und Netzexpert:innen aus der Community unter Nutzung frei zugänglicher Schnittstellen eine strukturelle Sicherheitslücke des Luca-Systems nach.

Das Unternehmen und die zuständige Berliner Beauftragte für Datenschutz und Informationsfreiheit wurden am 13. April 2021 darüber in Kenntnis gesetzt.

Die Konsequenzen der Sicherheitslücke sind gravierend. Dementsprechend fordert die Gruppe die Verantwortlichen dazu auf, über 100.000 bereits im Umlauf befindliche Luca-Schlüsselanhänger sofort aus dem Verkehr zu ziehen, um die Ausnutzung dieser Sicherheitslücke zu verhindern.

Luca App Schlüsselanhänger

Die sogenannte «Luca App» soll in weiten Teilen Deutschlands die Gesundheitsämter bei der digitalen Kontaktnachverfolgung unterstützen. Die Anwendung wurde bereits von vielen Bundesländern für insgesamt fast 20 Millionen Euro lizenziert. In vielen Städten soll ihr eine zentrale Rolle als flankierende Maßnahme zu Öffnungen im Einzelhandel, in der Gastronomie, aber auch in Schulen und Kindertagesstätten zukommen.

Für Nutzer:innen ohne Smartphone hält das Luca-Ökosystem Schlüsselanhänger mit aufgedrucktem QR-Code bereit.

Daten nur für das Gesundheitsamt? Nicht ganz…

«An die Daten kommt nur das Gesundheitsamt. Das heißt, man müsste für die Daten händisch in das Gesundheitsamt einbrechen» – Zitat Smudo, 30.03.2021, rbb inforadio

Eine Kombination verschiedener Komponenten des Luca-Systems ermöglicht es, die Historie einer beliebigen Nutzer:in offenzulegen – sofern diese das System über einen Schlüsselanhänger nutzt.

Sicherheitslücke Schlüsselanhänger

Luca verwendet zur Sicherung von sensiblen Daten ein Verschlüsselungsverfahren, das ermöglichen soll, dass nur Gesundheitsämter die Daten zu den Check-ins einer Nutzer:in entschlüsseln können. Die jeweilige Historie ist ansonsten nur auf dem jeweiligen Endgerät der Nutzer:in einsehbar. Prinzipbedingt enthalten Schlüsselanhänger des Luca Systems

allerdings nur aufgedruckte, unveränderliche QR-Codes. Damit entsteht die Sicherheitslücke LucaTrack.

Vorgehen im Detail

Offenlegen der Schlüsselanhänger-Informationen

Schlüsselanhänger des Luca Systems müssen aktiv von einer Location eingescannt werden. Um auf die Informationen eines Schlüsselanhängers zuzugreifen, braucht es zuerst die Registrierungsinformationen aus der Scanner-Anwendung des Luca Systems. Dieser Scanner ist eine simple Webseite, die sich in jedem gängigen Browser aufrufen lässt. Durch Setzen eines simplen Breakpoints (eines Haltepunkts, der Diagnoseinformationen ausgibt) im Browser lassen sich die Registrierungsinformationen eines beliebigen Schlüsselanhängers problemlos beim Scan auslesen.

Ausgabe der Historie des Schlüsselanhängers

Im nächsten Schritt wird die Luca Web App für Nutzer:innen eingesetzt. Die Web App hat ähnliche Funktionen wie die Luca App für iOS oder Android, kann aber im Browser ohne vorherige Installation genutzt werden.

Die ausgelesenen Registrierungsinformationen lassen sich nun in der Web App über eine einfache Anpassung wieder einspielen. Die Web App offenbart dadurch die komplette vorherige Historie der Nutzer:in, deren Registrierungsinformationen erlangt wurden.

Vereinfachung des Vorgehens

Zur Durchführung von LucaTrack können die notwendigen Informationen sogar noch einfacher gewonnen werden. Die Gruppe demonstriert das an einem funktionalen Prototypen, der nur den eigentlichen QR Code benötigt und daraus automatisch eine Standorthistorie des damit verbundenen Schlüsselanhängers der letzten 30 Tage auf einer Karte ausgibt. Der Prozess wurde per Video entsprechend dokumentiert.

Voraussetzung für die Ausnutzung der Sicherheitslücke LucaTrack

Ein Foto des QR-Codes des Schlüsselanhängers reicht bereits aus.

Welche Informationen legt LucaTrack offen?

- Vollständige Historie der Luca Check-ins der Nutzer:in der letzten 30 Tage
- Genaue Geo-Koordinaten aller genutzten Locations sowie Adressen der Check-ins
- Genaue Zeit des Check-ins an allen Locations

Die eigentlichen Personendaten hinter den Schlüsselanhängern konnten nicht direkt extrahiert werden, allerdings ist davon auszugehen, dass ein Bezug zur Nutzer:in sehr leicht herstellbar ist. Schlüsselanhänger müssen aktiv von einer Luca Location eingescannt werden, sodass im Moment des Scans eine eindeutige Zuordnung ermöglicht wird.

Wie gefährlich ist die Ausnutzung von LucaTrack?

Die Corona-Schutzverordnungen sehen in manchen Bundesländern eine strikte Dokumentationspflicht auch für höchst sensible Locations wie etwa religiöse Einrichtungen, Schulen oder Kitas, Selbsthilfegruppen oder politische Versammlungen vor. Die Dokumentation soll in manchen Bundesländern möglichst per Luca erfolgen, etwa in Mecklenburg-Vorpommern.

Die Preisgabe des Bewegungsprofils berührt daher einen besonders schützenswerten Bereich der Nutzer:innen. Da es sich bei den Schlüsselanhängern gemäß des Verwendungszwecks um persönliche Gegenstände handelt, ist unerheblich, dass die personenbezogenen Daten nicht direkt abgefragt werden können.

Darüber hinaus ist es möglich, Nutzer:innen in Zukunft bei jedem weiteren Check-in praktisch in Echtzeit zu überwachen. Überwachte Nutzer:innen sind so einem erhöhten Risiko von Stalking oder Missbrauch ausgesetzt.

Wie groß ist die Auswirkung dieser Sicherheitslücke?

Das betrifft derzeit alle Schlüsselanhänger im Luca-System. Aktuell (bis zum Zeitpunkt der Veröffentlichung) sind nach Angaben von Kreisen und Gemeinden über 100.000 Schlüsselanhänger in ganz Deutschland im Umlauf.

Wie lässt sich die Sicherheitslücke beheben?

Die Schlüsselanhänger im Luca System sollen mit ihrem QR-Code nur den Check-in ermöglichen, beinhalten aber zugleich den Schlüssel für den Zugriff auf ihre Daten. Diese Informationen sollten klar voneinander getrennt werden.

Empfehlung für die Nutzung von Schlüsselanhängern

Alle Schlüsselanhänger, die von der Sicherheitslücke betroffen sind, sind fachgerecht zu entsorgen.

Pressekontakt

Team LucaTrack
Bianca Kastl und Tobias Ravenstein
presse@lucatrack.de