Verwaltungsgericht Cottbus
Vom-Stein-Straße 27
03050 Cottbus
Telefax: 0355 4991-6499
Doppelte Ausführung
AZ: VG 8 K 518/21

Von:
Marcel Langner
[redacted]

Sehr geehrte Vorsitzende Richterin, Sehr geehrte Kammer,
es haben sich für das Verfahren neue Erkenntnisse ergeben, die ich Ihnen mitteilen möchte.

Luca in Brandenburg verfügbar

Inzwischen ist die Anwendung Luca in Brandenburg verfügbar. Sie ist meiner Einschätzung nach, trotz auch dort aufgetretener Schwachstellen, der Anwendung der Hochschule auf allen Gebieten überlegen (und wird trotzdem noch von IT Experten kritisiert). Die Anwendung der Hochschule hat sich bisher (außer mir) niemand genauer angeschaut.
Da ich nach meinem aktuellen Recherchestand ohne die Möglichkeit der Quellcodeeinsicht davon ausgehe, dass die Anwendung der Hochschule zum Schutz der personenbezogenen Daten nicht Stand der Technik nach Art. 32 DSGVO (hier kann nur Luca das Maß der Dinge sein) einsetzt, gehe ich folgerichtig auch davon aus, dass die Anwendung der Hochschule nicht mehr (bzw. noch nie) datenschutzkonform eingesetzt werden kann (konnte). Die Prüfung dieses Aspektes erachte ich nicht als Ihre Aufgabe in diesem Verfahren. Ich möchte damit aber aufzeigen, dass die Anwendung der Hochschule keine Alternative zu allen anderen (wirklich) am Markt vertretenen Anwendungen ist. Ein wirtschaftlicher Nachteil ist nun auch deshalb nicht erkennbar, weil ja Luca durch jeden in Brandenburg kostenfrei verwendet werden kann. Eine Argumentation mit eventuell entgangenen Einnahmen hinfällig.

Weitere Schwachstelle gefunden

Inzwischen habe ich eine weitere Schwachstelle in der Anwendung entdecken können, die ich Ihnen unverzüglich mitteilen werde. Ich habe damit aktuell Bedenken, da mir nicht bekannt ist, wie Sie in diesem öffentlichen Verfahren sicherstellen können, dass darüber keine unbefugten Dritten Kenntnis erhalten, damit die Hochschule Zeit hat, diese Schwachstelle zu beseitigen (Responsible Disclosure Frist: 01.09.2021). Die Hochschule hat seit 31.05.2021 Kenntnis über die Schwachstelle. Die Schwachstelle sehe ich als eine direkte Verletzung des Standes der Technik nach Art. 32 DSGVO und des Plausibilitätskriteriums von §1 (3) SARS-CoV-2-Eindämmungsverordnung. Ich bitte dazu um Rückmeldung Ihrerseits.

Open Source Strategie der Landesregierung

Die aktuelle Landesregierung von Brandenburg schreibt in ihrem Koalitionsvertrag:
„Der Wiederherstellung und Wahrung der digitalen Souveränität kommt im Zuge der zunehmenden Verwaltungsdigitalisierung in den kommenden Jahren eine entscheidende Rolle zu. Die Koalition wird sich dafür einsetzen, dass sich Einrichtungen der Landes-oder Kommunalverwaltung nicht in übermäßige Abhängigkeit zu einzelnen Herstellern begeben. Dazu wird die Koalition insbesondere auf die Einrichtung standardisierter bzw. offener Schnittstellen bei der Beschaffung von IT-Anwendungen setzen, die die Interoperabilität zum Datenaustausch von Anwendungen unterschiedlicher Hersteller sicherstellen. Wir ziehen die Beschaffung von Open-Source-Software der Beschaffung von proprietären IT-Produkten bei geeigneten Anwendungen vor.“

Vor diesem Hintergrund erscheint es mir nur folgerichtig, dass die Anwendung der Hochschule für Brandenburg keine Alternative darstellt. Ich möchte jedoch ausschließlich Einsicht in den Quellcode und seine verschiedenen Versionen nehmen. Auch wenn ich mir der Transparenz wegen eine Veröffentlichung als Open-Source wünschen würde, möchte ich diesen Wunsch nicht als Teil dieses Verfahrens verstanden wissen.
Dass ich selbst eine Weiterveröffentlichung nicht anstrebe und einen Vorschlag zur Urheberrechtswahrenden Einsicht gemacht habe, geht aus dem bisherigen Schriftverkehr hervor.

Konträre Auffassung zu führenden Wissenschaftlern

Die bisher durch die Hochschule vertretenen Auffassungen widersprechen ebenso der Meinung führender Wissenschaftler aus dem IT-Security und -Privacy Bereich (siehe Anlage 1).
Luca erfüllt inzwischen zumindest das Kriterium der Transparenz.
Die Anwendung der Hochschule erfüllt keines der dort geforderten Kriterien. Es gibt derzeit auch keine mir bekannte Rechtsgrundlage auf deren Basis diese Kriterien zu erfüllen sind. Es zeigt mir jedoch eine veraltete hinter den aktuellen Entwicklungen zurückbleibende Haltung der Hochschule, die ich dann auch in der Umsetzung der Anwendung befürchte. Die bisher gefundenen Schwachstellen sprechen jedenfalls dafür.

Andere Bundesländer

Auch die Landesbeauftragten der anderen Bundesländer müssen für Anfragen um Quellcodeeinsicht vermitteln. Sie finden in Anlage 2 die Stellungnahme der LfDI NRW, die meiner Lesart nach sowohl meiner Argumentation, als auch der der LDA Brandenburg entspricht.

[redacted] 13.06.2021
[redacted]

Anlage 1: Gemeinsame Stellungnahme zur digitalen Kontaktnachverfolgung

Digitale Werkzeuge, wie Apps zur Kontaktnachverfolgung, können einen unterstützenden Beitrag zur Bewältigung einer Pandemie leisten. Um ihr Potential voll entfalten zu können, müssen solche Werkzeuge zielgerichtet in eine Gesamtstrategie eingebettet werden und das Vertrauen der Bevölkerung genießen. Wenn durch ihre Einführung auch neue Risiken für Bürger:innen und Gesellschaftsgruppen entstehen, muss ihr Nutzen gegen diese Risiken abgewogen werden.

Vor einem Jahr haben mehr als 600 internationale Wissenschaftler:innen in einem offenen Brief an ihre Regierungen appelliert, Technologien zur digitalen Kontaktverfolgung verantwortungsbewusst und zielgerichtet zu entwickeln und einzusetzen. Dabei wurde die Einhaltung grundlegender Entwicklungsprinzipien gefordert, die in Deutschland mit der Corona-Warn-App größtenteils vorbildlich umgesetzt wurden:

- **Zweckbindung:** Das einzige Ziel muss die Pandemiebekämpfung sein. Eine Verknüpfung mit anderen Geschäftsmodellen, Anwendungsmöglichkeiten und Profitinteressen muss ausgeschlossen, idealerweise technisch unmöglich sein.
- **Offenheit und Transparenz:** Fachleuten, IT-Sicherheits- und Datenschutzexpert:innen muss frühzeitig die Möglichkeit gegeben werden, sich konstruktiv am Entwicklungsprozess zu beteiligen oder diesen unabhängig zu begutachten.
- **Freiwilligkeit:** Die Nutzung bestimmter Werkzeuge zur digitalen Kontaktverfolgung muss freiwillig sein. Bürger:innen, die das Werkzeug nicht benutzen möchten, dürfen nicht von sozialen Aktivitäten, dem Zutritt zu öffentlichen Gebäuden, Geschäften, usw. ausgeschlossen werden.
- **Risikoabwägung:** Die Beurteilung des Nutzens und der Risiken einer solchen Lösung muss im Vorfeld unabhängig und öffentlich geprüft werden können. Dies gilt ganz besonders dann, wenn der Effekt der technischen Lösung in wesentlichem Umfang auf dem Vertrauen der Bürger:innen basiert.

Der aktuell viel diskutierte Ansatz, digitale Hilfsmittel zur Kontaktnachverfolgung in öffentlichen Räumen und für Veranstaltungen einzubeziehen, erscheint sinnvoll. **Richtig** eingesetzt könnten sie Infektionsketten schneller unterbrechen und die Gesundheitsämter entlasten.

Konkrete funktionale Anforderungen für solch eine digitale Kontaktnachverfolgung wurden durch die verantwortlichen Behörden bislang nicht transparent und klar kommuniziert. Doch nur so ist es möglich effektive Lösungen zu entwickeln, welche einen sinnvollen Beitrag zur Eindämmung der Pandemie leisten können und dabei personenbezogene Daten nur in einem Umfang erheben, der auf das dafür notwendige Maß beschränkt ist.

LUCA

Das bereits in vielen Bundesländern eingesetzte LUCA-System erfüllt keine dieser Prinzipien. Es gibt keine technische Zweckbindung, sondern es wurden bereits weitere Geschäftsmodelle basierend auf LUCA diskutiert [1]. Damit entsteht eine Abhängigkeit von einem einzelnen Privatunternehmen mit Gewinnerzielungsabsicht als Betreiber des Systems. Es wurde ein intransparent entwickeltes System in Betrieb genommen und selbst leicht zu findende Sicherheitslücken konnten erst im laufenden Betrieb entdeckt werden. Wird die App Voraussetzung, um am öffentlichen Leben teilnehmen zu können oder gar von Corona-Schutzverordnungen vorgegeben [2], ist die Freiwilligkeit nicht gegeben, da ein *de facto* Nutzungszwang entsteht.

Der Nutzen des LUCA-Systems bleibt zweifelhaft, da sich die aktuelle Umsetzung im Wesentlichen auf die Automatisierung der manuellen Erfassung von Papierlisten beschränkt, die Auswertung jedoch weiter manuell durch die Gesundheitsämter erfolgt. Da mit LUCA falsche oder gar manipulierte Anmeldungen und Check-Ins leicht und in großer Zahl erzeugt werden können, entsteht zudem die Gefahr, dass die Belastung der Gesundheitsämter bei abnehmender Datenqualität zunimmt [3].

Gleichzeitig erfasst das LUCA-System in großem Umfang Bewegungs- und Kontaktdaten: wer war wo, mit welchen Personen am selben Ort, und wie lange. Die Daten werden zentralisiert und auf Vorrat bei einem Privatunternehmen gesammelt und gespeichert. Die viel beworbene doppelte Verschlüsselung der Kontaktdaten liefert schon deshalb nicht die versprochene Sicherheit, da sich Bewegungsprofile der Nutzer:innen allein aufgrund der anfallenden Metadaten erstellen lassen. Eine solche umfassende Datensammlung an einer zentralen Stelle birgt massives Missbrauchspotential und das Risiko von gravierenden Datenleaks [4].

Einzelne Systeme, die als zentrale Datenspeicher fungieren, sind attraktive und kaum vor Angriffen zu schützende Ziele. Selbst große Unternehmen sind nicht in der Lage, solche Systeme vollständig zu sichern. Es ist nicht zu erwarten, dass dies einem Start-Up, das bereits durch zahlreiche konzeptionelle Sicherheitslücken, Datenleaks und fehlendem Verständnis von fundamentalen Sicherheitsprinzipien [5] aufgefallen ist, besser gelingen sollte.

Fazit

Für den Erfolg von digitalen Hilfsmitteln zur Kontaktverfolgung ist eine breite Unterstützung der Bevölkerung essentiell. Das gilt insbesondere, wenn diese tief in die Privatsphäre der Bürger:innen eingreifen und in umfassender Weise vertrauliche Daten erheben. Das hierfür notwendige Vertrauen kann nur durch Transparenz und Privacy-by-Design, zum Beispiel durch echte Dezentralisierung, geschaffen werden. Sicherheit und Datenschutz sind elementare Voraussetzungen für die Akzeptanz und damit den erhofften Nutzen eines solchen Systems.

Es gibt bereits Systeme, die in diesem Sinne die Risiken für Bürger:innen auf ein Minimum reduzieren und dabei eine schnellere Benachrichtigung garantieren. Dies sind dezentrale Lösungen, wie sie in der Corona-Warn-App, NotifyMe (Schweiz), NHS COVID-19 (Großbritannien) und NZ COVID Tracer (Neuseeland) umgesetzt und bereits genutzt werden. Die mit dem LUCA System verbundenen Risiken erscheinen völlig unverhältnismäßig, da sie den erwarteten Nutzen deutlich überwiegen.

Wir empfehlen eindringlich die Rückbesinnung auf die oben genannten Prinzipien und deren Anwendung bei der Entwicklung digitaler Werkzeuge zur Kontaktnachverfolgung. Insbesondere sollte es aus unserer Sicht keinen *de facto* Zwang zur Nutzung einer Lösung geben, die diese Prinzipien eklatant verletzt.

Falls es konkrete Anforderungen gibt, die von bestehenden dezentralen Systemen noch nicht erreicht werden, dann müssen diese klar formuliert werden, so dass zielgerichtet entsprechende Erweiterungen entwickelt werden können. Auch in einem dezentralen und datensparsamen System können notwendige Informationen zur Pandemiebekämpfung erhoben und den Gesundheitsämtern zur Verfügung gestellt werden.

Vollständig mit Quellenangaben und Unterzeichnern hier: https://digikoletter.github.io/

Anlage 2: Stellungnahme der Landesbeauftragten für den Datenschutz und die Informationsfreiheit NRW

Mein Aktenzeichen 209.2.3.1.11-11328/20
Informationsfreiheitsgesetz Nordrhein-Westfalen (IFG NRW)

Antrag des Herrn … Antragsteller/in Antragsteller/in vom 21.10.2020 auf Zugang zu Kosten und Quellcode von Apps

Ihre E-Mail vom 11.05.2021

Sehr geehrte…,

vielen Dank für Ihre E-Mail vom 11.05.2021 bezüglich Ihrer weitergehenden Begründung zur Ablehnung. Hierzu teile ich Ihnen mit:

Zum einen begründen Sie Ihre Ablehnung nach § 8 IFG NRW, dem Schutz von Geschäfts- und Betriebsgeheimnissen damit, dass für die TU Dortmund zu befürchten sei, dass –im Falle einer Veräußerung- durch das vorherige Bekanntwerden ein wirtschaftlicher Nachteil entstünde. Wie der Antragsteller selber am 17.12.2020 erläuterte, ist dies nicht der Fall. Zudem ist Ihre Argumentation vor dem Hintergrund von Open Source in der Digitalstrategie der Landesregierung (https://www.wirtschaft.nrw/pressemitteilung/land-startet-pilotprojekt-fuer-open-source-software), eines eventuellen wirtschaftlichen Schadens nicht nachzuvollziehen. Außerdem müsste auch ein wahrscheinlicher Schaden eintreten können. Für eine Versagung auf der Grundlage des § 8 IFG NRW ist maßgeblich, inwieweit mögliche Mitbewerber tatsächlich einen wirtschaftlichen Nutzen aus der Offenlegung der begehrten Informationen ziehen können. Hier wäre eine weitere Konkretisierung erforderlich: Mit wem befindet sich die TU Dortmund im Wettbewerb? Inwiefern wäre eine Schwächung dieses Wettbewerbs möglich?

Ihre Bedenken auf der Grundlage des § 6 Satz 1 lit. a) IFG NRW sind nicht ausgeräumt, da der Quellcode der Corona-Warn-App und von Luca offen liegt. Diese Anwendungen bieten ähnliche Funktionalitäten wie die Komponente, bei der für den Fall der Veröffentlichung ein Sicherheitsproblem gesehen wird.
Die Herausgabe des Quellcodes könnte zudem an Bedingungen geknüpft werden kann (z. B. GPL-Lizenzierung), um die Nutzungsmöglichkeiten einzuschränken, insofern trägt das Argument des Eingriffs in die Nutzungs- und Verwertungsrechte hier nicht.

Ich bitte diese Argumente bei Ihren Überlegungen miteinzubeziehen. Bei Rückfragen können Sie mich in der Regel bis 14.00 Uhr erreichen.

Mit freundlichen Grüßen