TECHNISCHE DARSTELLUNG IN KURZFORM

Themen | Bereich	Vorwurf	Kategorie ● Missbrauch ● Check-in Daten ● Kontaktdaten	Trifft zu?	Kritikalität CVSS	Technische Begründung	Erweiterung geplant / umgesetzt
Gesundheitsamt	Falsche Daten durch nicht verifizierte Telefonnummern, Missbrauch Check-ins Peng! luci	●	JA	INFO	Grundsatz der Datensparsamkeit, Verifizierung auf Client Seite	Daten mit nicht korrekt verifizierten Telefonnummern werden aufgrund falscher Signatur nicht mehr an das GA übermittelt (31.5.2021)
Gesundheitsamt	Cyberangriff | CSV Importe	●	NEIN		React, OWASP,...plus SORMAS Schutz	Indirekte Mission zur Schulung der GAs im Umgang mit digitalen Mitteln ähnlich wie eMail
Gesundheitsamt	luca spart keine Zeit | Aufwendige Datenbearbeitung		NEIN		Diverse Datenfilter für RKI Empfehlung „Enge KP“, Auswahl der Orte, Filterung nach Bereichen, Überschneidungszeit	
Gesundheitsamt	Überprüfbarkeit der Echtheit der GA Anfrage durch Betreiber:in		JA	LOW	Bis zum vollständigen RollOut der Bundesdruckerei Zertifikate zwecklos, ab dann umgesetzt	GA Schlüssel kann durch Betreiber:in und Nutzer:in geprüft werden, um GA zu verifizieren (31.5.2021)
Gesundheitsamt	luca Update schreibt direkt auf GA Server	●	NEIN		Falsch. REST Schnittstellen werden nach Standard benutzt, Code Injection, CSV Injection verhindert und geprüft	
Schlüsselanhänger	Check-in mit unregistrierten Schlüsselanhängern	●	JA	LOW	Grundsatz Datensparsamkeit, keine Metadaten Erzeugung bei der Prüfung der Registrierung	Bloom Filter: Nicht verifizierte Schlüsselanhänger können nicht mehr zum Check-in bei Betreiber:innen verwendet werden (31.5.2021)
Schlüsselanhänger	Schlüsselanhänger Check-in Orte auslesbar	●	JA (nur wenn in Besitz eines Anhängercodes)	INFO	Art. 15 DSGVO Auskunftpflicht, neue Lösung mit Datenschutzbehörde gefunden zur Auskunftpflicht	Möglichkeit deaktiviert, bis im Frontend als Feature angeboten (umgesetzt)
Konzept	Falsches Konzept, u.a. zentrale Speicherung	● ●	NEIN		Begründung für zentrale Speicherung im Austausch mit den GAs Corona Verordnung, nach 30 Tagen gelöscht	
IT-Sicherheit	Mangelhafte, ungeprüfte Software	● ● ●	NEIN		ENRW Penetration Test; Datenschutzrechtliche Prüfung in diversen Ländern, DSK: System weist eine im Grunde nach tragfähige Architektur auf, Entspricht Anforderungen der GAs und im übrigen den Forderungen der Politik hinsichtlich mehr Erkenntnis, wo Infektionen stattfinden, Entlastung GAs, etc	
IT- Sicherheit | Metadaten	Bewegungsprofile | pseudonymisierte Nutzer:innen | Identifizierbarkeit durch IP Adressen	●	NEIN		Quellcode der Versionen nachvollziehbar veröffentlicht, zusätzlich Einsatz eines Reverse Proxy geplant	
IT- Sicherheit | Verschlüsselung	Ein zentraler Schlüssel für die GAs		NEIN		GA hat 3 individuelle Schlüssel, zentraler Tagesschlüssel nur für Zuordnung, plus individueller Schlüssel der Betreiber:innen zum Entsperren der Daten erforderlich	