Original-URL des Artikels: https://www.golem.de/news/datenleck-corona-kontaktliste-ungeschuetzt-im-internet-abrufbar-2007-149492.html **Veröffentlicht:** 07.07.2020 11:21 **Kurz-URL:** https://glm.io/149492

Datenleck

Corona-Kontaktliste ungeschützt im Internet abrufbar

Ein Datenleck bei der digitalen Corona-Kontaktliste von Lunchgate hat den Abruf der persönlichen Daten aller Gäste ermöglicht.

Ähnlich wie in Deutschland müssen Restaurants in der Schweiz die Kontaktdaten ihrer Gäste Corona-bedingt erfassen. Das geht nicht nur per Stift und Papier, sondern auch digital, beispielsweise mit dem Tischreservierungsdienst Foratable des Zürcher Startups Lunchgate, das diesen kurzerhand um eine Covid-19-Tracing-Funktion ergänzt hat. Doch dort konnte nicht nur der Restaurantbesitzer die Kontaktdaten einsehen, sondern prinzipiell jeder, der eine URL in einen Browser tippen kann. Entdeckt hatten die nicht existenten Sicherheitsvorkehrungen Sven Faßbender, Joël Gunzenreiner und Thorsten Schröder von der Sicherheitsfirma Modzero.

Ende Juni besuchte Gunzenreiner eine Bar, deren Betreiber QR-Codes bei Foratable generiert hatte. Einen solchen musste er scannen, seinen Namen und seine Telefonnummer in eine Webapplikation eintragen und der Datenschutzerklärung zustimmen. Anschließend wurden die Daten an den Server von Lunchgate gesendet und dem Sicherheitsforscher wurde eine Bestätigungsseite mit seinen Daten und dem besuchten Restaurant angezeigt.

Die URL der Bestätigungsseite endet mit der ID 174395. Lunchgate hatte die ID nicht zufällig generiert, sondern aufaddiert. Auch anderweitige Schutzmaßnahmen gab es nicht. Entsprechend konnte sich Gunzenreiner auch die Daten der Gäste mit den IDs 174396 und 174394 anzeigen lassen - und die aller anderen Gäste, die in den vergangenen Wochen den Tracing-Dienst von Lunchgate verwendet hatten. Name, Telefonnummer, Besuchszeit und teilweise die komplette Adresse der Gäste waren für alle einsehbar im Internet. Ein Datenleck.

Das Restaurant beziehungsweise die Bar konnten sie mit diesem Trick jedoch nicht auslesen: Angezeigt wurden nur die Daten der Besucher. Später gelang es den Sicherheitsforschern jedoch, auch die Daten der Gäste eines Restaurants einzusehen, inklusive des besuchten Tisches. Details hierzu wurden bisher nicht veröffentlicht.

"Lädt man sich die komplette Covid-19-Contact-Tracing-Datenbank herunter und korreliert sämtliche Datensätze, lassen sich über einen längeren Zeitraum möglicherweise Bewegungsprofile ganzer Gruppen erstellen", schreiben die Sicherheitsforscher in einem Blogeintrag. Wer mit wem ein Restaurant oder eine Kneipe besucht hatte, gar am gleichen Tisch saß.

<#youtube id="nD0MAnXHvq8"> Die Daten dürften auch für Kriminelle interessant sein: Sie *"wissen genau, wann eine Person wo war, sie haben die Telefonnummer und die Namen der Personen - mehr braucht es nicht, um potenziellen Opfern per Anruf unkluge Handlungen plausibel erscheinen zu lassen. Denn genau so funktioniert Social Engineering. Enkeltrick reloaded*", schreiben die Sicherheitsforscher.

Nach 14 Tagen wird gelöscht - außer aus dem Backup

Laut der Covid-19-Verordnung des Schweizerischen Bundesrates dürfen die erfassten Kontaktdaten zu keinem anderen Zweck verwendet werden und müssen nach 14 Tagen gelöscht werden. Doch die Sicherheitsforscher konnten am 2. Juli 2020 die Daten eines Restaurantbesuches vom 12. Juni 2020 einsehen.

Bei dem 21 Tage alten Eintrag handle es sich um eine Reservierung für der 25. Juni, erklärt Yves Latour von Lunchgate auf Nachfrage von Golem.de. Denn auch die Reservierungen, die über die Plattform abgewickelt werden, würden in der Corona-Tracing-Datenbank gespeichert. Über die von Modzero entdeckte Schwachstelle sei auch der Zugriff auf die Reservierungsdaten möglich gewesen.

Zudem werden die Daten weitere 10 Tage in einem Backup der gesamten Datenbank vorgehalten. Das widerspricht der grün hinterlegten Ankündigung beim Registrieren per QR-Code, dass die Daten "*in 14 Tagen wieder gelöscht*" würden. Auf die Daten könnten die Gäste zwar nicht mehr zugreifen, aber die Systemadministratoren hätten prinzipiell weiterhin Zugriff und auch die Polizei könnte die Daten anfragen, erklärt Latour. In Hamburg hatte die Polizei beispielsweise kürzlich die Kontaktliste eines Restaurants angefordert.

Am 3. Juli habe Modzero Lunchgate auf das Problem hingewiesen. Noch am selben Abend will die Firma laut einer Stellungnahme, die Golem.de vorliegt, das Problem behoben haben. Insgesamt nutzen das Tool 900 Betriebe. Rund 200.000 Gäste seien bisher erfasst worden, die Daten von 120.000 seien bereits wieder entfernt worden, teilt Lunchgate mit. Ein Anzeichen für einen Missbrauch der Schwachstelle gebe es derzeit nicht.

Besser mit Stift und Papier

Derweil geben die Sicherheitsforscher in ihrem Blog Tipps, wie es technisch besser gemacht werden kann. Die einfachste Lösung seien jedoch Stift und Papier, dann können Angreifer so oder so nicht die Daten aller Restaurants abgreifen, schreiben die Sicherheitsforscher.

Doch auch die Papiervariante hat ein Problem: Eine lange Liste, auf der sich jeden Tag alle Gäste eintragen, widerspricht zumindest dem Datenschutzrecht, das die Gäste die Daten gegenseitig einsehen können oder gar abfotografieren könnten. Doch auch hierfür gibt es eine Lösung: ein oder zwei Einträge pro Blatt.

Nachtrag vom 7. Juli 2020, 16:00 Uhr

Wir haben den Artikel um eine Stellungnahme von Lunchgate ergänzt. (mtr)

Verwandte Artikel:
Corona-Gästeliste: Gesundheitsbehörden auf der Suche nach Darth Vader
(18.09.2020, https://glm.io/150950)
Corona: Großbritannien erforscht Social Distancing mit KI-Kameras
(11.10.2020, https://glm.io/151441)
Coronakrise: Datenschutzbeauftragter prüft Fiebermessen im Apple Store
(12.05.2020, https://glm.io/148410)
Datenschutz: Amazon-Insider gab Mailadressen weiter
(28.10.2020, https://glm.io/151769)
Windows XP Leak: XP hatte eine geheime MacOS-ähnliche Oberfläche
(26.09.2020, https://glm.io/151129)
