Ctrl-Alt-R

#Lunchgate

Aus Angst vor Missbrauch verweigern Restaurantgäste ihre Kontaktangaben. Doch wie sicher waren die Daten eigentlich vor der Pandemie?

Von Adrienne Fichter, 28.08.2020

In der Pizzeria einmal ungeniert in die Runde husten: In normalen Zeiten ist das unanständig, in diesen grenzt es an fahrlässige Körperverletzung. Das Covid-19-Ansteckungsrisiko in Restaurants und Bars ist real – darum ist es wichtig, potenziell Infizierte nachverfolgen und testen zu können.

Unterdessen ist allerdings klar: Beim Erfassen dieser Kontaktdaten funktioniert das Prinzip Freiwilligkeit und Eigenverantwortung nicht wirklich. Deshalb fordern nun die ersten Kantone Verbindlichkeit: Restaurants und Bars in Bern und Zürich beispielsweise müssen die Daten der Gäste für das Contact-Tracing verbindlich einfordern.

Viel wurde in den vergangenen Monaten darüber diskutiert, in welcher Form Restaurants persönliche Informationen sammeln dürfen. Nach den Öffnungen vom 11. Mai lagen noch etliche Listen auf den Tischen, auf denen sich Gäste eintragen konnten. Betonung auf *konnten*. Doch das Restaurantpersonal war es bald leid, die Gäste ständig auffordern zu müssen. Zeit verstrich, und die Listen verschwanden wieder von den Tischen.

Viele Gäste weigern sich, weil sie nicht wissen, was die Restaurants sonst noch damit anstellen und wie lange die Daten aufbewahrt werden.

Die Ironie dabei ist allerdings: Schon vor Corona wurden solche Daten weder sicher aufbewahrt noch gelöscht, wie eine Datenauskunft beim Platzhirsch unter den Schweizer Reservationstools zeigt – Lunchgate.

Klingt gut, aber stimmt es auch?

Etliche Gastronomie-Plattform-Betreiber werben damit, Reservationen datenschutzkonform durchzuführen. Auch das Zürcher Start-up Lunchgate weist auf die Covid-19-Schutzverordnung hin. Wer also via diese Plattform einen Tisch bucht, kann vom Contact-Tracing-Team kontaktiert werden. Dabei wird der Gast darauf hingewiesen, dass seine Daten 14 Tage aufbewahrt und danach gelöscht würden.

Klingt gut, stimmt aber nicht – das deckte Anfang Juli das IT-Sicherheitsunternehmen Modzero auf. In einem unterhaltsam geschriebenen Blogbeitrag schildern die drei IT-Experten Sven Fassbender, Joël Gunzenreiner und Thorsten Schröder ihre Recherchen. Sie fanden heraus, dass Lunchgate nicht nur die 2-Wochen-Frist nicht einhält, sondern darüber hinaus die gespeicherten Gästedaten für alle frei einsehbar aufbewahrt.

Wie das möglich ist?

Bei der Reservation erscheint die persönliche ID-Nummer in der URL, also der Webadresse, der Bestätigungsseite. Das bezeichnen die IT-Profis als ersten grundlegenden Fehler. Sie beschreiben diese Schwachstelle als eine sogenannte IDOR-Schwachstelle (Insecure Direct Object Reference). Grund sei ein «schwaches Zugriffsrechtsmanagement».

Darüber hinaus war die ID-Zuweisung alles andere als clever umgesetzt. So konnten auch technisch nicht bewanderte Personen einfach herausfinden, wer wie reservierte. Man experimentiere ein wenig mit der URL und tausche ein paar Ziffern aus. Statt der erhaltenen ID 174396 tippten die Blogger in ihrer Recherche zum Beispiel 174394 ein – und erhielten die Reservation einer wildfremden Person angezeigt, samt ihrer Telefonnummer, teilweise ihrer Adresse sowie der Besuchszeit und dem gebuchten Tisch. Dabei stellten die Modzero-Experten auch fest, dass die Daten über eine Woche länger gespeichert waren als die erlaubten 14 Tage.

Modzero kontaktierte Lunchgate vor der Publikation des Blogbeitrags.

Das Start-up versicherte am 3. Juli, «dass die IDOR-Schwachstellen behoben seien». Die Modzero-Blogger merkten am Schluss ihres Artikels an: «Zur 14-Tage-Löschfrist hiess es, hier bestünden keine Probleme.»

Doch wie handhabte Lunchgate das alles eigentlich vor der Pandemie und dem Contact-Tracing? Das wollte ich genauer wissen.

Was der Datenschützer dazu sagt

Ich benutzte Lunchgate selber mehrfach für Restaurantreservationen und verlangte beim Start-up kurz nach Publikation des Modzero-Beitrags alle über mich gespeicherten Daten. Der Managing Partner Yves Latour antwortete umgehend und versicherte eine umfassende Datenauskunft, für Schweizer Verhältnisse ist das erst einmal vorbildlich. Ein paar Tage später erhielt ich die Daten in kopierter Tabellenform – und staunte.

Aufgelistet sind alle meine Restaurantbesuche, Reservationsuhrzeiten, meine Telefonnummer und die E-Mail-Adresse sowie die Angaben, wie viele Gäste ich angemeldet hatte, und alle Bewertungen, die ich abgegeben habe.

All dies bis zurück ins Jahr 2015.

Ein Blick in die Nutzungsbedingungen des Foratable-Reservationstools (so heisst das Buchungssystem von Lunchgate für Gäste) zeigt: Lunchgate nennt tatsächlich kein Ablaufdatum zur Speicherung der Daten. «Diese Daten sind für die Durchführung einer Reservation notwendig und werden ausschliesslich dem Restaurant zur Weiterverarbeitung zur Verfügung gestellt und bei der Lunchgate AG gespeichert.»

Sind solche Nutzungsbedingungen datenschutzkonform? Weshalb bewahrt Lunchgate die Daten nach dem Restaurantbesuch über fünf Jahre lang auf?

Eine klare Antwort auf diese Frage habe ich vom Zürcher Start-up nicht erhalten. Lunchgate-Managing-Partner Yves Latour erklärt lediglich: «Unsere Kunden, die Gastronomen, führen Gästedatenbanken, um zu sehen, welche Gäste oder Stammgäste seit wann und wie oft zu Besuch kommen.»

Der eidgenössische Datenschützer kritisiert diese Bestimmungen. EDÖB-Sprecherin Silvia Böhlen sagt: «Lunchgate muss die Grundsätze der Zweckbindung, der Transparenz und der Verhältnismässigkeit wah-

ren. Nach einer ersten Einschätzung auf Basis der auffindbaren Informationen genügen die Nutzungsbestimmungen den gesetzlichen Anforderungen nicht in jedem Fall und müssten ausgebaut werden.»

Ein klares No-Go aus Sicht des eidgenössischen Datenschützers sind die Nutzungsbedingungen für die Restaurants, also die Kunden der Plattform.

Denn Lunchgate bedingt sich etliche Haftungsrisiken weg, mit Sätzen wie: «Ausserdem übernimmt Lunchgate keine Verantwortung und gibt keine Garantie dafür ab, dass die Funktionen auf Lunchgate.ch nicht unterbrochen werden oder fehlerlos sind, dass Fehler behoben werden oder dass Lunchgate.ch oder der jeweilige Server frei von Viren oder schädlichen Bestandteilen ist.»

Man werde ein Auge auf Lunchgate haben, so EDÖB-Sprecherin Böhlen.

Ich habe zwischenzeitlich die Löschung meiner Daten beantragt. Lunchgate bestätigte vor ein paar Tagen die Entfernung meiner Historie.

Die von Modzero aufgedeckte unsichere Handhabung der Gästedaten im Juli hatte in der Schweiz eine Handvoll Medienberichte zur Folge. In Deutschland könnte der Fall sogar ein juristisches Nachspiel haben, wo er weit mehr Aufsehen erregte als hierzulande. «In der Schweiz begegnet man der Herausforderung von Corona-Kontaktlisten mit der Sicherheitsattitüde der 90er», schreiben die «Logbuch:Netzpolitik»-Podcaster Linus Neumann und Tim Pritlove.

Fazit: Die Debatte um die Gästedaten-Speicherung in der Schweiz idealisiert die Zeit vor Corona. Zu Unrecht, denn diese Pandemiemassnahme ist nicht eine Abweichung von einem zufriedenstellenden Status quo. Der Datenschutz war bei vielen Schweizer Unternehmen bereits vor Corona eingeschränkt – wenn überhaupt vorhanden.

Die gute Nachricht: Die Pandemie macht diese Defizite nun endlich sichtbar.

Zu Tisch bitte, es ist angerichtet.