Datenleck im Legoland

Legoland-Hotelbuchungen der letzten sieben Jahre einsehbar

Die Buchungsseite für Übernachtungen im bayerischen Legoland spuckte bereitwillig die Daten etlicher tausend Gäste aus. Die Buchungsbestätigungen waren online über eine URL mit fortlaufender Nummer einsehbar. Informiert wurden die Kunden auch im Nachhinein nicht.


LEGOLAND HOLIDAYS

LEGOLAND Holidays Deutschland
LEGOLAND Allee 1
89312 Günzburg

BESTÄTIGUNG

KD.NR.: [redacted]

Buchungsnummer: [redacted]
Buchungsdatum [redacted]
Bearbeiter: Online LEGOLAND Hol

Frau
[redacted]
Deutschland

Reisezeitraum: [redacted]22 - [redacted]22

Wir bedanken uns für Ihre Buchung und bestätigen Folgendes.

Teilnehmer: 4 Personen
001 [redacted]
002 [redacted]
003 [redacted]
004 [redacted]

Datum	Dauer	Anz. Pax	Leistungen	Einzelpreis
[redacted]22 - [redacted]22		1	Room Only	

Von Marie-Claire Koch

Bei dem zur Merlin Entertainments Group gehörenden Legoland Deutschland Resort im bayerischen Günzburg waren etliche tausend Datensätze aus allen seit Mai 2015 getätigten Buchungen öffentlich durch eine trivial ausnutzbare Sicherheitslücke einsehbar. Darauf machte uns ein Leser aufmerksam, woraufhin wir den Fall untersuchten.

Bei einer Buchungsanfrage muss man die Anzahl der reisenden Erwachsenen sowie die Anzahl der Kinder in einem Formular eintragen. Auch die Namen der Mitreisenden und die Anschrift des Buchenden sowie der gewünschte Reisezeitraum werden durch das System abgefragt. Der Leser wurde misstrauisch, als er im Anschluss an seine Buchung die PDF-Datei mit der Buchungsbestätigung über eine auffällige URL abrufen sollte.

Die URL hatte folgendes Schema: https://mylogin.legolandholidays.de/api/booking/document/**123456**/0/CONFIRMATION. Besonders die mehrstellige Zahl in der URL ließ ihn genauer hinschauen. Sie entsprach seiner Buchungsnummer. Er überlegte, ob auch andere Buchungen über eine veränderte Version des Links einsehbar sind.

Also probierte er eine kleinere Zahl im Browser aus und erhielt erneut Zugang zu einer PDF-Datei. Diesmal allerdings nicht für seine eigene Buchung, sondern mit der Adresse und den Namen mehrerer anderer Personen. Angaben zur Buchung wie den Preis und die erworbene Leistung enthielt das Dokument ebenfalls. Daraufhin wandte sich der Leser an die c't-Redaktion.

Wir konnten das Leck nachvollziehen und stichprobenartig Buchungen fremder Personen abrufen. Mit jeder Buchung wurde dem Kunden eine fortlaufende Zahl zugewiesen, die sowohl im PDF-Dokument als Buchungsnummer als auch in der URL zu sehen war. Ein Zugriffsschutz war nicht vorgesehen, das Durchzählen der Nummer reichte aus, um beliebige PDF-Dateien einzusehen.

Das älteste Dokument, das wir finden konnten, stammt von 2015. Begonnen mit der Nummer 100001 und endend mit Nummer 604104 waren auf diese Weise mutmaßlich mehrere hunderttausend Datensätze öffentlich einsehbar. Und während unserer Recherche kamen laufend neue Datensätze hinzu. Um die Daten einzusammeln, hätten Unbefugte mit einem simplen Skript oder `curl`-Aufruf sämtliche PDFs abgreifen können.

Trivialer Fehler

Dieser und ähnliche triviale Fehler führen immer wieder zu verheerenden Datenlecks. Persönliche Daten sollten stets gut geschützt und niemals über eine URL abrufbar sein, die nach einem vorhersehbaren Muster generiert wurde. Im besten Fall ist der individuelle Teil der URL lang und zufällig generiert. So eignen sich zum Beispiel sogenannte Universally Unique Identifier (UUID) für diesen Zweck [1]. Zudem sollte der Zugriff auf die URL möglichst durch eine Authentifizierung geschützt sein.

Wir informierten Legoland über die in der Datenschutzerklärung hinterlegte E-Mail-Adresse. Am nächsten Tag funktionierten die Zugriffe auf die Buchungsbestätigungen nicht mehr. Einige Tage später bekamen wir eine Antwort, in der Merlin Entertainments die Deaktivierung des PDF-Abrufs bestätigte. Außerdem sei der Datenschutzverstoß der DSGVO entsprechend beim Bayerischen Landesamt für Datenschutzaufsicht gemeldet worden.

Kunden werden nicht informiert

Merlin erklärte gegenüber c't, dass „eine umfassende Untersuchung durchgeführt und zusätzliche Sicherheitsmaßnahmen ergriffen [werden], um unbefugten Zugriff auf Buchungsdaten zukünftig zu verhindern". Seine Kunden hat das Unternehmen nicht informiert, weil es bei der „eingehenden Risikobewertung des Datenschutzvorfalls zu dem Ergebnis gekommen [ist], dass dieser Vorfall ein geringes Risiko für die betroffenen Personen darstellt." Als Begründung nannte die Merlin Entertainments Group, dass „zu keinem Zeitpunkt [...] auf Bank- oder Kreditkartendaten zugegriffen oder diese entwendet" werden konnten. *(rei@ct.de)* **ct**

Literatur

[1] Jan Mahn, Zufall schlägt das System, Ein Plädoyer für UUIDs in Datenbanken, c't 6/2022, S. 138