

DER LANDESBEAUFTRAGTE FÜR DEN DATENSCHUTZ NIEDERSACHSEN INFORMIERT:



Wichtige Information an Beherbergungsbetriebe und Campingplätze in Niedersachsen

Bei einem erfolgreichen Cyberangriff auf großen Buchungsdienstleister sind erneut Buchungsdaten von Gästen abgeflossen. Eine Information, was Betriebe in solchen Fällen tun müssen – mit praktischer Checkliste.

Der Landesbeauftragte für den Datenschutz Niedersachsen (LfD) richtet sich mit diesem Informationsschreiben an alle Übernachtungsbetriebe im Land, also Hotels, Campingplätze, Ferienwohnungsvermietungen und Herbergen.

Derzeit kommt es im Zusammenhang mit Hotel- und Übernachtungsreservierungen zu betrügerischen Kontaktaufnahmen mit den Gästen, insbesondere über SMS, E-Mail, WhatsApp und andere Messenger-Dienste. Dabei verfügen die Absender über die tatsächlichen Buchungsinformationen, was die Nachrichten besonders authentisch wirken lässt.

Hintergrund sind mehrere IT-Sicherheitsvorfälle bei größeren technischen Dienstleistern insbesondere zur Buchungsverwaltung, die von Hotels, Campingplätzen und anderen Übernachtungsbetrieben bundesweit genutzt werden. Auch zahlreiche Unternehmen in Niedersachsen sind betroffen – dies belegt eine signifikant gestiegene Zahl von Datenpannenmeldungen beim LfD. Über Schwachstellen konnten Unbefugte auf Buchungsinformationen wie Hotelname, Buchungsnummer, Name, E-Mail-Adresse und Telefonnummer der Gäste, An- und Abreisedatum sowie den Gesamtbetrag der Buchung zugreifen. Grundsätzlich ist zu beobachten, dass erfolgreiche Cyberangriffe auf externe IT-Dienstleister zunehmen.

Was müssen Sie als Verantwortliche wissen?

Auch wenn externe Dienstleister etwa zur Buchungsverwaltung genutzt werden, bleiben Hotels und andere Übernachtungsbetriebe gemäß Datenschutz-Grundverordnung (DSGVO) verantwortlich für die Daten ihrer Gäste. Die Dienstleister müssen Sie über etwaige Vorfälle unverzüglich informieren. Achten Sie daher auf eingehende Nachrichten Ihrer Dienstleister.

Erfahren Sie von einer Datenpanne, sind Sie verpflichtet, Ihre Gäste ebenfalls umgehend zu benachrichtigen. Diese Benachrichtigung muss an alle Gäste gerichtet werden, die betroffen sein könnten, nicht nur an solche, die gefälschte Nachrichten erhalten haben.¹ Zu Ihren Pflichten zählen ferner auch die Meldung der Datenpanne an die zuständige Datenschutzaufsichtsbehörde, die Benennung einer Ansprechperson für die Gäste und die Dokumentation des Vorfalls.

Checkliste: Was muss ich tun, wenn mein Betrieb betroffen ist?

1. Benachrichtigen Sie Ihre Gäste über den Vorfall und den (möglichen) Abfluss ihrer Daten, damit diese vor den Phishing-Angriffen gewarnt sind. In den meisten Fällen stellen die Dienstleister Ihnen eine Vorlage zur Verfügung.
2. Reichen Sie eine Meldung über die Datenpanne beim LfD ein. Nutzen Sie dafür das Online-Formular für Datenpannenmeldungen gem. Art. 33 DSGVO – das Formular finden Sie auf [unserer Webseite](#).
3. Sensibilisieren Sie alle Mitarbeitenden im Allgemeinen für das Thema Phishing sowie zu bekannten Vorfällen und weisen Sie auf die aktuelle Gefährdungslage hin. Links oder Anhänge aus verdächtigen E-Mails dürfen nicht geöffnet werden. Ihre Mitarbeitenden sollten den Gästen gegenüber auskunftsfähig sein, insbesondere wenn bereits Daten eingegeben wurden oder entsprechende Zahlungen erfolgt sind (siehe unten). Mitarbeitende sollten bei Gästeanfragen die Buchung im offiziellen Buchungssystem und die entsprechenden Kontaktwege intern prüfen.

¹EDSA-Leitlinien 9/2022 für die Meldung von Verletzungen des Schutzes personenbezogener Daten gemäß der DSGVO Version 2.0, abrufbar unter https://www.edpb.europa.eu/documents/guideline/guidelines-92022-on-personal-data-breach-notification-under-gdpr_de

4. Es müssen alle Passwörter der Benutzerkonten, die mit dem kompromittierten Dienstleister im Zusammenhang stehen, geändert werden. Es sollten neben dem Zugriff auf die betroffenen Dienste auch alle angeschlossenen Systeme überprüft werden.
5. Technische Protokolle sollten auf ungewöhnliche Anmeldeversuche oder Systemzugriffe kontrolliert werden.
6. Überprüfen Sie, ob Ihr Backup-System dem aktuellen technischen Standard entspricht und bessern Sie gegebenenfalls nach.
7. Grundsätzlich sollte für alle Systeme eine Zwei-Faktor-Authentifizierung eingerichtet werden.
8. Richten Sie eigene Warnhinweise auf Ihren Kommunikationskanälen ein, um Gäste für Phishing zu sensibilisieren und vor möglichen Angriffen zu warnen.

Stichpunkte für die Kommunikation mit betroffenen Gästen

1. Vorfall erläutern

Im Zusammenhang mit den bekannten IT-Sicherheitsvorfällen bei den Dienstleistern erhalten manche Gäste täuschend echte Nachrichten mit ihren korrekten Reisedaten und werden aufgefordert, angeblich fehlende Daten (z. B. Kreditkartennummern) beispielsweise in Formularen zu ergänzen oder Zahlungen zu leisten.

2. Risiko erklären

Die erbeuteten Buchungsdaten können Kriminelle für Phishing-Nachrichten per SMS, E-Mail und Messenger wie WhatsApp nutzen. Wenn Gäste auf diese Nachrichten antworten oder gar Geld überweisen, drohen nicht nur finanzielle Schäden, sondern auch weitere Risiken wie Identitätsdiebstahl oder Erpressungsversuche.

3. Wenn Gäste noch keine Phishing-Nachrichten erhalten haben

Mitarbeitende sollten die Gäste auf folgende Punkte hinweisen:

- Prüfen Sie eingehende E-Mails und Nachrichten besonders sorgfältig auf Absenderadresse oder ungewöhnliche Zahlungsaufforderungen.
- Seien Sie in jedem Fall vorsichtig, wenn ein Hotel Sie per E-Mail oder Messenger-Dienst darum bittet, weitere Informationen anzugeben oder eine Zahlung anzuweisen. In der Regel haben Sie bei der Buchung bereits alle erforderlichen Daten angegeben. Kontaktieren Sie im Zweifel das Hotel über eine offizielle Telefonnummer oder Adresse. Überweisen Sie nie Geld auf Grundlage einer Nachricht, deren Echtheit Sie nicht eindeutig überprüfen können.
- Geben Sie nie persönliche Daten oder Zahlungsinformationen über zugesandte Links preis.
- Wenn Sie unsicher sind, ob die Nachricht echt ist, versichern Sie sich am besten durch einen Anruf bei dem betreffenden Hotel.

4. Wenn Gäste wegen erhaltener Phishing-Nachrichten bei Ihnen nachfragen

Wenn Gäste betrügerische Nachrichten empfangen haben, sollten sie ausdrücklich durch die Mitarbeitenden darauf hingewiesen werden, keinerlei Daten einzugeben oder Zahlungen vorzunehmen. Bei bereits eingegebenen Daten oder getätigten Zahlungen sollten die Gäste zudem darüber informiert werden, umgehend ihre jeweiligen Bank- bzw. Zahlungsdienstleister und die Polizei zu kontaktieren. Zudem sollten sie schnellstmöglich etwaige Zugangsdaten über die offizielle Webseite bzw. App ändern.

Praxistipp: Notfallplan

In den Betrieben müssen derartige Vorfälle entsprechend intern erfasst und dokumentiert sowie an die Datenschutzaufsichtsbehörde gemeldet werden. Cyberangriffe nehmen zu. Haben Sie daher einen Notfallplan zur Hand: Wer ist im Falle eines Cyberangriffs erreichbar und entscheidet ggf. über die Abschaltung der Systeme? Was sind die nächsten Schritte? Weitere Informationen und hilfreiche Tipps finden Sie auch im [Praxisleitfaden „Gästedaten sicher verarbeiten“ – Datenschutzkonforme Verarbeitung personenbezogener Daten in Beherbergungsbetrieben](#) des LfDI MV.

Stand: Oktober 2026