Sehr geehrte Gäste,

bei unserem Reservierungsdienstleister RESERViSiON ist es zu einem Cyberangriff gekommen. Dabei wurden personenbezogene Daten von Gästen unbefugt abgerufen. Auch Daten zu Ihrer Tischreservierung bei uns können betroffen sein.

Wir bedauern diesen Vorfall sehr. Uns ist bewusst, dass diese Nachricht Sorgen auslösen und Fragen aufwerfen kann. Wir möchten Ihnen deshalb erklären, was bisher bekannt ist, welche Folgen möglich sind und wie Sie sich schützen können.

**Was ist passiert?**

Für die Verwaltung unserer Tischreservierungen nutzen wir das System der RESERViSiON GmbH, Seestr. 29, 64354 Reinheim. Das Unternehmen verarbeitet die dafür erforderlichen Gästedaten in unserem Auftrag.

Nach den bisherigen Untersuchungsergebnissen verschaffte sich ein Angreifer am 8. November 2026 über ein Kundenkonto Zugang zum Reservierungssystem. Eine Sicherheitslücke ermöglichte ihm, auch Reservierungsdaten anderer Betriebe abzurufen. Am 8. und 9. November 2026 wurden auf diesem Weg Gästedaten in großem Umfang kopiert.

Seit dem 9. November 2026 sind betrügerische E-Mails bekannt, in denen echte Reservierungsangaben verwendet wurden. Gäste wurden darin zu Zahlungen oder zur Eingabe von Kreditkartendaten auf gefälschten Internetseiten aufgefordert. Teilweise wurde behauptet, eine Reservierung müsse noch bestätigt werden oder werde andernfalls storniert.

Bei mehreren Betrieben wurden außerdem Zugangsdaten für den E-Mail-Versand missbraucht. Deshalb können solche Nachrichten auch von echten E-Mail-Adressen der Restaurant- und Hotelbetriebe stammen. Eine bekannte Absenderadresse und zutreffende Reservierungsangaben sind daher kein sicherer Beleg für die Echtheit einer Nachricht.

**Welche Ihrer Daten können betroffen sein?**

Nach den Angaben von RESERViSiON können insbesondere folgende Daten betroffen sein, soweit diese im Reservierungssystem gespeichert wurden:

- Vor- und Nachname, E-Mail-Adresse, Mobil- und Festnetznummer sowie Firmenangaben.
- Angaben zur Tischreservierung, insbesondere Datum, Uhrzeit und Personenzahl.
- Allergieangaben und weitere Reservierungsoptionen.

Der unbefugte Datenabruf wurde nach den technischen Untersuchungen festgestellt. Welche einzelnen Gästedatensätze kopiert wurden, lässt sich derzeit jedoch nicht abschließend ermitteln. Deshalb müssen wir auch Ihre im System gespeicherten Reservierungsdaten als potenziell betroffen behandeln.

Es können sowohl vergangene als auch zukünftige Reservierungen betroffen sein. Eine Beschränkung auf Online-Reservierungen ist nach dem bisherigen Kenntnisstand nicht möglich.

**Welche möglichen Folgen bestehen für Sie?**

Die erlangten Informationen können genutzt werden, um betrügerische Nachrichten besonders glaubwürdig zu gestalten. Die Täter kennen möglicherweise Ihren Namen und Einzelheiten Ihrer Reservierung. Dadurch kann der Eindruck entstehen, eine Nachricht stamme tatsächlich von uns oder unserem Reservierungsdienstleister.

Das Ziel kann sein, Sie zu einer Zahlung zu bewegen oder weitere persönliche Daten zu erlangen. Insbesondere Kreditkarten- und andere Zahlungsdaten können auf diesem Weg abgefragt werden. Daraus können finanzielle Schäden und weitere Betrugsversuche entstehen.

Soweit Sie Allergieangaben hinterlegt haben, können außerdem Informationen zu Ihrer Gesundheit unbefugt bekannt geworden sein.

**Was wurde bisher unternommen?**

Nach Angaben von RESERViSiON hat der beauftragte IT-Dienstleister die erkannten Angreiferadressen gesperrt. Betroffene Benutzerkonten wurden deaktiviert und deren aktive Sitzungen beendet. Zusätzlich wurden technische Zugänge eingeschränkt und automatisierte Massenabrufe begrenzt.

Beginnend ab dem 9. November 2026 hat RESERViSiON bereits eine erste Warn-E-Mail an zahlreiche Gäste versendet. Mit diesem Schreiben erhalten Sie ergänzende Informationen zum Datenschutzvorfall und zu Ihren Schutzmöglichkeiten.

Die Untersuchung ist noch nicht abgeschlossen. Nach dem zuletzt mitgeteilten technischen Stand ist eine vollständige Behebung der Sicherheitslücken noch nicht bestätigt. Weitere erforderliche Maßnahmen betreffen die Absicherung der Anwendung und den Austausch gefährdeter Zugangsdaten.

Die Passwörter beim E-Mail-Anbieter wurden geändert, unser Personal wurde informiert.

Wir haben den Vorfall am 10.11.2026 der für uns zuständigen Datenschutzaufsichtsbehörde gemeldet.

**Was sollten Sie jetzt beachten?**

Bitte seien Sie bei Nachrichten zu Ihrer Reservierung besonders aufmerksam. Das gilt auch für mögliche Kontaktaufnahmen per SMS, Messenger oder Telefon.

- Öffnen Sie keine Links oder Anhänge in verdächtigen Nachrichten. Geben Sie auf darüber aufgerufenen Internetseiten keine persönlichen Daten, Passwörter oder Zahlungsinformationen ein.
- Leisten Sie keine Zahlungen aufgrund solcher Nachrichten. Lassen Sie sich auch durch die Androhung einer Stornierung nicht unter Druck setzen.
- Fragen Sie im Zweifel direkt bei uns nach. Verwenden Sie dafür die Ihnen bereits bekannten Kontaktdaten oder die Angaben auf unserer offiziellen Internetseite. Nutzen Sie nicht die Kontaktdaten aus einer verdächtigen Nachricht.

Haben Sie bereits Kreditkartendaten eingegeben oder eine Zahlung geleistet? Kontaktieren Sie bitte unverzüglich Ihre Bank oder Ihren Kreditkartenanbieter. Lassen Sie eine betroffene Karte sperren und klären Sie, welche weiteren Schritte erforderlich sind. Prüfen Sie Ihre Kontoauszüge und Kreditkartenabrechnungen auf unbekannte Umsätze.

Bewahren Sie verdächtige Nachrichten und gegebenenfalls Zahlungsbelege für die weitere Aufklärung auf.

**An wen können Sie sich wenden?**

Für Fragen zum Vorfall und zum Schutz Ihrer Daten erreichen Sie unsere Anlaufstelle unter:

Restaurant Cafe Madrid, Herr Andreas Rau

E-Mail: reservierung@cafe-madrid.de

Telefon: 0341-9938813

Sollten sich weitere wesentliche Erkenntnisse zu Ihrer Betroffenheit oder zu erforderlichen Schutzmaßnahmen ergeben, werden wir Sie darüber informieren.

Wir bedauern die entstandene Verunsicherung und die möglichen Belastungen für Sie. Bitte nehmen Sie die Warnhinweise ernst und wenden Sie sich bei Zweifeln an uns.

Mit freundlichen Grüßen