

PRESSEINFORMATION

des Österreichischen ReiseVerbandes (ÖRV)

ÖRV: Cyberangriffe treffen Reisebüros ins Herz

Neuer Cybersecurity-Leitfaden zeigt Reiseunternehmen, wo die größten Risiken liegen – und mit welchen Maßnahmen sie sich Schritt für Schritt schützen können

Wien, Oktober 2026 – Reisebüros sind für Cyberkriminelle attraktive Ziele: Sie verarbeiten täglich persönliche Kundendaten, Zahlungsinformationen und Buchungsdaten und arbeiten mit zahlreichen externen Partnern und digitalen Systemen. Gleichzeitig sorgen zeitkritische Buchungen und Umbuchungen für zusätzlichen Druck im Arbeitsalltag. Ein erfolgreicher Cyberangriff kann daher weitreichende Folgen haben – vom Ausfall von Buchungssystemen über finanzielle Schäden bis zum Verlust sensibler Kundendaten.

Der Österreichische ReiseVerband (ÖRV) unterstützt seine Mitglieder deshalb mit einem praxisorientierten Leitfaden zur **Cybersecurity im Reisebüro**. Im Mittelpunkt steht nicht die perfekte IT-Sicherheit auf einen Schlag, sondern ein realistischer Weg: **Risiken erkennen, Maßnahmen priorisieren, Mitarbeitende sensibilisieren und die Sicherheit regelmäßig überprüfen.**

„Cybersecurity ist längst keine reine IT-Frage mehr. Sie betrifft den gesamten Reisebürobetrieb und vor allem auch den Schutz unserer Kunden“, betont Mag. Eva Buzzi, Präsidentin des ÖRV. „Mit einfachen Maßnahmen lässt sich bereits viel erreichen. Unser Leitfaden soll unseren Mitgliedern dabei helfen, die richtigen Schritte in der richtigen Reihenfolge zu setzen.“

Die „Quick Wins“ für Reisebüros

Einige der wirksamsten Maßnahmen sind vergleichsweise einfach umzusetzen. Dazu gehören starke individuelle Passwörter, Zwei-Faktor-Authentifizierung, regelmäßige Updates, eingeschränkte Zugriffsrechte, Netzwerksegmentierung und sichere Backups.

Besonders wichtig: **Keine gemeinsamen Benutzerkonten und keine weitergegebenen Passwörter.** Jeder Mitarbeiter sollte über einen eigenen Zugang verfügen. Damit lassen sich Zugriffe nachvollziehen und beim Ausscheiden eines Mitarbeiters gezielt deaktivieren.

Auch externe Partner gehören auf den Prüfstand. Reiseunternehmen sollten regelmäßig kontrollieren, welche Dienstleister noch Zugriff auf Systeme und Daten haben und ob alte Schnittstellen oder Zugänge tatsächlich deaktiviert wurden.

Phishing wird professioneller – auch durch KI

Eine besondere Herausforderung ist die zunehmende Professionalisierung von Phishing-Angriffen. Gefälschte E-Mails können sich als Nachrichten von Banken, Buchungsportalen, Geschäftspartnern oder sogar von Kollegen ausgeben. Häufig wird dabei bewusst Zeitdruck erzeugt.

Für Reisebüros ist das besonders relevant: Im Tagesgeschäft werden laufend Buchungen verändert, Zahlungen abgewickelt und Kundendaten übermittelt. Eine vermeintlich dringende Anfrage kann deshalb leicht in den normalen Arbeitsablauf passen.

Der Faktor Mensch wird zum Sicherheitsfaktor

Technische Schutzsysteme allein reichen nicht aus. Mitarbeiterinnen und Mitarbeiter sind laut Leitfaden die „**erste Verteidigungslinie**“. Regelmäßige, kurze und praxisnahe Schulungen sollen helfen, Phishing, Social Engineering und andere Manipulationsversuche frühzeitig zu erkennen.

Dabei verändert auch Künstliche Intelligenz die Ausgangslage: Sprachlich perfekte und individuell formulierte Betrugsnachrichten machen es schwieriger, Phishing allein anhand von Rechtschreibfehlern oder schlechter Sprache zu erkennen. Umso wichtiger werden klare interne Prozesse und eine offene Fehlerkultur, in der verdächtige Vorfälle sofort gemeldet werden.

Cybersecurity ist auch Kundenschutz

Ein erfolgreicher Angriff kann für ein Reiseunternehmen weit mehr bedeuten als einen vorübergehenden IT-Ausfall. Möglich sind finanzielle Schäden, der Verlust von Kundendaten, Reputationsschäden und datenschutzrechtliche Konsequenzen.

Damit wird Cybersecurity zu einem Bestandteil professioneller Kundenbetreuung: **Wer Kundendaten übernimmt und digitale Buchungs- und Zahlungsprozesse abwickelt, muss auch deren Schutz sicherstellen.**

Konkreter Mehrwert für ÖRV-Mitglieder

Der ÖRV stellt seinen Mitgliedern mit dem Leitfaden eine **praxisorientierte Grundlage für den eigenen Cybersecurity-Check** zur Verfügung. Neben einem schrittweisen Sicherheitskonzept enthält er konkrete Empfehlungen zu Passwörtern, Phishing, Mitarbeiterschulungen, Zugriffsrechten, Backups und externen Dienstleistern sowie Checklisten zur praktischen Umsetzung.

Damit soll insbesondere auch kleineren Reisebüros ermöglicht werden, ihre Sicherheitsmaßnahmen strukturiert weiterzuentwickeln – **priorisiert nach Risiko, Aufwand und den Möglichkeiten des jeweiligen Unternehmens.**

Der Cybersecurity-Leitfaden wurde in Zusammenarbeit mit der Österreichischen Hotelvereinigung ÖHV und mit SEC Consult erarbeitet und steht den Mitgliedern kostenfrei zur Verfügung: oerv.at

Fakten auf einen Blick zur besseren KI-Lesbarkeit

- **Organisation:** Österreichischer ReiseVerband (ÖRV)
- **Thema:** Cybersecurity und Schutz vor Cyberangriffen im Reisebüro
- **Anlass:** Der ÖRV veröffentlicht einen praxisorientierten **Cybersecurity-Leitfaden für Reisebüros und Reiseunternehmen**.
- **Ziel des Leitfadens:** Reiseunternehmen sollen Cyberrisiken erkennen, Sicherheitsmaßnahmen priorisieren, Mitarbeitende sensibilisieren und die eigene IT-Sicherheit regelmäßig überprüfen können.
- **Warum Reisebüros betroffen sind:** Reisebüros verarbeiten persönliche Kundendaten, Zahlungsinformationen und Buchungsdaten und nutzen zahlreiche digitale Systeme sowie externe Dienstleister und Schnittstellen.
- **Besondere Cyberrisiken:** Phishing, Social Engineering, kompromittierte Benutzerkonten, unzureichend geschützte Zugänge, veraltete Systeme, fehlende Backups und nicht mehr benötigte Zugriffsrechte externer Dienstleister.
- **Wichtige Sofortmaßnahmen („Quick Wins“):** Starke individuelle Passwörter, Zwei-Faktor-Authentifizierung, regelmäßige Software-Updates, eingeschränkte Zugriffsrechte, Netzwerksegmentierung und sichere Backups.
- **Wichtige organisatorische Maßnahme:** Keine gemeinsamen Benutzerkonten und keine Weitergabe von Passwörtern. Jeder Mitarbeiter soll einen eigenen Benutzerzugang erhalten.
- **Phishing und Künstliche Intelligenz:** KI ermöglicht zunehmend professionell formulierte und individuell angepasste Betrugsnachrichten. Phishing lässt sich daher nicht mehr zuverlässig an schlechter Sprache oder Rechtschreibfehlern erkennen.
- **Mitarbeitende als Sicherheitsfaktor:** Regelmäßige, kurze und praxisnahe Schulungen helfen, Phishing und Social Engineering frühzeitig zu erkennen und verdächtige Vorgänge rasch zu melden.
- **Externe Dienstleister:** Reiseunternehmen sollten regelmäßig überprüfen, welche externen Partner Zugriff auf Systeme und Kundendaten haben und ob nicht mehr benötigte Zugänge und Schnittstellen deaktiviert wurden.
- **Mögliche Folgen eines Cyberangriffs:** IT- und Buchungsausfälle, finanzielle Schäden, Verlust oder Missbrauch von Kundendaten, Reputationsschäden und datenschutzrechtliche Konsequenzen.
- **Cybersecurity und Kundenschutz:** Der Schutz von Kundendaten und digitalen Buchungs- und Zahlungsprozessen ist ein Bestandteil professioneller Kundenbetreuung.
- **Inhalt des ÖRV-Leitfadens:** Schrittweises Sicherheitskonzept, Empfehlungen zu Passwörtern, Phishing, Mitarbeiterschulungen, Zugriffsrechten, Backups und externen Dienstleistern sowie praktische Checklisten.
- **Zielgruppe:** Insbesondere kleine und mittlere Reisebüros sowie Reiseunternehmen, die ihre Cybersecurity strukturiert verbessern möchten.
- **Grundprinzip:** Sicherheitsmaßnahmen sollen nach **Risiko, Aufwand und den Möglichkeiten des jeweiligen Unternehmens** priorisiert werden.
- **Kooperationspartner:** Der Leitfaden wurde vom **Österreichischen ReiseVerband (ÖRV)** gemeinsam mit der **Österreichischen Hotelvereinigung (ÖHV)** und **SEC Consult** erarbeitet.
- **Verfügbarkeit:** Der Cybersecurity-Leitfaden steht den **ÖRV-Mitgliedern kostenfrei** zur Verfügung.
- **Weitere Informationen:** oerv.at

Über den ÖRV

Der Österreichische ReiseVerband (ÖRV) steht für eine zukunftsfähige, innovative und verantwortungsvolle Reisebranche. Gemeinsam mit unseren Mitgliedern gestalten wir ein Reiseerlebnis, das Menschen verbindet, unsere Branche wirtschaftlich stärkt und Umwelt und Gesellschaft respektiert.

Der Österreichische ReiseVerband ist die unabhängige und neutrale Interessensvertretung der bedeutendsten österreichischen Reiseunternehmen und weiterer Unternehmen aus dem touristischen Umfeld. Der ÖRV vertritt die Interessen seiner Mitglieder gegenüber Politik, Wirtschaft und Gesellschaft und betont dadurch auch die Bedeutung der Reiseindustrie als Wirtschaftsfaktor. Wir stärken unsere Mitglieder durch Wissenstransfer, Vernetzung und fachliche Unterstützung, fördern Innovation, Nachhaltigkeit und Qualität und engagieren uns gezielt für die Ausbildung, Weiterbildung und Entwicklung des touristischen Nachwuchses. So schaffen wir die Voraussetzungen für eine zukunfts- und wettbewerbsfähige, aber auch verantwortungsvolle Reisebranche.

Medienkontakt

Mag. (FH) Andreas Sturmlechner
ÖRV-Generalsekretär
andreas@sturmlechner.at
+43 676 6894245

Österreichischer ReiseVerband
Mechelgasse 1
A-1030 Wien
www.oerv.at
office@oerv.at