clavis/cyber

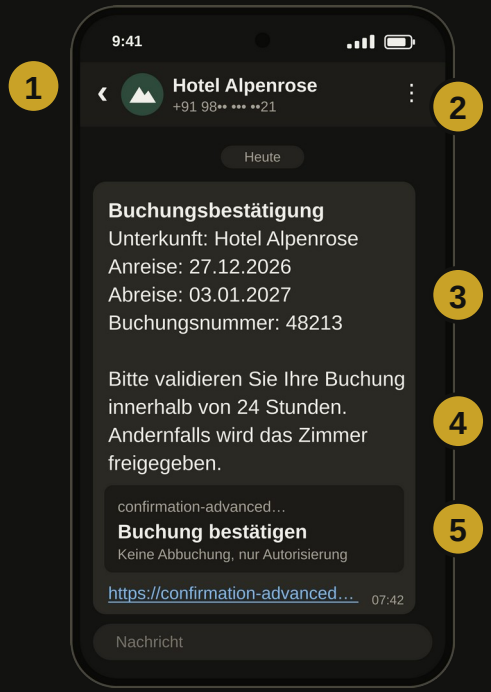
WEBINAR · 11. NOVEMBER 2026 · 11:30 UHR

Datenleck im Tourismus

Was Hotels und Destinationen jetzt tun müssen

Vincent Mahler A1 Telekom Austria
Abdelkader Cornelius Clavis Cyber

So sieht die Nachricht beim Gast aus



1. **Name und Profilbild.** Kann jeder frei wählen. Hotelname und Logo sind in einer Minute kopiert.
2. **Die Nummer.** Im dokumentierten Fall ausländisch. Bei SMS und Anrufen lässt sich sogar eine echte Nummer vortäuschen.
3. **Die Buchungsdaten.** Echt. Sie stammen aus dem Datenleck, deshalb wirkt die Nachricht glaubwürdig.
4. **Die Frist.** 24 Stunden, sonst sei das Zimmer weg. Druck, damit der Gast nicht nachfragt.
5. **Der Link.** Führt auf eine nachgebaute Seite. Dort soll der Gast seine Kartendaten eingeben.

Der Gast kann es kaum erkennen. Sagen Sie ihm vorher, wie Zahlungen angefordert werden und wo er sicher nachfragen kann.

Nachgestellt nach dem dokumentierten Aufbau (Tiroler Tageszeitung über skinachrichten.de, 28.10.2026); Hotel, Daten und Nummer erfunden. Spoofing: Watchlist Internet über WKO, 09.10.2026.

Wer heute mit Ihnen spricht

Abdelkader Cornelius

Gründer und Geschäftsführer, Clavis Cyber

KÜCHE	Gelernter Koch, führte ein Sternerestaurant
SEIT 2007	Beobachtet den Datenhandel im Darknet
18 JAHRE	Ermittlung, Einsatz bei Angriffen, Forensik
2022	Co-Autor „Underground Economy“, NZZ Libro

Vincent Mahler A1, Cyber Security & AI Defence Hub

CLAVIS CYBER

Wir werden gerufen, wenn es passiert ist.

Einsatz bei Cyberangriffen, rund um die Uhr.

Wir sehen, was im Untergrund gehandelt wird.

Analyse von Darknet-Märkten und gestohlenen Zugängen.

Wir greifen im Auftrag an.

Sicherheitsprüfungen, bevor es andere tun.

Was laut feratel passiert ist

Drittsystem
Angreifer erlangt dort Zugangsdaten

→

Schnittstellen-partner
Seine Deskline-Zugangsdaten werden missbraucht

→

Deskline
Buchungsdaten werden abgerufen

→

Gast
Betrugsnachricht im Namen des Hotels

23:00 – 01:15 Uhr

25. auf 26. Oktober 2026, die Nacht auf den Nationalfeiertag. Bislang festgestellter Abruf, die Untersuchung läuft.

ABGERUFEN

Name, Adresse, Telefon, E-Mail, Reisedaten, Betrieb, Reisepreis, Zahlungsstatus

NICHT ABGERUFEN

Kreditkartendaten

Quellen: feratel-Partnerinformation, veröffentlicht bei Borncity, 29.10.2026; feratel gegenüber ORF, 31.10.2026. Laut feratel keine Hinweise auf einen Einbruch in die eigenen Systeme.

Was über das Ausmaß bekannt ist

1.700

Betriebe in Tirol

Rund, potenziell betroffen. Laut feratel etwa ein Drittel tatsächlich.

97

Betriebe in Salzburg

In elf oder zwölf Tourismusverbänden, je nach Bericht.

3.000

Gäste in der Steiermark

Rund, laut Kleiner Zeitung. Alle Verbände, keine offizielle Zahl.

Kein Einzelfall. Seit August meldeten auch Seekda, HotelNetSolutions, Amadeus iHotelier und Straiv Datenabflüsse mit demselben Betrugsmuster. Ein Zusammenhang mit diesem Vorfall ist nicht belegt.

Quellen: tirol.ORF.at und salzburg.ORF.at, 31.10.2026; Kleine Zeitung, 30.10.2026; Seekda-Kundeninformation; DEHOGA Berlin, 26.10.2026.

Wer ist wofür verantwortlich?

VERANTWORTLICHER

Tourismusverband oder Betrieb

Je nach Buchungsweg, auch beide gemeinsam

- Meldet an die Datenschutzbehörde, binnen 72 Stunden ab Kenntnis (Art. 33)
- Benachrichtigt die Gäste bei hohem Risiko (Art. 34)
- Dokumentiert jeden Vorfall, auch ohne Meldung (Art. 33 Abs. 5)

AUFTRAGSVERARBEITER

Softwareanbieter

Zum Beispiel feratel, nach eigener Angabe

- Informiert den Verantwortlichen unverzüglich (Art. 33 Abs. 2)
- Unterstützt bei Meldung und Aufklärung (Art. 28 Abs. 3)
- Verarbeitet nur nach Vertrag und Weisung (Art. 28)

Die Hauptlast trägt der Verantwortliche. „Der Dienstleister war schuld“ entlastet nicht: Er muss sorgfältig ausgewählt worden sein (Art. 28 Abs. 1).

DSGVO Art. 26, 28, 33, 34; feratel-Partnerinformation, veröffentlicht bei Borncity, 29.10.2026. Allgemeine Orientierung, keine Rechtsberatung.

So kommen Angreifer an Ihre Gästedaten

Über den Dienstleister

Die Zugangsdaten eines Partners werden gestohlen. Niemand merkt es.

BEISPIEL

Deskline, Oktober 2026

Über die Betriebe

Viele Vermieter haben eigene Zugänge zum Buchungssystem. Ein infizierter Rechner genügt.

BEISPIEL

Kampagne gegen Hotels laut Microsoft; Fall auf Folie 10

Über das eigene Büro

Schadsoftware auf einem Rechner im Verband. Ein Zugang reicht für viele Betriebe.

SO FUNKTIONIERT ES

Folien 8 und 9

Es geht nicht immer um Daten. Seehotel Jägerwirt, Turracher Höhe: Schlüsselkarten der Zimmer blockiert, 1.500 Euro an die Erpresser gezahlt.

Quellen: feratel-Partnerinformation bei Borncity, 29.10.2026; Microsoft Threat Intelligence, 13.03.2025; APA, Jänner 2017.

Was ist ein Infostealer?

Wörtlich: Informationsdieb. Ein Schadprogramm, das Passwörter stiehlt. Es startet einmal, kopiert alles und verschwindet. Der Rechner läuft normal weiter.

1 DER WEG HINEIN

- Mail mit Link, angeblich vom Buchungsportal
- Anhang einer angeblichen Gästeanfrage
- Gratis-Programm aus dem Internet

2 DIE BEUTE

- Im Browser gespeicherte Passwörter
- Die offene Anmeldung („angemeldet bleiben“)
- Gespeicherte Kartendaten

3 DIE FOLGE

- Das Paket wird im Darknet verkauft
- Der Käufer meldet sich mit Ihren Daten an
- Er sieht Ihre Buchungen und schreibt Ihren Gästen

Die drei Wege hinein sind die typischen. Beispiel für den ersten: Kampagne gegen Hotels laut Microsoft Threat Intelligence, 13.03.2025.

Warum das Passwort nicht reicht

Eine Anmeldung im Internet funktioniert wie ein Check-in im Hotel.

	IM HOTEL	IM BUCHUNGSSYSTEM
1	Ausweis beim Check-in	**Benutzername, Passwort, Code**
2	Zimmerkarte für den Aufenthalt	**„Angemeldet bleiben“ (Cookie)**
3	Mit der Karte ins Zimmer	**Ins System, ohne Passwort**

Der Infostealer kopiert die Zimmerkarte. Der Täter muss nicht an die Rezeption: Er braucht weder Passwort noch Code. Passwort ändern allein beendet die offene Anmeldung nicht bei jedem Dienst.

Die digitale Zimmerkarte gilt, bis man sich abmeldet oder sie abläuft. Nach einem Fund deshalb: überall abmelden, Passwörter ändern, Rechner neu aufsetzen.

Echter Fall: ein Rechner in einem Betrieb

Ein Beherbergungsbetrieb in Österreich, wie es ihn in jeder Region gibt. Diese Zugangsdaten hatte ein Infostealer ausgelesen.

ZUGANGSDATEN FÜR	DAMIT KANN EIN FREMDER
Buchungssystem	alle Buchungen und Gästedaten sehen
Buchungsportale	Gästen im Namen des Hauses schreiben
Hotelsoftware	Gästekartei und Rechnungen einsehen
Kartenzahlung	Umsätze und Abrechnungen einsehen
Einkauf	auf Rechnung des Hauses bestellen
Website	Inhalte ändern und Besucher umleiten

clavis/cyber

Quelle: Clavis Cyber, eigene Auswertung, anonymisiert. Rechte Spalte: was ein solcher Zugang erlaubt. Mit dem Deskline-Vorfall hat der Fund nichts zu tun.

Fünf Dinge für diese Woche

1	**Betroffene ermitteln**	Report „Potenzielle Buchungen Datenvorfall“ im ExpertClient von feratel auswerten.
2	**Betriebe informieren**	Mustertext von feratel nutzen. Gästen sagen, wie Zahlungen angefordert werden.
3	**Zweiten Faktor einschalten**	Für WebClient und ExpertClient, per Ticket bei feratel. Für Verband und Vermieter.
4	**Zugänge aufräumen**	Mitarbeiter, Ehemalige, Vermieter, Schnittstellenpartner: Nicht Benötigtes sperren.
5	**Rechner prüfen**	Im Büro und in den Betrieben: keine Passwörter im Browser, regelmäßig abmelden.

Ausführlich im Anhang ab Folie 13. Quelle zu Report und Mehr-Faktor-Anmeldung: feratel-Partnerinformation, veröffentlicht bei Borncity, 29.10.2026.

Der Check für Verband und Betriebe

IM INTERNET

Was ist von außen erreichbar?

IM EIGENEN NETZ

Wo ist das eigene Netz offen?

IM DARKNET

Sind Zugangsdaten bereits im Umlauf?

Sie erhalten einen verständlichen Bericht mit konkreten Maßnahmen für Ihre IT-Betreuung. Zum Festpreis.

Einen Vorfall bei einem Dienstleister verhindert der Check nicht. Er zeigt, wo Verband und Betriebe selbst offen stehen.

KONTAKT

a1.kooperation@a1.at

Im Notfall **0800 220 001**

Sofortmaßnahmen für Tourismusverbände

1	**Betroffene ermitteln**	Report „Potenzielle Buchungen Datenvorfall“ im ExpertClient auswerten. Nur verschlüsselt weitergeben.
2	**Betriebe informieren**	Betroffene Betriebe benennen, den Mustertext von feratel (Deutsch und Englisch) weitergeben, einen Ansprechpartner im Verband nennen.
3	**Meldung klären**	Mit den Betrieben festlegen, wer an die Datenschutzbehörde meldet. Die Frist von 72 Stunden läuft ab Kenntnis. Schriftlich festhalten.
4	**Zugänge zurücksetzen**	Passwörter im WebClient zurücksetzen, offene Anmeldungen beenden, den zweiten Faktor für WebClient und ExpertClient per Ticket bei feratel aktivieren.
5	**Zugänge aufräumen**	Konten ehemaliger Mitarbeiter und Vermieter sperren. Bei feratel erfragen, welche Schnittstellenpartner auf die Daten der Region zugreifen.
6	**Weniger Daten erheben**	Nur abfragen, was gebraucht wird. Ein Tiroler Verband hat das Feld für die Telefonnummer aus der Buchungsmaske genommen.

Quellen: feratel-Partnerinformation und Rundmail eines Tiroler Tourismusverbands, veröffentlicht bei Borncity, 29.10.2026.

Sofortmaßnahmen für Betriebe

1	**Betroffenheit klären**	Beim Tourismusverband nachfragen, ob eigene Buchungen im Report von feratel stehen.
2	**Gäste warnen**	Gäste mit kommender Anreise anschreiben, Mustertext im Anhang. Dabei sagen, wie Ihr Haus Zahlungen anfordert.
3	**Team einweisen**	Die Kurzanweisung im Anhang an alle mit Gästekontakt geben, auch an Saisonkräfte und Aushilfen.
4	**Zweiten Faktor einschalten**	Für WebClient, Buchungsportale, Hotelsoftware und E-Mail. Er schützt das Passwort, nicht die offene Anmeldung.
5	**Rechner aufräumen**	Keine Passwörter im Browser, abmelden statt „angemeldet bleiben“, Updates einspielen, Gäste-WLAN vom Betriebsnetz trennen.
6	**Bei Verdacht richtig handeln**	Rechner vom Netz nehmen, nicht selbst reparieren, Fachleute holen. Passwörter von einem anderen Gerät aus ändern, überall abmelden.

Im Notfall: A1 Notfallnummer 0800 220 001.

Datenschutz und Haftung: was wann zu tun ist

SOFORT	Vorfall dokumentieren: was, wann, welche Daten, welche Maßnahmen. Gilt auch, wenn keine Meldung nötig ist (Art. 33 Abs. 5).
BINNEN 72 STUNDEN	Meldung an die Datenschutzbehörde, außer es besteht voraussichtlich kein Risiko für die Gäste (Art. 33). Fehlende Angaben dürfen nachgereicht werden.
BEI HOHEM RISIKO	Betroffene Gäste unverzüglich benachrichtigen, in klarer und einfacher Sprache (Art. 34).
DANACH	Vertrag mit dem Dienstleister prüfen: Meldewege, Unterstützung im Vorfall, Sicherheitsmaßnahmen (Art. 28).

HAFTUNG

Gegenüber dem Gast haftet der Verantwortliche. Der Auftragsverarbeiter haftet, wenn er eigene Pflichten verletzt oder Weisungen missachtet (Art. 82).

Frei ist nur, wer nachweist, dass er für den Schaden nicht verantwortlich ist (Art. 82 Abs. 3).

Gute Dokumentation ist deshalb der beste Schutz.

DSGVO Art. 28, 33, 34, 82. Meldung an die österreichische Datenschutzbehörde über dsb.gv.at. Allgemeine Orientierung, keine Rechtsberatung.

Kurzanweisung für Mitarbeiter

WENN EIN GAST ANRUFT

1. Ruhig bleiben und die Buchung im System prüfen.
2. Klarstellen: Die Nachricht kam nicht von uns.
3. Schon bezahlt? Sofort Bank oder Kartenanbieter anrufen und Anzeige bei der Polizei erstatten.
4. Festhalten: Buchungsnummer, Absendernummer, Datum, Uhrzeit, Screenshot.
5. Weitergeben an: [Ansprechpartner im Haus oder Verband]

AM EIGENEN RECHNER

- Keine Anhänge und Links aus unerwarteten Nachrichten öffnen, auch nicht „vom Buchungsportal“.
- Keine Passwörter im Browser speichern.
- Nach der Schicht abmelden statt angemeldet bleiben.
- Verdacht sofort melden, nicht selbst reparieren.

Zum Aushängen an der Rezeption und im Gästeservice. Die festgehaltenen Angaben helfen bei Anzeige und Aufklärung.

Mustertext für Ihre Gäste

Betreff: Wichtiger Hinweis zu Ihrer Buchung

Liebe Gäste,

derzeit versenden Betrüger Nachrichten im Namen von Unterkünften, per WhatsApp, SMS oder E-Mail. Sie enthalten teils echte Buchungsdaten und fordern dazu auf, über einen Link Kartendaten einzugeben.

Zahlungen fordern wir ausschließlich so an: **[Ihr Zahlungsweg]**.

Wenn Sie eine solche Nachricht erhalten, klicken Sie bitte nicht auf den Link und rufen Sie uns an: **[Telefonnummer wie auf Ihrer Website]**.

Haben Sie bereits Daten eingegeben, kontaktieren Sie sofort Ihre Bank und erstatten Sie Anzeige.

Herzliche Grüße, **[Name, Betrieb]**

Warnhinweis zum Versand an Gäste mit kommender Anreise. Ersetzt keine Benachrichtigung nach Art. 34 DSGVO, falls diese nötig ist.

Sample text for your guests

Subject: Important information about your booking

Dear guest,

fraudsters are currently sending messages in the name of accommodation providers via WhatsApp, text message or email. Some contain genuine booking details and ask you to enter card details via a link.

We only request payments as follows: **[your payment method]**.

If you receive such a message, please do not click the link and call us instead: **[phone number as shown on your website]**.

If you have already entered your details, contact your bank immediately and report it to the police.

Kind regards, **[name, property]**

Englische Fassung des Warnhinweises. Ersetzt keine Benachrichtigung nach Art. 34 DSGVO, falls diese nötig ist.