



Beim Einloggen in ein öffentliches WLAN besteht das Risiko, Opfer von Datendieben zu werden.



Vorsicht vor Taschendieben: Diensthandys können wertvolle Beute und auch Informationsquelle mit sensiblen Daten sein.

Sicher unterwegs

Kriminelle Angriffe, Unfälle oder medizinische Notfälle stellen Risiken für Geschäftsreisende dar. Mit richtiger Vorbereitung können problematische Situationen verhindert bzw. gemeistert werden.

Verspäteter Flug, verlorenes Gepäck, fremde Stadt: Auf Reisen ergeben sich oft herausfordernde Situationen. Die Konzentration sinkt, man ist unaufmerksam. Die Gedanken drehen sich darum, schnell ins Hotel zu kommen. Ab diesem Zeitpunkt können Geschäftsreisende im Ausland besonders leicht Ziel für kriminelle Angriffe werden – Diebstahl, Raub, Erpressung, Entführung oder terroristischer Angriff. Vorsichtsmaßnahmen und gute Vorbereitung sind auch in Ländern mit einer weniger riskanten sicherheitspolitischen Lage notwendig. Geschäftsreisende verfügen meist nicht nur über eigene finanzielle Mittel, sondern sind auch von ihrem Unternehmen abgesichert. 4,1 Millionen Dienstreisen wurden im Jahr 2014 von Österreicherinnen und Österreichern unternommen, mehr als die Hälfte davon führten ins Ausland.

Taschendiebe erkennen Reisende auf den ersten Blick. Sie nutzen Momente aus, in denen sie abgelenkt sind, und greifen nach den Wertgegenständen. Diensthandys, Laptops oder Tablets sind nicht nur eine wertvolle Beute, sondern oft auch Informationsquellen mit sensiblen Daten. Ihr Diebstahl bedeutet oft einen größeren Schaden für das Unternehmen. Vor Raub und Taschendiebstahl kann man sich in vielen Fällen schützen, indem man seine Umgebung und die Menschen beobachtet.

Beamte des Bundeskriminalamts empfehlen, Wertgegenstände möglichst eng am Körper zu tragen, Kreditkarten und Bargeld sollten in den Innentaschen der Kleidung aufbewahrt werden. Man sollte dunkle und abgelegene Straßen meiden, aber auch bei Menschenansammlungen vorsichtig sein.

Cybercrime. Auch beim Einloggen in ein öffentliches WLAN besteht das Risiko, Opfer von Datendieben zu werden. Bei öffentlichen Hotspots in Restaurants, Hotels oder am Flughafen wird oft auf Verschlüsselungen verzichtet. Cyber-Kriminelle können so unter anderem auf fremde Bankdaten und Passwörter zugreifen. IT-Unternehmen empfehlen, öffentliche Wlan-Netze niemals für Einkäufe oder Transaktionen zu verwenden. Alle internetfähigen Geräte sollten mit einer Sicherheitssoftware ausgerüstet werden.

Reiseinformation. Man sollte sich vor jeder Reise über das Zielland informieren.



Wertgegenstände sollten nie unbeaufsichtigt liegen gelassen werden.

mieren. Die hygienischen Umstände, wie Sauberkeit des Trinkwasser, und häufige Erkrankungen vor Ort sollen bei der Reiseplanung miteinbezogen werden. Zusätzliche Impfungen und entsprechende Vorsichtsmaßnahmen können Infektionskrankheiten vorbeugen. Das Bundesministerium für Europa, Integration und Äußeres erteilt Auskunft über Sicherheit, Kriminalität und gibt Reisewarnungen. Außerdem gibt es die Möglichkeit, sich vor einem Auslandsaufenthalt online unter www.reiseregistrierung.at anzumelden. Im Fall einer Krise oder Naturkatastrophe kann das Außenministerium Österreicherinnen und Österreicher im Ausland rasch kontaktieren und Hilfe leisten.

Versicherung. Dienstgeber haften für ihre Mitarbeiterinnen und Mitarbeiter. Das bedeutet, dass im Ernstfall eine medizinische Versorgung zu leisten ist und wenn nötig der Rücktransport organisiert werden muss. Außerdem kommt der Arbeitgeber für Schäden an allen privaten Gegenständen auf, die der Arbeitnehmer zur Erfüllung seiner dienstlichen Pflichten benutzt, z. B. Laptop, Smartphone, Reisegepäck und Fahrzeug. Der Unfallversicherungsschutz auf Dienstreisen oder während Ausbildungs- und Fortbildungsveranstaltungen besteht auch bei einer Betätigung, die mit dem Beschäftigungsverhältnis „rechtlich wesentlich zusammenhängt“.

Anna Strohdorfer