

Sicherheit auf Geschäftsreisen

Achtung, Datendiebe!

Wirtschaftsspionage verursacht Schäden in Milliardenhöhe. Doch Unternehmen sind nicht nur in Deutschland selbst gefährdet, auch auf Geschäftsreisen lauern die Datendiebe. Lesen Sie, wie Reisende sich und ihre Informationen schützen können.

DATEN-LANG-FINGER Der Info-Klau erfolgt auf Dienstreisen oft unbemerkt.

TEXT: MARTIN JÜRS

Die Zahlen sind erschreckend: Zwei Drittel aller deutschen Unternehmen sind laut einer aktuellen Umfrage des Allensbacher Instituts schon einmal Opfer von Hacker-Angriffen geworden. Bei 15 Prozent der Firmen kommt es sogar häufig zu solchen Cyber-Attacken, 20 Prozent berichten von gelegentlichen virtuellen Angriffen, bei 29 Prozent der befragten Unternehmen ist dies eher selten der Fall.

Firmen handeln oft fahrlässig

Dabei versuchen die privaten wie staatlichen Datendiebe aber nicht nur über das Internet in die Computersysteme der Unternehmen einzudringen. Der Informationsklau droht auch auf Geschäftsreise. Gerade hier wird es den Kriminellen oft sehr leicht gemacht.

„Der Umgang selbst mit sensiblen Daten ist auf Reisen oft sehr fahrlässig“, hat Unternehmensberaterin und IT-Security-Managerin Alexandra Klawonn festgestellt. Das beginnt bereits bei der Menge der mitgenommenen Unterlagen. In der Regel gehen viel zu viel Informationen zu wenig geschützt mit auf Dienstreise. Insbesondere dann, wenn die Mitarbeiter ihr Firmen-Notebook dabei haben. „Nehmen sie wirklich nur die absolut notwendigen Informationen mit“, rät Christian Schaaf, Geschäftsführer der Sicherheitsberatung Corporate Trust aus München.

Tipps zum Datenschutz

➔ **BACKUP ANFERTIGEN** Bevor es mit sensiblen Daten auf Reisen geht, diese unbedingt auf einem externen Speicher sichern. Dann wiegt der Verlust des Laptops nicht ganz so schwer.

➔ **KOMPLEXE PASSWÖRTER** Passwörter sind ein erster Schutz vor Datenklau. Zu einfach sollten sie nicht sein. Ein Mix aus zehn bis zwölf Zahlen, Ziffern und Sonderzeichen macht es Datendieben schwer.

➔ **DATEN VERSCHLÜSSELN** Nutzen Sie moderne Verschlüsselungs-Software! Vor deren Einsatz sollte aber geprüft werden, ob diese im Zielland auch verwendet werden darf. Das ist nicht überall der Fall.

➔ **VOLUMEN BESCHRÄNKEN** Je weniger Informationen mit auf Reisen gehen, umso weniger kann ausspioniert werden. Daher genau prüfen, welche Daten mit müssen.

Um zu verhindern, dass zu viele wichtige Daten das Unternehmen via Laptop verlassen, empfehlen Klawonn und Schaaf gleichermaßen, möglichst nur spezielle Reise-Notebooks einzusetzen, auf denen sich lediglich Basisprogramme befinden, um unterwegs arbeiten zu können. „Nach der Rückkehr sollten diese Geräte auf keinen Fall an das Firmennetzwerk angeschlossen werden“, sagt Klawonn. Cyber-Kriminelle könnten unbemerkt Viren und andere Schadprogramme auf den Rechner aufgespielt haben.

Wer zudem glaubt, man könne einen Laptop mit geheimen Daten, nachdem man die Festplatte gelöscht und alle Programme neu aufgespielt hat, ohne Bedenken auf Reisen einzusetzen, der irrt. Klawonn: „Das einmalige Löschen der alten Inhalte bringt oft nichts. Mitunter muss man die Festplatte bis zu 20 Mal säubern, um Programme wirklich zu vernichten.“

Hotspots unbedingt meiden

Meiden sollten Reisende, die von unterwegs ihren E-Mail-Account via Notebook oder Smartphone einsehen wollen, öffentliche Hotspots. „Da kann praktisch jeder mitlesen“, sagt Klawonn. Gerade staatliche Daten-Spione würden sich über die örtlichen Provider in die scheinbar passwortgeschützte Kommunikation einklinken und eifrig mitlesen. Selbst https-Verbindungen bieten keine Sicherheit. Die garantieren nur sogenannte Virtuell Private Networks (VPN). Doch deren Nutzung wird zum Beispiel in China gestört.

Wer sein Unternehmen vor Datenklau bewahren will, sollte aber nicht nur mit seinen mobilen Endgeräten sorgsam umgehen, diese mit spezieller Software verschlüsseln und auf Reisen möglichst nicht aus den Augen lassen. Er sollte sich auch überlegen, wen er vorher alles über seine Reisen informiert.

Sonst kann es ihm ergehen wie dem Mitarbeiter einer deutschen Firma, der seine Reise über ein Social Network breit angekündigt hatte. Während seiner Abwesenheit tauchte dann ein Unbekannter am Firmensitz auf und erklärte, eben jener Geschäftsreisende habe ihn beauftragt, den Drucker zur Wartung abzuholen. Verdacht schöpfte niemand. Und so verschwand das Gerät. Darauf gespeichert waren zahlreiche Vertrags- und sonstige Unterlagen. >>

Interview mit Christian Schaaf, Corporate Trust

Wie groß ist die Gefahr, auf Geschäftsreise Opfer von Datendieben zu werden?

Leider recht groß. Der Diebstahl sensibler Informationen findet praktisch überall auf der Welt statt – auch wenn die Gefahr in Ländern wie China oder Russland besonders groß ist.

Wer ist denn besonders gefährdet?

Nachrichtendienste fremder Länder oder Konkurrenzfirmen haben es nicht nur auf leitende Angestellte abgesehen. Auch Vertriebsmitarbeiter oder Mitarbeiter, die auf Messen vertreten sind und über spezielles Wissen verfügen, geraten ins Visier von Wirtschafts- und Industriespionen.

Mit welchen Tricks wird gearbeitet?

Zum einen werden Unterlagen oder Geräte wie Laptops einfach gestohlen. Dann gibt es Versuche, heimlich Viren oder andere Schadprogramme auf mobile Endgeräte zu installieren, um so an sensible Daten zu kommen. Daneben nimmt das Social Engineering zu. Hier geht es um den Aufbau persönlicher Beziehungen, aber auch darum, Menschen mittels kompromittierender Situationen erpressbar zu machen.

Wie schützt man sich und seine Daten?

Natürlich kann man sich mit technischen Hilfsmitteln absichern. Mindestens genauso wichtig ist es aber, die eigenen Mitarbeiter in diesem Punkt zu sensibilisieren, zum Beispiel durch Schulungen, online wie offline.

www.biztravel.de

Weitere Berichte zum Thema **Datensicherheit**: www.biztravel.de (Rubrik Reisetipps)

