Datenschutz auf Auslandsentsendungen und Geschäftsreisen ins Ausland

Was Unternehmen wissen sollten

Die Häufung von Cybervorfällen führt weltweit zu einer Verschärfung und Internationalisierung des Datenschutzrechts, das vor allem Unternehmen in die Pflicht nimmt. Das hat auch Auswirkungen auf die Global-Mobility-Praxis deutscher Firmen.

Immer mehr wirtschaftliche Schäden weltweit werden durch sogenannte Cybervorfälle verursacht. Dabei handelt es sich, vereinfacht ausgedrückt, um Angriffe auf die digitale Infrastruktur eines Unternehmens mit dem Ziel, diese zu stören und beispielsweise an Geschäftsgeheimnisse und personenbezogene Daten zu gelangen. Tatsächlich rangieren Cybergefährdungen laut dem aktuellen Allianz Risk Barometer derzeit auf Rang drei der zehn wichtigsten globalen Geschäftsrisiken 2017. Zum Vergleich: Noch vor vier Jahren lag dieses Risiko lediglich auf Platz 15. Die Besorgnis der Unternehmen nimmt auch deshalb zu, weil diese Art der Gefährdung größtenteils noch eine „Blackbox" darstellt und nicht auf eine bestimmte Branche oder Firmengröße begrenzt ist – sie kann im Grunde jeden treffen. Nach professionellen Hackerangriffen ist die Hauptursache für einen Cyberangriff in einer Firma eine Daten- oder Sicherheitsverletzung (siehe Grafik). Deshalb gewinnt der Schutz von Daten innerhalb von Betrieben und Institutionen eine rasant zunehmende Bedeutung.

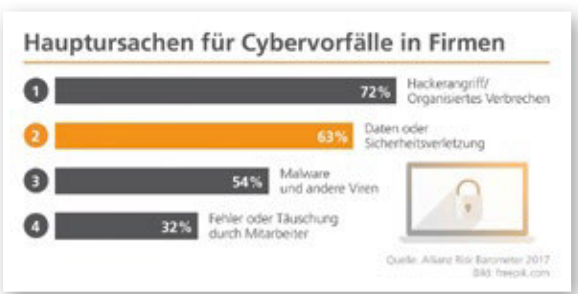
Ein wichtiger Schritt in Richtung Cybersicherheit ist die neue EU-Datenschutz-Grundverordnung (DS-GVO), die ab dem 25. Mai 2018 das Datenschutzrecht innerhalb der Europäischen Union (EU) vereinheitlichen, aber auch verschärfen soll. Im Kern sorgt die neue Verordnung dafür, dass der Ort der Datenverarbeitung keine Rolle mehr spielt. Wer immer sein Angebot oder seine Dienstleistung an EU-Bürger richtet, muss sich dem europäischen Datenschutzrecht unterordnen – das gilt z. B. auch für Facebook und Google. Datenschutzverstöße von Mitarbeitern oder anderen Beteiligten, unabhängig von deren Aufenthaltsort, müssen künftig innerhalb von 72 Stunden der zuständigen Aufsichtsbehörde gemeldet werden. Internationale Firmen und Organisationen melden Vorfälle dann nur noch an die für ihren Hauptsitz zuständige „federführende Aufsichtsbehörde".

Deutliche Erhöhung der finanziellen Sanktionen

Die Kommission hat darüber hinaus die Bußgelder bei Datenschutzverstößen drastisch erhöht. So können Strafen bis zu 20 Millionen Euro oder vier Prozent des gesamten global erzielten Jahresumsatzes betragen. Für Konzerne können dies unter Umständen Milliardenbeträge sein. Damit ist Europa nicht allein, denn weltweit verschärfen die Regierungen ihre Datenschutzregelungen. Besonders strenge Gesetze gibt es bereits in den USA, im Nahen Osten, in Australien und Singapur. In den Vereinigten Staaten betrug die höchste bisher gezahlte Strafe wegen Verletzung des Datenschutzes gegenüber einem Kunden satte 100 Millionen US-Dollar. In den arabischen Ländern drohen selbst bei geringen Verstößen schnell Haftstrafen.

Was bedeutet dies für Unternehmen, die Mitarbeiter ins Ausland entsenden? In ihrem eigenen Interesse und zum Schutz vor Geld- wie Reputationsverlusten sollten Global-Mobility-Verantwortliche Expats und Geschäftsreisende über Sicherheitsmaßnahmen sowie Sicherheitsrisiken und vor allem über entsprechende Maßnahmen umfassend informieren. Idealerweise sollten Travel-Manager und Personaler das Thema Datenschutz in die Entsende- und Geschäftsreiserichtlinie integrieren. Bereits der „Faktor Mensch" bereitet Probleme, denn allein an den acht größten Flughäfen Europas verschwinden jährlich 175.000 Laptops mit wertvollen Daten (siehe Grafik). Mehr als der Verlust der Hardware wiegt jener der oftmals sensiblen Daten. Nicht erfasst in der Statistik sind etwa verloren gegangene USB-Sticks, Firmenhandys oder -tablets. Es ist daher sinnvoll, die inzwischen miteinander vernetzten Geräte nicht nur durch entsprechende Programme zu schützen, sondern möglichst Verbindungen zu anderen firmeninternen PCs und technischen Anlagen vor einer Reise zu kappen.

Empfehlenswert ist es zudem, nur die nötigsten für die Entsendung oder Geschäftsreise relevanten Daten mitzuführen und zu speichern (siehe dazu auch Infokasten „Tipps für Datenschutz auf Auslandsreisen"). Aber Achtung bei verschlüsselten Geräten und Daten: Viele Länder, und dazu gehören nicht nur autokratisch geführte Regimes, verlangen oft die Herausgabe von Passwörtern. In Frankreich und Großbritannien etwa dürfen die Be-



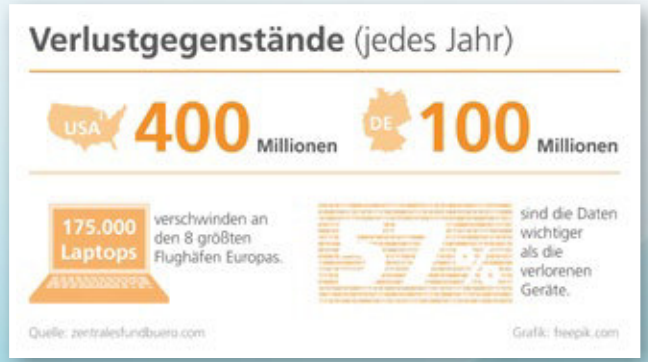
hörden dies sogar per Gesetz. Wer sich bei einer Kontrolle am Flughafen weigert, das Passwort zu nennen, darf in Zwangshaft genommen werden. Unter https://en.wikipedia.org/wiki/Key_disclosure_law sind alle Länder aufgeführt, welche dieses Recht für sich in Anspruch nehmen können.

Vorsicht bei Apps und Co.

Ein weiterer riesiger Unsicherheitsfaktor sind Smartphone-Apps auf den mobilen Endgeräten der Mitarbeiter. Viele von diesen ermöglichen einen direkten Zugriff auf sensible Firmendaten z. B. auf dem Handy. Laut dem Geschäftsreise Verband VDR haben 65 Prozent der Unternehmen ihren Mitarbeitern keine entsprechenden Vorgaben zur Nutzung gemacht. Das ist überaus fahrlässig, und bei Datensicherheitsverstößen werden die Unternehmen sehr wahrscheinlich zur Verantwortung gezogen werden. Ein weiteres unterschätztes Risiko sind die Führungskräfte auf Reisen. Nicht selten kommt es vor, dass diese z. B. in der Business-Lounge am Flughafen lautstark Telefonate führen oder freie Sicht auf Firmeninterna auf ihrem Laptop oder Tablet bieten und somit Spionen geheime Daten wortwörtlich auf dem Silbertablett servieren. Hier gilt es, nicht nur im Vorfeld aufzuklären, sondern auch mögliche Sanktionen festzulegen.

Ein anderes, nicht minder aktuelles datenschutzrechtliches Problem stellt sich insbesondere bei Auslandsentsendungen in Krisenregionen. So bieten immer mehr auf Travel Management spezialisierte Dienstleister sogenannte Traveller Tracking Tools an. Per Klick lässt sich mit dieser Software der Aufenthaltsort von Mitarbeitern ermitteln, um im Notfall sofort Hilfe zu organisieren. Geht dem Expatriate beispielsweise ein lebensnotwendiges Medikament aus, könnte sein Unternehmen dafür sorgen, dass der Dienstleister die Arznei binnen weniger Stunden zum Mitarbeiter vor Ort bringt. Die Antwort auf die Frage, wo der Mitarbeiter sich aktuell aufhält, ist sozusagen Teil des Krisenmanagements von Unternehmen.

Die Grundlage solcher Tracking-Systeme bilden die Reise- und Buchungsdaten der jeweiligen entsandten Mitarbeiter. So werden bei der Flugbuchung



die sogenannten PNR-Daten (Passenger Name Record) über Schnittstellen aus den diversen Buchungssystemen in die Tracking-Software eingespielt. Kommt es zu einer Krisensituation (z. B. Terroranschläge, politische Unruhen oder Naturkatastrophen), prüft der Dienstleister binnen weniger Minuten, wo sich der Mitarbeiter im entsprechenden Moment aufhält und kann ihn evakuieren. Es ist jedoch fraglich, inwieweit dies mit den neuen Datenschutzregeln vereinbar ist, denn schlussendlich ist es ein Leichtes, auf Basis dieser Daten ein umfangreiches Bewegungsprofil zu erstellen, von dem der Mitarbeiter nicht möchte, dass es in falsche Hände gelangt.

Transparenter Gesundheitszustand des Mitarbeiters

Und noch ein weiteres, weitgehend unbekanntes Datenschutzproblem betrifft insbesondere Mitarbeiter von Unternehmen, die im Ausland sind: Während Personaler für gewöhnlich niemals Einblick in die Gesundheitsakte ihrer in Deutschland verbleibenden Mitarbeiter erhalten könnten, wissen sie bei Expats und Auslandsreisenden – unfreiwillig – unter Umständen ganz genau, unter welchen Krankheiten und Beschwerden diese leiden. Der Grund: Laut Paragraf 17 des fünften Sozialgesetzbuches (SGB V) erhält der gesetzlich oder freiwillig in der GKV versicherte Arbeitnehmer – sowie dessen mitversicherte Angehörige – die Kosten, die während des Auslandsaufenthalts entstanden sind, durch den Arbeitgeber ersetzt. Um diese Gesundheitskosten jedoch erstattet zu bekommen, muss er die vom medizinischen Dienstleister überlassene Rechnung dem Arbeitgeber vorlegen, der somit genau Bescheid weiß, welche mitunter gravierenden oder unangenehmen (man denke nur an durch Sexualverkehr übertragbare Krankheiten) gesundheitlichen Probleme den Mitarbeiter plagen. Eine datenschutzrechtliche Lösung hat der Gesetzgeber hier bislang nicht geschaffen – die Lücke bleibt bestehen. Um Konfliktpotenzial zu reduzieren, empfiehlt es sich, eine Restkostenversicherung abzuschließen, die den Erstattungsprozess mit den Kassen direkt vornimmt, ohne dass Travel Manager oder Personaler Einblick in die Rechnungen der Mitarbeiter im Ausland nehmen kann. ◀

Tipps für Datenschutz auf Auslandsreisen

1. Nur die nötigsten Geräte und relevanten Datenträger mitnehmen, immer an dieselbe Stelle legen; Datenträger niemals unbeaufsichtigt lassen
2. Backup- und Security-Software stets auf dem neuesten Stand halten
3. Keine öffentlichen WLAN-Netzwerke „Hotspots" z. B. auf Flughäfen nutzen (besser UMTS-Sticks)
4. Auf Reise-Apps verzichten
5. Nutzung von Sichtschutzfolien auf Laptop oder Tablets
6. Kameras auf Laptops, Tablets und Smartphones zukleben
7. Daten verschlüsseln, aber Achtung: Bei vielen Ländern (z. B. USA, China, arabische Staaten) verlangt der Zoll, die Daten offenzulegen (Einreiseverbot und sogar Beugehaft drohen)
8. Geheime Daten verstecken: z. B. per Stenografie hinter einem Bild (spezielle Programme)
9. Vernetzung mit anderen Datenträgern und PCs im Unternehmen kappen
10. Zweitgeräte für Vielreisende: oft günstiger als spezielle Sicherheitsvorkehrungen, und es gibt keine Vernetzung/Synchronisation (z. B. VPN) mit anderen Geräten

Autorin
Anne-Katrin Schulz
Pressesprecherin der auf Auslandsentsendungen und Auslandsversicherungen spezialisierten BDAE GRUPPE