teclegal
Habel Rechtsanwälte
Partnerschaft

Bei Grenzkontrollen droht Durchsuchung von Computern

Die U.S. Customs and Border Protection fordert nach Medienberichten von Reisenden bei der Ein- und Ausreise an den Grenzen der USA häufig Zugriff auf die Daten mitgeführter Laptops. Auch andere Datenspeicher wie z. B. Handys, USB-Sticks, MP3-Player oder Digitalkameras sollen betroffen sein. Die Behörde verlangt von Reisenden z. B. Einsicht in den auf dem Rechner gespeicherten E-Mail-Verkehr und Zugriff auf Word-Dokumente. Wenn diese Daten durch Passwörter oder Verschlüsselungstechniken geschützt sind, muss der Betroffene die Zugangsdaten mitteilen oder die Daten entschlüsseln. Wer die Durchsuchung oder seine Mitwirkung verweigert, darf in der Regel trotzdem in die USA einreisen. In diesem Fall können die mitgeführten Datenspeicher aber beschlagnahmt werden und werden möglicherweise erst Tage oder Wochen später von den US-Behörden zurückgegeben. Die Kontrollen erfolgen angeblich verdachtsunabhängig. Bislang ist unbekannt, was mit den Daten geschieht.

Nach Auskunft des Bayerischen Landesamtes für Verfassungsschutz (LfV), das u. a. für die Spionageabwehr zuständig ist, ist die Kontrolle und der Zugriff auf mitgeführte Datenspeicher bei der Ein- oder Ausreise auch in anderen Staaten üblich. Z. B. sollen die chinesischen Behörden teilweise die Einreise verweigern oder mitgeführte Geräte sogar zerstören, wenn eine Durchsuchung oder Mitwirkung verweigert wird. Im Ausland kann auch der Einsatz von Verschlüsselungstechnik verboten und sogar strafbar sein. Gefahr droht auch, wenn über das Mobilgerät auf das Unternehmensnetzwerk zugegriffen werden kann.

Unternehmen sollten sich gegen mögliche Wirtschaftsspionage deshalb technisch und rechtlich absichern. Mögliche Maßnahmen umfassen u. a. Verhaltensanweisungen an Mitarbeiter zum Umgang mit geschäftlich genutzten Geräten. Dort kann z. B. geregelt werden, dass kritische Daten bei Auslandsreisen von mitgeführten Mobilgeräten entfernt werden müssen. Ergänzend können Mitarbeiter im Umgang mit betrieblich genutzten Mobilgeräten und im Verhalten gegenüber Grenzbeamten geschult werden, die Zugriff auf geschäftlich genutzte Geräte verlangen. Außerdem kann für Geschäftsreisen die Verwendung spezieller Reisegeräte angeordnet werden, die das Unternehmen bereitstellt und die weder kritische Daten, Verschlüsselungstechnik noch aktivierbare Unterstützung für das Unternehmensnetzwerk enthalten. Schließlich soll nach Auskunft des LfV das Risiko der Spionage geringer sein, wenn auf der Reise benötigte Unternehmensdaten über einen gesicherten Zugang im Internet zur Verfügung gestellt werden. In diesem Fall sollte der Reisende die Zugangsdaten aber nicht auf einem mitgeführten Datenspeicher ablegen. Alternativ bietet sich an, kritische Daten z. B. auf einem USB-Stick am Körper mitzuführen, weil Reisende selten körperlich durchsucht werden, so das LfV.

Rechtsanwalt Eckart C. Müller
teclegal Habel Rechtsanwälte Partnerschaft, München