

US-Grenzbeamte schnüffeln ohne Verdacht

US-Grenzbeamte behändigen ohne richterlichen Befehl Computer von Geschäftsleuten bei der Einreise. Jetzt regt sich Widerstand gegen diese Praxis.

Die Kontrolle läuft laut dem Anwalt eines Betroffenen so ab: «Bitte schalten Sie Ihren Computer an. Wir möchten ihn durchsuchen.» Wird ein Passwort aufgerufen, so muss der Einreisewillige es aushändigen. Ist er nicht bereit dazu, kann er zurückgehalten werden. Wonach genau gesucht wird, weiss der Betroffene nicht. «Wir führen eine Zufallskontrolle durch», wird ihm beschieden. Später: «Wir werden den Computer zwecks Sicherung des Inhalts zurückbehalten.» Er werde ihn zu gegebener Zeit zurückerhalten.

«Dabei wird oft die ganze Festplatte kopiert, einschliesslich gelöschter Dateien», sagt Susan Gurley von Acte, dem Verein für Geschäftsreisende in Führungspositionen (www.acte.org). Betroffen waren sogar schon Anwälte – trotz Recht auf Berufsgeheimnis. Bekannt sind auch Fälle von eingezogenen Handys und Handhelds.

In einer Umfrage unter 2500 Vereinsmitgliedern, darunter auch Schweizern, wollte Gurley wissen, «ob Mitarbeiter Ihrer Firma in den letzten drei Jahren von einer Durchsuchung oder einer Beschlagnahmung elektronischer Geräte betroffen waren». Vor drei Wochen publizierte sie die Ergebnisse: Sieben von hundert Chefs bestätigten einen Vorfall im eigenen Unternehmen. Die Geräte wurden eine Woche bis drei Monate zurückbehalten, in Einzelfällen mehr als ein Jahr lang. Fast allen Fällen gemein ist, dass die Geschäftsleute weder erfahren, «warum sie durchsucht wurden, wo ihre Daten gespeichert sind und ob die Daten nach erfolgloser Durchsuchung gelöscht wurden», kritisiert Gurley. Die US-Regierung nehme keine Stellung.

Verstoss gegen die Verfassung

In den USA regt sich deshalb heftiger Widerstand. Ende Juni gab es vor dem Rechtsausschuss des Senats eine Anhörung dazu. Die renommierte Zeitung «The New York Times» forderte vor zwei Wochen, die Grenzbeamten seien in die Schranken zu weisen. Politiker und Bürgerrechtler behaupten, dass eine auf Inhalte von Computern ausgeweitete Zollfahndung gegen die Verfassung verstosse. Denn auch in den USA gilt der Grundsatz: Keine Durchsuchung oder Beschlagnahmung ohne richterliche Erlaubnis.

So handelt jedenfalls die Schweizer Grenzwaache. «Für die Überprüfung des Inhalts eines Computers bedarf es eines Durchsuchungsbefehls. Letzterer wird von einem Untersuchungsrichter beziehungsweise Staatsanwalt ausgestellt», sagt Oliver Brand, Chef Abteilung Strafsachen von der Oberzolldirektion. Eine Ausnahme gebe es nur, wenn Gefahr in Verzug sei. Dies könnte zum Beispiel «im Rahmen einer Fahndung wegen eines schweren Verbrechens der Fall sein, wo die Kenntnis des Inhalts des Computers unverzüglich erforderlich ist», so Brand. Eine weitere Ausnahme sei, wenn Hinweise für ein zollrechtliches Delikt vorlägen, etwa Schmuggel. Aber auch dann ist der Durchsuchungsbefehl eines Zollkreisdirektors nötig, damit Fahnder zugreifen dürfen.

Schweizer wappnen sich

Konkrete Hinweise, dass Schweizer Unternehmen betroffen sind, liegen nicht vor. Der Leiter der schweizerisch-amerikanischen Handelskammer, Martin Naville, sagt, er habe von Fällen gehört, aber einen Betroffenen kenne er nicht. Eine Umfrage unter internationalen Firmen zeigt ein widersprüchliches Bild. Für die ABB sind die Grenzkontrollen «kein Problem». Nestlé schreibt, ihr seien «keine Durchsuchungen von Nestlé-Laptops durch US-Grenzbeamte bekannt». Die Grossbanken CS und UBS wollen die Kontrollen nicht kommentieren. Das IT-Unternehmen IBM spricht unverbindlich von «eventuellen Zwischenfällen, bei denen IBM eng mit den jeweiligen Behörden zusammenarbeitet». Nur das Beratungsunternehmen KPMG bestätigt die Gefahr. «Die Durchsuchungen von Laptops an US-Grenzen sind bei den von uns beratenen Firmen definitiv ein Thema», sagt Matthias Bosshardt, Experte für Datensicherheit bei KPMG.

Damit Geschäftsdaten nicht in falsche Hände gelangen, kennt er drei Strategien. Erstens: mit so wenig Daten wie möglich reisen und benötigte Daten nach Grenzübertritt online über sichere Verbindungen beziehen. Zweitens: Die

Daten verschlüsselt auf einem unauffälligen Speichermedium transportieren, beispielsweise auf der Speicherkarte einer digitalen Fotokamera. Und drittens: Dateien so gründlich verstecken, dass selbst Spezialisten, sogenannte IT-Forensiker, sie nicht aufspüren. Dafür gibt es Programme. «Forensiker sehen dann nur zufällige Daten ohne Struktur, die keinen Rückschluss auf das Vorhandensein von vertraulichen Informationen zulassen», sagt Bosshardt.



© Tamedia AG – Quellen: tagesanzeiger.ch – Agenturen – » [Fenster schliessen](#)