| Erstellt am: Dienstag | 17.06.2008 | 07:00

US-Flughäfen: Laptops als Datenkoffer
Die Durchsuchung der Notebooks von Einreisenden ist nach dem Spruch eines US-Berufungsgerichts mit dem Öffnen von Gepäckstücken gleichzusetzen und auf dem Weg zur Routine. "Daten verstecken statt verschlüsseln" sei für Geschäftsreisende aus Europa angesagt, meint der österreichische Forensiker Nicolas Ehrschwendner.

Seit ein US-Berufungsgericht Ende April das Urteil eines Bezirksrichters aufgehoben hatte, das die anlasslose Durchsuchung von Laptops durch Zollbeamte untersagt hatte, häufen sich die Meldungen, dass Passagiere aufgefordert werden, das mitgeführte Notebook hochzufahren.

Das dreiköpfige Richtergremium hatte nämlich entschieden, dass ein Laptop ein Transportbehälter sei, der den Status eines Koffers habe, also vom Zoll durchsuchbar sei.

Die "Stöberfahndung"
Darauf folgen die unterschiedlichsten Prozeduren, je nach Reaktion des Passagiers und Beamten, zumal es offenbar keine genormte Vorgangsweise seitens der US-Zollbehörden gibt.

Einmal werden vor dem Passagier der Browser-Cache und Mailfolder durchstöbert, einmal sieht sich der Zöllner die Festplatte genauer an. Dann wieder verschwinden Beamte mit den Maschinen und kehren erst nach Stunden wieder.

"Security by curiosity"
"Ich würde das als 'security by curiosity' bezeichnen. Professionell ist das ganz sicher nicht", sagt der Computerforensiker Ehrschwendner zu ORF.at.

Ausgenommen natürlich, wenn im letzteren Fall die Festplatte ausgebaut, Bit für Bit kopiert und mit einer Prüfsumme versehen wurde, denn nur dann würden von der Maschine stammende Dateien vor Gericht als Beweismittel zugelassen.

Suche nach Fotos
"Bei jedem Start eines Betriebssystems werden auf der Festplatte Zeitstempel manipuliert, temporäre Dateien angelegt, die Daten werden verändert und sind daher nicht mehr beweistauglich." Das gelte freilich nur "vor einem ordentlichen Gericht in einem Rechtsstaat", fügt Ehrschwendner hinzu.

Zur Abwechslung wird in den USA wieder mehr nach Kinderschändern Ausschau gehalten als nach Terroristen

Kinderschändern Aussehen gehalten als nach Terroristen, man sucht also meistens nach Fotos.

Schuhe und Festplatten
Dazu gibt es auch einen Anlassfall aus dem Jahr 2004, als der Laptop eines in die USA einreisenden Kanadiers neben gewöhnlichen Nacktfotos auch Fotos von missbrauchten Kindern enthielt.

So wie seit dem Auffliegen des "Schuhbombers" Richard Reid Passagiere die Schuhe ausziehen müssen, wurde nach Festnahme des Kanadiers das Hochfahren des Laptops angesagt.

"Host protected Area"
Zwar sind längst Programme zur Mustererkennung auf dem Markt, die etwa nach Fotos suchen und aus der Farbverteilung schließen, dass sie nackte Haut enthalten. Im Falle von Flughafenkontrollen hält Ehrschwendner das aber kaum für praktikabel. Wenn nicht ein großer, schneller Rechner für die Beamten vorhanden sei, dauere das zu lange.

Zudem sei es möglich, mit einem Festplattenkommando eine "Host protected Area" einzurichten, so dass Teile der Platte einfach nicht sichtbar seien und daher auch vom Kopiervorgang gar nicht erfasst würden.

Gelernte Forensiker
Das in Windows eingesetzte NTFS-Dateisystem unterstütze zum Beispiel "Alternate Data Streams", womit man [verkürzt gesagt, siehe Links unten] an eine unverfängliche Datei andere Dateien anhängen könne, ohne dass die sichtbar würden.

"Es hängt immer davon ab, wie intensiv und mit welchen Mitteln man sucht", sagt Ehrschwendner - und ob da ein gelernter Forensiker am Werke sei, der solche Methoden natürlich kenne, oder eben nicht.

"Verstecken besser als Verschlüsseln"
Wie aber schützt sich zum Beispiel ein Anwalt oder Berater, der vertrauliche Daten von Dritten auf dem Rechnern mitführt, davor, dass die Daten, für deren Vertraulichkeit er haftet, nach der Landung in den USA kopiert werden?

Noch dazu, wo dort nahezu täglich eine mittlerweile unübersehbare Anzahl von Datenlecks und -verlusten bei US-Behörden durch die Medien gehen?

"Verstecken ist besser als Verschlüsseln", sagt Ehrschwendner, "denn Verschlüsselung weckt automatisch Verdacht."

Nackte Notebooks
In der Tat wurde eine ganze Reihe Laptops beschlagnahmt, oder es wurde mit dieser Maßnahme gedroht, wenn sich Reisende etwa unter Berufung auf die Vorschriften ihres Unternehmens weigerten, verschlüsselte Festplatten den Zöllnern zugänglich zu machen.

Auf die Frage, was vom Vorschlag des Sicherheitsexperten Bruce Schneier zu halten sei, die - sicher verschlüsselten - Daten auf einem USB-Stick zu transportieren und das Notebook sozusagen nackt mitzuführen, meint Ehrschwendner: "Dann werden sie das Notebook aller Wahrscheinlickeit nach ebenfalls beschlagnahmen."

"Dateien nicht mitführen"
Im Grunde könne man unter diesen Umständen "Daten eigentlich nur nicht mitführen". Am sichersten sei noch immer eine VPN-Verbindung im jeweiligen Zielland, um sensible Daten dann von einem eigenen Server abzuholen, so der Experte abschließend.

Mittlerweile verdichten sich die Hinweise darauf, dass sich die Suche der Zollbehörden in Zukunft möglicherweise nicht auf Indizien für schwere Verbrechen wie Kindesmissbrauch und Terrorismus auf mitgeführten Datenträgern beschränken wird.

ACTA und die "Raubkopien"
Hinter verschlossenen Türen verhandeln die USA mit Repräsentanten Englands, Deutschlands, Frankreichs, Japans sowie der EU-Kommission über ein neues "Anti-Produktpiraterie"-Abkommen [ACTA].

Das einzige dazu bisher bekanntgewordene Dokument enthält eine ganze Anzahl von neuen Ermächtigungen für Zollbeamte und andere Behörden und ist so allgemein formuliert, dass die Durchsuchung von Laptops, iPods und anderen Datenträgern etwa nach "Raubkopien" in der Bandbreite locker enthalten ist.

"Festplatten zu durchsuchen fällt nicht in die Kompetenz von österreichischen Zollbeamten", sagt der Pressesprecher des österreichischen Finanzministeriums, Harald Waiglein, zu ORF.at.

Dafür brauche es hierzulande nämlich einen richterlichen Bescheid.

Ehrschwendner betreibt mit seinem Kompagnon Peter Franck das auf Datenrettung und Computerforensik spezialisierte Unternehmen Attingo mit Sitz in Wien und Hamburg.

IPod-Kontrollen auf dem Flughafen
Attingo

"Alternate Data Streams"
"Host protected Area"

[futurezone | Erich Moechel]