Tages-Anzeiger

4. Mai 2009

# Bakom: Passleser lässt sich aus 500 Metern anzapfen

*Beim Test durch das Bundesamt für Kommunikation sind die Lesegeräte für den biometrischen Pass durchgefallen – der Bund muss nachbessern.*

Für die Fachleute ist der Fall klar: «Bei beiden Geräten kann das Signal mit einfachen Mitteln beim normalen Lesevorgang mitgehört werden.» Der Befund lässt aufhorchen. Denn er stammt nicht aus der Abstimmungspropaganda gegen den biometrischen Pass, sondern aus einem offiziellen Bericht des Bundesamts für Kommunikation (Bakom). Dieses wurde vom Bundesamt für Polizei (Fedpol) beauftragt, die «Datenauslesung auf Distanz beim biometrischen Pass» zu untersuchen.

**Mehrere Sicherheitsmängel**

Die Frequenzspezialisten des Bakom wurden fündig. In ihrem bisher unveröffentlichten Schlussbericht vom 28. November 2008, der dem «Tages-Anzeiger» vorliegt, decken sie vor allem bei den Passlesern mehrere Sicherheitsmängel auf:

Mithören aus der Luft: Um den verschlüsselten Chip des biometrischen Passes lesen zu können, brauchen Grenzwächter und Fluggesellschaften ein dazu passendes Lesegerät mit Magnetfeld. Das Bakom hat zwei Modelle getestet: den Cross Match A100 und das ACG Passport Reader Module. Bei beiden konnte es mit einer 50 Zentimeter grossen Antenne problemlos Daten abfangen, die das Lesegerät aus dem Pass abrief. Das funktioniere auch mit einem gewöhnlichen Kurzwellenempfänger. Fazit der Tester: «Unter idealen Bedingungen ist das drahtlose Mithören bis zu einer Distanz von etwa 25 Metern möglich.» Der gewonnene Datenstrom könne nach einer Aufzeichnung auch offline weiterbearbeitet werden.

Mithören über das Stromnetz: Aus noch weit grösserer Distanz lassen sich die Lesegeräte über das Stromnetz anzapfen. Denn die Spezialisten des Bakom fanden heraus, dass die Apparate (mit angeschlossenem Notebook) die gelesenen Daten «ungewollt über das 230-Volt-Netz weiterleiten». Messungen und Berechnungen hätten gezeigt, dass «ein Mitlesen auf der Hausinstallation bis zu einer Distanz von über 500 Metern möglich ist».

**Lesegeräte bekommen nun Filter**

Roman Vanek vom Fedpol betont zwar, dass die Daten, die drahtlos und über das Stromnetz abgefangen wurden, immer noch verschlüsselt seien. Dennoch hat der Bericht des Bakom im Departement von Eveline Widmer-Schlumpf für Aufsehen gesorgt. «Das Fedpol hat die Ergebnisse mit Interesse zur Kenntnisse genommen», sagt EJPD-Sprecher Guido Balmer. Den Befund, dass sich die Passleser übers Stromnetz abhören lassen, stufte die Bundespolizei gar als derart wichtig ein, dass sie

ihn der Internationalen Zivilluftfahrtbehörde ICAO präsentierte. Deren New Technologies Working Group überwacht weltweit die Einführung und den Einsatz biometrischer Pässe.

Das Fedpol zieht jetzt Konsequenzen aus dem brisanten Bericht: Es will vor der Einführung des neuen Passes die Lesegeräte mit Filtern nachrüsten. Damit setzt es Empfehlungen des Bakom um. Dieses legte dem Fedpol dringend nahe, die Passleser besser abzuschirmen und darin Netzfilter einzubauen, damit das Mitlesen aus der Luft und übers Stromnetz erschwert wird. «Damit macht die Schweiz mehr, als die für elektronische Geräte anzuwendenden Normen verlangen», heisst es beim EJPD. Andere Warnungen des Bakom schlägt es dagegen in den Wind.

**Braucht der E-Pass eine Schutzhülle?**

Das Bundesamt für Kommunikation (Bakom) warnt davor, den biometrischen Pass ohne Schutzhülle aufzubewahren. Grund: Es hat nachgewiesen, dass sich der Pass aus Distanz heimlich lesen lässt – auch wenn dieser zugeklappt in der Handtasche liegt.

Das Lesen gelang einerseits aus 35 bis 50 Zentimeter Entfernung mit einer Antenne, die in einem Koffer versteckt war. Andererseits bauten die Tester eine Antenne in einen Türrahmen ein, die den Chip im Pass sogar lesen konnte, wenn sich dessen Besitzer langsam bewegte. «Der Bau einer Türrahmenantenne ist aufwendig. Wenn sich aber an einem Schalter oder an einer Kasse eine Person für 10 Sekunden nicht bewegt, kann man die Konstruktion stark vereinfachen.»

Der E-Pass nur mit Hülle? Für den Projektausschuss des Bundesamts für Polizei zielt diese Empfehlung ins Leere. «Die Hülle ist unnötig», sagt Guido Balmer, Sprecher des Justizdepartements. Auch wenn der Chip im Pass heimlich von ausserhalb aktiviert werden könne, seien Personalien und Foto durch den Zugriffsschutz der Internationalen Zivilluftbehörde gesichert.

Diese Basic Access Control verhindere, dass sich die Daten beim Vorbeigehen ausspionieren liessen. Tatsächlich sagt auch das Bakom, dass es dafür «die Daten zur Generierung des Schlüssels» brauche. Will jemand noch dazu an die Fingerabdrücke herankommen, muss er einen weiteren Sicherheitscode knacken, über den nur Schweizer Behörden verfügen. Balmer: «Wer genug Zeit hat, kann alle Schlüssel ausprobieren. Das dauert aber bis 300 Jahre.» (pak)