



Zum TV-Beitrag der Sendung „einstein“ am 19. März 2009

Der biometrische Pass ist sicher: „einstein“-Beitrag wird von SF relativiert

Der Beitrag der SF-Sendung „einstein“ vom 19. März 2009 betreffend Sicherheit des neuen biometrischen Passes hat in interessierten Kreisen hohe Wellen geworfen. Da das Komitee „Ja zur Reisefreiheit“ feststellen musste, dass in der Schlussphase des Abstimmungskampfes dieser Beitrag immer öfter als „Beweis“ für die Unsicherheit des neuen e-Passes verwendet wird, haben wir uns diesen Beitrag nochmals genau angeschaut:

In der Anmoderation dieses Beitrages wird angekündigt, der neue biometrische Pass sei „technisch knackbar“ und es wird auf die „Abdrücke der Zeigefinger“ verwiesen, obwohl im Chip des neuen Passes lediglich die Vektoren der Fingerabdrücke abgelegt werden. Zum Schluss der Sendung wird bilanziert, nach 4 Stunden seien „...die biometrischen Daten auf dem Laptop des Hackers...“.

Dazu befragt, meinte der Chefredaktor von SF, Ueli Haldimann, in einem Mail von gestern 27. April 2009 an das Komitee:

„Der Einstein Beitrag basierte zu 100% auf einem „Temps Présent“-Beitrag von Oktober 2008. Er wurde von den welschen Kollegen im Spätsommer 2008 gedreht.

Der Beitrag hat gezeigt, wie ein HEUTIGER biometrischer Pass geknackt (dh. von Unbefugten gelesen) werden kann. Im Text wurde nie etwas anderes gesagt. Der HEUTIGE biometrische Pass enthält keine Fingerabdrücke. Die Diskussion über Vektoren und ähnliches ist hinfällig.

Der Beitrag enthielt leider einen andern Fehler. Im biometrischen Pass wird das Gesicht nicht 3D-mässig vermessen, sondern nur 2D-mässig. Wegen dieses Fehlers, der nicht matchentscheidend ist, wurde der Beitrag vom Netz genommen.“

Fazit:

Im „einstein“- resp. „Temps Présent“-Beitrag wurde ein bestehender Pass 06 (mit einem abgespeicherten Foto, jedoch ohne Fingerabdrücke) für den neuen biometrischen Pass ausgegeben. Zudem wurden zur im Beitrag gezeigten Übungsanlage keine Angaben gemacht (so wurde z. B. nicht erwähnt, dass entscheidende Eckwerte zum vorliegenden Pass bekannt waren, weil der Inhaber bekannt war). Dadurch mussten viel weniger Kombinationen für das Basic Access Control (BAC) durchprobiert werden. Kurz: Der Beitrag spiegelte falsche Tatsachen vor.