«Diebstahl der Identität ist das grösste Risiko»

Ein ETH-Informatiker warnt vor Schwachstellen beim biometrischen Pass – die Bundesbehörden widersprechen

Professor als Hacker. ETH-Mann Serge Vaudenay beweist, dass man E-Pässe problemlos knacken kann. Foto Mischa Christen

RUEDI STUDER, Lausanne

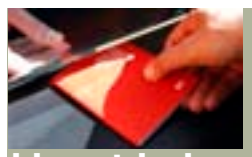
Die heute benutzte Technik für biometrische Pässe sei nicht sicher genug, findet der Verschlüsselungsexperte Serge Vaudenay von der ETH Lausanne. Einzig die Fingerabdrücke seien genügend gesichert.

Bereits 60 Staaten stellen derzeit biometrische Pässe aus – seit 2006 tut dies im Rahmen eines Pilotprojekts auch die Schweiz. Auf einem kleinen Chip im Passdeckel werden dabei die üblichen Personendaten sowie ein digitales Foto des Passinhabers gespeichert.

Im Abstimmungskampf um die Vorlage über den biometrischen Pass, auch E-Pass genannt, ist auch die Sicherheit der Chipdaten ein Thema. Kein Problem, heisst es dazu beim Bund: «Die Daten im neuen E-Pass sind in Anwendung der internationalen Normen so gesichert, dass sie nicht unbemerkt manipuliert oder kopiert werden können», sagt Roman Vanek vom Bundesamt für Polizei (Fedpol). «Werden alle Normen bei der Produktion und der Kontrolle von Ausweisen angewendet, treten keine Sicherheitsmängel auf.»

IN SEKUNDEN GEKNACKT. Ganz anders sehen dies die Gegner der Vorlage: Professionelle Hacker könnten die Daten knacken, argumentieren sie. Einer, der sich mit Verschlüsselungstechnik auskennt, ist der Franzose Serge Vaudenay, Leiter der Abteilung Sicherheit und Kryptografie von der Fakultät für Informatik und Kommunikation der ETH Lausanne.

Anhand eines von der BaZ mitgebrachten Passes demonstriert er, wie schnell sich die Daten von einem Chip lesen lassen, die nur mit der Technik «Basic Access Control» (BAC; grundlegende Zugriffskontrolle) gesichert sind. Ohne irgendwelche Vorangaben dauere das Knacken des Chips mehrere Stunden, so Vaudenay. «Wir haben es schon in vier Stunden geschafft.» Beschafft man sich jedoch Passnummer, Geburtsdatum und Ablaufdatum des Passes, lässt sich der Chip mit einem handelsüblichen Softwareprogramm innert Kürze lesen.



biometrischer pass
Eidgenössische Abstimmung vom 17. Mai 2009

Vaudenay demonstriert dies auch gleich, indem er diese drei Angaben auf seinem Computer eintippt und den Pass auf ein Lesegerät legt – wenige Sekunden später präsentieren sich sämtliche, auf dem Chip gespeicherte digitale Angaben auf seinem Computer. Nicht nur die üblichen Personendaten, sondern auch das digitale Foto. Zudem lässt sich auch die Signatur des Passes ablesen. In der heute bei biometrischen Pässen verwendeten BAC-Technik sieht Vaudenay denn auch den grössten Schwachpunkt. Diese sei «miserabel» und erlaube das Kopieren und Klonen von Pässen. «Der Diebstahl der Identität ist das grösste Risiko», sagt er.

FINGERABDRUCK SICHER. Eine Aussage, die bei Fedpol-Mann Roman Vanek Stirnrunzeln auslöst: «Ende 2008 waren weltweit rund 100 Millionen E-Pässe in Umlauf, Ende 2009 werden es 160 Millionen sein», sagt er. «Und bisher ist keines der Horroszenarien eingetroffen.» Das Lesen des E-Passes ohne die von Vaudenay benutzten Angaben sei praktisch unmöglich, sagt Vanek: «Wenn man keinerlei Angaben hat, bräuchte man 300 Jahre, um den Chip zu knacken.» Selbst mit den benötigten Angaben sei es nicht möglich, den Chip im Vorbeigehen oder aus der Ferne zu lesen. Das bestätigt Vaudenays Demonstration: Erst bei einer Distanz von wenigen Zentimetern funktioniert der Datenaustausch zwischen Chip und Lesegerät.

Der Franzose verweist aber darauf, dass einer seiner Forscherkollegen das Auslesen eines E-Passes schon aus mehreren Metern Distanz geschafft habe. Die Gegner des biometrischen Passes befürchten denn auch, dass der E-Pass dereinst der Überwachung der Bürger dienen könnte. Technisch wäre dies laut Vaudenay denkbar, aber «es gibt einfachere Wege, die Leute zu verfolgen, beispielsweise über das Handy».

Immerhin in einem Punkt sind sich Vanek und Vaudenay einig: bei der Sicherheit der Fingerabdrücke, die im geplanten E-Pass zusätzlich erfasst werden sollen. Diese werden durch den Zugriffschutz «Extended Access Control» (EAC; erweiterte Zugriffskontrolle) viel besser gesichert. Wer den Fingerabdruck lesen will, braucht dazu ein spezielles Auslesezertifikat. «Die Fingerabdrücke zu lesen ist unmöglich, da es einen Zugriffsschlüssel braucht», sagt Vanek. «Technisch sind die Fingerabdrücke sicher», bestätigt Vaudenay.

Deshalb plädiert er dafür, dass die EAC-Technik nicht nur beim Fingerabdruck, sondern für sämtliche auf dem Chip abgelegten Daten zum Zug kommt. Zudem hält er es für unnötig, dass die Fingerabdrücke zusätzlich auf einer zentralen Datenbank gespeichert werden.

SICHERERE TECHNIK. Als Franzose kann Vaudenay am 17. Mai zwar nicht mitentscheiden. Wäre er aber stimmberechtigt, würde er Nein stimmen, wie er der BaZ verrät. Die Schweizer könnten als einziges Volk über die Sicherheitstechnik beim E-Pass abstimmen, so Vaudenay – und damit auch ein Signal für einen besseren Schutz setzen. «Der biometrische Pass ist eine Notwendigkeit», so Vaudenay, «es braucht aber eine sicherere Technik dafür.»