



Stefan Grünwald

## Wasserdichte Biometrie?

*Univ.-Ass. Dipl.-Ing., TU Graz,  
Institut für Wirtschafts- und  
Betriebswissenschaften, Abteilung für  
Unternehmensführung und  
Organisation*

**W**ie viele Passwörter und PINs muss man sich heute eigentlich merken? Sicherheitsbewusste Zeitgenossen, welche eine korrekte Handhabung von Zugangscodes praktizieren, kommen mit Leichtigkeit an die zwanzig Stück. Wichtige sollte man natürlich nicht notieren, und eine verschlüsselte Passwortsammlung trägt auch nicht zur bequemen Nutzung bei. In dieser Situation scheint die Biometrie ein Silberstreif am Horizont zu sein. Ist sie das aber wirklich und was genau steckt hinter dem Begriff?

**U**nter Biometrie lassen sich Erkennungssysteme anhand von individuellen menschlichen Merkmalen einordnen; neben den bekannten Verfahren wie Fingerabdruck-, Gesichts-, Iris-, Stimmerkennungssystemen zählen dazu auch Unterschriftenerkennung und einige andere Verfahren.

**V**orteilhaft an der Biometrie scheint oberflächlich betrachtet, dass sie eine praktikable und sichere Handhabung gewährleistet, da man z.B. Finger, Auge oder Gesicht meistens bei sich hat. Natürlich müssen die Systeme ausgeklügelte Lebenderkennung mittels Pulsabastung oder Überprüfung der Augenaktivität integriert haben, um sie vor

allzu leichtem Missbrauch zu schützen. Doch auch nach dem neuesten Stand der Technik (und damit teure) eingesetzte Systeme sind vor Fehlern und Umgehung nicht gefeit.

Unterschiedliche Testreihen kommen zu ähnlichen Ergebnissen, nämlich zu Fehlerraten von 2 bis zu 20 %. Die technische Herausforderung an der Biometrie liegt daran, dass die abgenommenen biometrischen Daten naturgemäß variieren, also die Rohdaten ein und derselben Person sehr stark schwanken. Selbst bei einer Erkennungssicherheit von 99,99 % (die heutige Systeme nicht einmal unter Laborbedingungen schaffen) würden im Mittel bei 10 Millionen kontrollierten Personen 1000 Fehlalarme ausgelöst werden bzw. 1000 Terroristen mit gefälschten Papieren könnten ungehindert passieren. Beim heutigen Stand der Technologie sind biometrische Systeme für den Masseneinsatz noch ungeeignet.

Ein breiter, alltagstauglicher Einsatz wird nicht vor fünf, realistischer in zehn Jahren zu erwarten sein.

**D**atenschutzrechtliche Aspekte bei der Erhebung, Speicherung (zentral oder dezentral) und Übertragung von Biometriedaten sind sicherlich in die

Diskussion einzubeziehen, um die Bürger vor Austausch und Verknüpfung ihrer Daten zu Marketingzwecken zu verhindern.

**D**er hohe organisatorische Aufwand bei der Implementierung biometrischer Systeme lässt darüber hinaus die Wirtschaftlichkeit aktueller Anwendungen in einem ungünstigen Licht erscheinen. Die extrem hohen Sicherheitsanforderungen bei der Aufnahme von Referenzmustern und dem Aufbringen der Merkmale auf Chipkarten erhöhen zusätzlich die Kosten.

**I**n dunklen Zeiten des letzten Jahrhunderts war es schon einmal üblich, Fingerabdrucke auf Ausweisen zu haben. In unseren Tagen wird nun unter dem Deckmantel der Terrorismusbekämpfung und durch Schüren von Ängsten in Demokratien versucht, den ohnehin schon sehr gut überwachten Menschen noch etwas gläserner zu machen, um noch mehr Kontrolle zu haben. Die Gesellschaft läuft heute Gefahr, einige von Orwells Visionen in 1984 – welche die (meisten) Individuen nicht akzeptieren würden – in der Realität zu überholen.

*Stefan Grünwald*