

## **Biometrie - eine kontroverse Technologie**

**Biometrie präsentiert sich als Zukunftslösung für IT-Sicherheitsprobleme und wird allmählich zum Bestandteil unseres täglichen Lebens. Die Technologie ist jedoch nicht unfehlbar und gibt Anlass zu gewissen Bedenken, vor allem im Hinblick auf persönlichen Datenschutz. Im Folgenden finden Sie einige Erklärungsansätze:**

Angesichts weit verbreiteter Bedrohungen durch Virenangriffe, Trojanische Pferde und andere Hacker-Methoden wenden sich sowohl individuelle Benutzer als auch Unternehmen zunehmend vermeintlich unfehlbaren Lösungen wie der Biometrie zu. Die futuristischen Aspekte von biometrischen Methoden wie Fingerabdruck-, Hand- oder gar Iriserkennung üben eine große Faszination auf die Öffentlichkeit aus und werden von den Verantwortlichen gefördert, da sie sehr hohen Schutz bieten - und das nicht nur im Bereich der Informationssicherheit. Die Europäische Kommission empfiehlt die Aufnahme von biometrischen Elementen in EU-Personalausweise, und eine japanische Bank setzt bereits ein Handerkennungssystem ein, damit ihre Kunden nicht länger einen PIN-Code eingeben müssen, wenn Sie den Geldautomaten benutzen. Es sind bereits seit einigen Jahren verschiedene Informationssicherheitslösungen auf dem Markt, die auf biometrischen Methoden basieren. In einigen Schulen wird sogar Fingerabdruckererkennung eingesetzt, um den Zugang zur Mensa zu autorisieren.

### **Die Technologie ist nicht unfehlbar**

Die Mitgliedsstaaten der EU sehen sich dem Druck der USA ausgesetzt und müssen sich entscheiden, ob biometrische Elemente in Identitätsdokumente aufgenommen werden sollen oder nicht. Experten sind allerdings der einhelligen Meinung, dass die Konsequenzen einer so breit angelegten Verwendung der Technologie nicht abzuschätzen sind. Biometrie ist derzeit noch weit davon entfernt, unfehlbar zu sein - die Fehlerraten in Bezug auf Gesichtserkennung liegen bei bis zu 40 Prozent. Fingerabdruckererkennung gilt als die zuverlässigste biometrische Methode, im Jahr 2002 durchgeführte Forschungen in Japan ergaben jedoch, dass auch Fingerabdrücke gefälscht werden können: Es wurden Gelatinekopien von Fingerabdrücken hergestellt, mit denen elf der 15 biometrischen Systeme getäuscht werden konnten. Dieses Experiment wurde im letzten Chaos Computer Club in Berlin wiederholt - diesmal kopierten die teilnehmenden Hacker Fingerabdrücke unter Verwendung von Flüssiglatax.

### **Theoretisch unveränderbare und unersetzliche „Hilfsmittel“**

In den meisten Fällen müssen die Informationen für Fingerabdruck-, Iris-, Hand- oder Gesichtserkennung gespeichert werden. Wo zieht man jedoch die Grenze zwischen der notwendigen Speicherung von Informationen und einer Verletzung des Datenschutzes? Laut Angaben von Datenschutzorganisationen führt die Verbreitung von Biometrie - besonders in Ländern, in denen die Menschenrechte nicht sehr geachtet werden - zur weit verbreiteten Speicherung persönlicher Daten. Die französische Datenschutzbehörde CNIL befand, dass der Einsatz der Fingerabdruckererkennung zur Identifizierung von Schülern in Schulmensen „übertrieben“ sei.

Biometrie gibt darüber hinaus Anlass zu kontroversen Argumenten, weil sie auf „Hilfsmitteln“ basiert, die bei auftretenden Problemen nicht verändert oder ersetzt werden können. Ihre größten Kritiker reden sogar von möglichem „Organdiebstahl“, sollte der Einsatz von Hand- oder Fingerabdruckererkennung weite Verbreitung im Bankwesen finden. Andere zeichnen ein düsteres Bild der Zukunft, indem sie Vergleiche zum Film „Minority Report“ aufstellen: Der Protagonist des Films muss sich einer Augentransplantation unterziehen, nachdem seine Iris auf die „Schwarze Liste“ der Behörden gesetzt wurde. Wenn es auch noch nicht absehbar ist, dass solche haarsträubenden Science-Fiction-Beispiele zur Realität werden, steht die Biometrie doch vor der Herausforderung, einen gesunden Mittelweg zwischen Sicherheit und Datenschutz zu finden - und diese Diskussion steht noch ganz am Anfang.