

Datenschutz in der Biometrie

38. Jahrestag der Gesellschaft für Informatik

8. – 13. September 2008 in München

Vortrag am 9. Sep. 2008

Dr. Manfred Bromba - Biometrieberater

<http://www.bromba.com>

TeleTrust auf der Suche nach Lösungen

TeleTrust ist ein interdisziplinärer Zusammenschluss von ca. 85 Mitgliedern aus **Industrie, Wissenschaft u. Forschung und Behörden** und hat sich zur Aufgabe gemacht, **vertrauenswürdige** und verlässliche Rahmenbedingungen für den Einsatz von **Informations- und Kommunikationstechnik** zu schaffen

Innerhalb der TeleTrust ist die Arbeitsgruppe 6 zuständig für das Thema **Biometrie**

Innerhalb der AG 6 hat sich ein **Arbeitskreis Recht** gebildet, der sich mit rechtlichen Fragen des Einsatzes von Biometrie beschäftigt

Der AK Recht setzt sich aus **Datenschutzbeauftragten und Biometrie-Experten** zusammen

Um potenziellen Anwendern und Betreibern mehr Sicherheit bei der Auswahl und beim Betrieb biometrischer Systeme zu geben, wurde ein Projekt zur Erarbeitung eines **White Papers** initiiert

Inhalt des White Papers

1 Grundlagen

2 Gefährdungen

3 Schutzmaßnahmen

4 Empfehlungen

5 Entscheidungen von Gerichten und Datenschutzkommissionen

Autoren: Heinz Biermann, Manfred Bromba, Christoph Busch, Gerrit Hornung, Martin Meints, Gisela Quiring-Kock

Download: <http://www.teletrust.de/index.php?id=150>

Google: <white paper datenschutz biometrie>

Was ist Biometrie?

In diesem Zusammenhang: *automatisierte Erkennung von Individuen anhand ihrer verhaltensmäßigen oder biologischen Charakteristika*

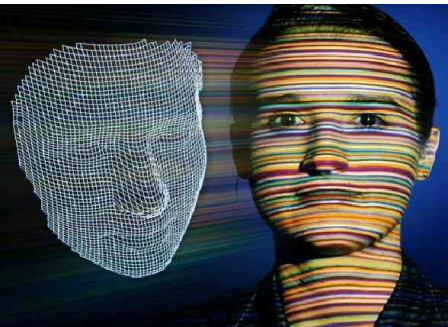
Wie funktioniert Biometrie?

Voraussetzung: Die Charakteristika müssen möglichst **individuell** und **konstant** sein, sollten **bei jedem** Individuum vorkommen, gut **messbar** und dabei **anwenderfreundlich** sein.

Umsetzung: Ein Charakteristikum lässt sich über einen **Sensor** in ein Muster umwandeln, das sich mit den Methoden der **Mustererkennung** bearbeiten und als **Referenz** abspeichern lässt.

Zur Erkennung wird das Referenzmuster mit einem aktuell über den Sensor aufgenommenen Muster **verglichen** und bei ausreichender Übereinstimmung als **wiedererkannt** erklärt.

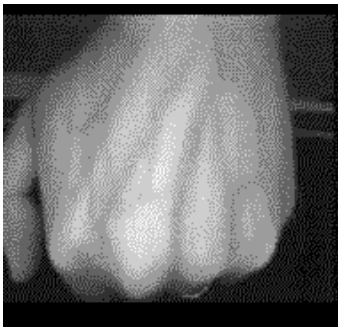
Biometrische Charakteristika



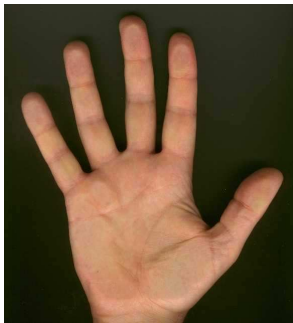
Gesicht (3D)



Retina



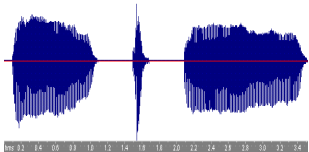
Venenstruktur



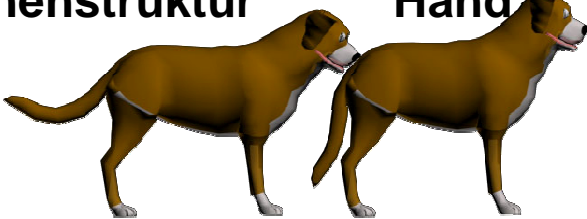
Hand



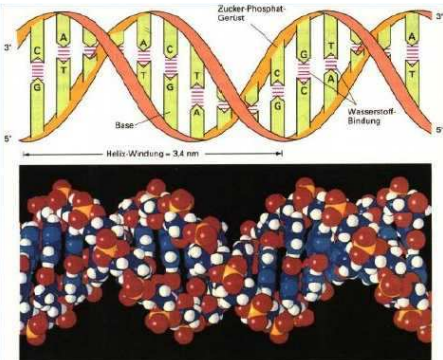
Unterschrift



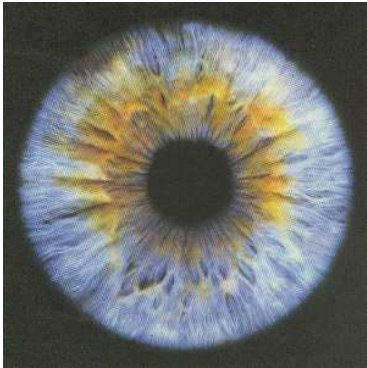
Stimme



Geruch



DNA



Iris



Fingerabdruck

Was ist Datenschutz?

Aufgabe des Datenschutzes ist es, die Verarbeitung personenbezogener Daten zu regeln

Dabei steht das vom Bundesverfassungsgericht im Volkszählungsurteil entwickelte Grundrecht auf informationelle Selbstbestimmung im Mittelpunkt

Die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen, darf nur durch Rechtsvorschriften eingeschränkt werden

Um wen geht es im White Paper?

White Paper wendet sich an **Betreiber** und „**Betroffene**“

Biometrie für Mitarbeiter

Insbesondere in größeren Unternehmen, die dem Mitbestimmungsgesetz unterliegen

Zutritts-, Zugangs- und Zugriffskontrolle

Biometrie für Verbraucher

Z.B. Bezahlanwendungen, Mitgliedsausweise

Nicht betrachtet werden:

Biometrie für persönliche Anwendungen (Betreiber = Betroffener)

Dieser Fall ist relativ einfach abzuhandeln

Biometrie für Staatsbürger, Reisende und Flüchtlinge

Diese Fälle wurden nicht betrachtet

Gefährdungen

Warum braucht die Biometrie Datenschutz?

Biometrische Daten haben in Bezug auf Datenschutz insbesondere mit zwei Problemfeldern zu tun:

1. Biometrische Daten lassen sich (näherungsweise) als individuelle Personen Kennziffern nutzen

Das Bundesverfassungsgericht hat sich 1983 in seinem Volkszählungsurteil sehr kritisch zur Einführung solcher Kennziffern geäußert

Biometrische Daten bleiben teilweise ein Leben lang erhalten und lassen sich nicht ändern oder zurückziehen

2. Biometrische Daten können Zusatzinformationen enthalten

D.h., Informationen, die zur Erkennung nicht unbedingt erforderlich sind, aber Aufschlüsse über sonstige private Eigenschaften des Betroffenen liefern könnten

Bio-Charakteristika als "Personenkennziffer"

Identitäts"diebstahl" (Vortäuschen einer fremden Identität)

Beispiel: Kreditkartennutzung über Internet – warum ein Problem?

Biometrie: Problem, wenn biometrisches Merkmal als geheim angesehen werden muss

Datenverkettung

„Suchmaschine“

Google Picasa 3: „name tags“ mit Gesichtserkennung

Überwachung (wie lässt sich Kriminalität perfekt aufklären?)

Datenzusammenführung (ID, Ort, Zeit, Tätigkeit)

Biometrie als gemeinsamer Identifikator (ID)

Identifizierungsfehler als Gefahr für Betroffene

Wann ist eine **falsche** Identifizierung eine Gefahr für den Betroffenen?

Wenn das **Vertrauen in das Ergebnis einer Identifizierung größer ist als die Zuverlässigkeit des Identifizierungsverfahrens**

und in der Folge der Betroffene unverschuldet auf dem Schaden sitzen bleibt

Positives Beispiel: Kreditkartenzahlung: Haftungsbegrenzung

Maßnahme 1: Vertrauen anpassen

Setzt genaue Verfahrenskennntnisse voraus

Maßnahme 2: Zuverlässigkeit erhöhen

Hat natürliche Grenzen

Maßnahme 3: Möglichkeit der Rückgängigmachung durch den Betroffenen

Beispiele für Identifizierungsfehler

Falschrückweisung (FRR, FER): Fluggast kann Reise nicht antreten, weil Verifizierung mit Reisepass mehrfach fehlschlägt

Abhilfe: Diskriminierungsfreies Ausweichverfahren anbieten

Falschakzeptanz (FAR, FIR): Bei einer DNA-Analyse wird der Betroffene fälschlich als gesuchter Verbrecher identifiziert und arrestiert

Abhilfe: Es müssen weitere Identifikatoren und Indizien zum Einsatz kommen

Fälschung: Einkauf mit falschem Fingerabdruck

Abhilfe: Kulanz mit nachfolgendem Fingerwechsel, Unterschrift zur Verifikation heranziehen

Sonderfall: Einkauf mit eigenem Fingerabdruckplagiat und Leugnung

Identifizierung als Gefahr für den Betroffenen

Wann ist eine **richtige** Identifizierung eine Gefahr für den Betroffenen?

1. Wenn das Ergebnis falsch interpretiert wird

Beispiel: Fingerabdruck wird am Tatort gefunden

Das ist kein Beweis für die Täterschaft, sondern höchstens für die Anwesenheit des Betroffenen

Natürlich könnte ein gewiefter Täter auch falsche Spuren auslegen. Das war aber zumindest in den letzten 100 Jahren kein ernsthaftes Problem!

2. Wenn das politische System totalitär ist

Beispiel: Diskriminierung von Bevölkerungsgruppen

Vorbeugender Verzicht erforderlich?

Schutzmaßnahmen

Schutz der Referenzdaten

Gefahr: Rekonstruktion der Ursprungsdaten (prinzipiell möglich!)

Nachfolgend Erstellung von Plagiaten und Identitätsbetrug, da biometrische Systeme nur unzureichend gegen Fälschungen schützbar sind

Schutz vor Diebstahl

IT-Standardmaßnahmen

Schutz gestohlener Daten vor Missbrauch

Verschlüsselung

- 100-jährige Verschlüsselungshaltbarkeit

- Mehrfachverschlüsselung (Algohersteller, Integrator, Betreiber, Betroffener)

Erschwerung der Personen-Beziehbarkeit ("Schlüssel mit Adressanhänger")

Verzicht auf die Nutzung standardisierter Referenzdaten-Formate

- Keine Austauschbarkeit, wo keine gebraucht wird

Beispiele aus der Rechtsprechung

Biometrische Zeiterfassung in Krankenhaus

Ein österreichisches Bezirkskrankenhaus mit 430 Mitarbeitern wollte eine biometrische Zeiterfassung einführen

Dabei wurde weder die Zustimmung der Mitarbeiter, noch die des Betriebsrats eingeholt

Der Österreichischer Oberster Gerichtshof stellte klar, dass diese Anwendung mitbestimmungspflichtig ist

Urteil vom 20. Dezember 2006, 90bA 109/06d

In diesem speziellen Fall konnten weder Erforderlichkeit noch Verhältnismäßigkeit nachgewiesen werden

Folglich lassen sich ähnliche betriebliche biometrische Anwendungen nicht gegen den Betriebsrat durchsetzen

Dies gilt in leicht abgeschwächter Form auch für Deutschland

Fazit: Den Betriebsrat vor Anschaffung fragen und überzeugen!

Der Club (Thermalbad Mondorf - Luxemburg)



Leistungen

alles rund um Entspannung, Schönheit, Gesundheit, Krafttraining, Wellness

Preise

z.B. Abonnement 12 Monate: 890 €

Das Problem

Übertragbarkeit der Clubausweise

Die Lösung: Fingerprint-Authentifizierung



Bilder: EWV Kontrollsysteme

Realisierungsgeschichte

Zunächst alle Fingerprint-Referenzen in PC verschlüsselt gespeichert

Chip diente nur als Identifikator zur Auswahl der richtigen Referenz

**Diese Lösung wurde von der zuständigen Datenschutzkommission
abgelehnt**

Ursache war im Wesentlichen die fehlende Verhältnismäßigkeit

**Daraufhin wurde das Konzept zugunsten einer ausschließlichen
Speicherung der biometrischen Daten auf dem Chip abgewandelt**

Dieser Lösung erteilte die Datenschutzkommission die Zustimmung

**Nicht weiterverfolgt wurde der technisch vorteilhaftere Lösungsansatz,
die Referenzen zwar zentral auf dem PC zu speichern, jedoch individuell
mit einem auf dem Chip gespeicherten Schlüssel zu verschlüsseln**

Diese Lösung hätte wegen größerer Referenzen eine niedrigere Fehlerrate
zur Folge gehabt

Besten Dank für Ihre Aufmerksamkeit!