# Biometrie – Beschleuniger oder Bremser von Identitätsdiebstahl

Christoph Busch

Hochschule Darmstadt
CASED
Mornewegstr. 32
64293 Darmstadt
christoph.busch@h-da.de

**Abstract:** Der Beitrag betrachtet die Fragestellung, ob Biometrie als Beschleuniger oder Bremser von Identitätsdiebstahl betrachtet werden sollte. Dazu werden Szenarien betrachtet, in denen umfangreich Gesichtsbilddaten gesammelt werden. Diese Szenarien werden anhand etablierter Definitionen analysiert. Ferner werden Vorfälle von Identitätsmissbrauch betrachtet und eine Bewertung von Schutzmechanismen gegeben.

## 1 Einführung – Suchen und Sammeln

Die Qualität und Macht von Suchmaschinen hat in einem Ausmaß an Bedeutung gewonnen, das noch vor 10 Jahren undenkbar war. Die effizienten Suchdienste von Google gehören zu den Arbeitswerkzeugen, die täglich von Jedermann genutzt werden. Nicht überraschend, dass der Börsenwert von Google trotz Finanzkrise noch über 100 Milliarden US-Dollar liegt und das Unternehmen damit weltweit die wertvollste Marke am Aktienmarkt darstellt – vor Microsoft, Coca-Cola und IBM. Auch nicht überraschend, dass es einerseits immer wieder neue Versuche zur Nach-Ahmung dieses Erfolges gibt, wie jüngst die Produktankündigung ‚WolframAlpha'[Heise09a], und andererseits immer neue Suchfunktionalität ergänzt wird, um Marktpositionen auszubauen oder zu erobern. Wo liegt nun der Bezug zur Biometrie?

Nicht einmal drei Jahre ist es her, dass Google mit dem Zukauf des Unternehmens Neven Vision eine Biometrie-Technologie erwarb, die zu den besten verfügbaren Technologien gehörte wie der Anfang 2007 publizierte Face Recognition Vendor Test [FRVT2006] bestätigte. Die Spekulationen zum Hintergrund dieses Kaufs sind inzwischen Realität: Seit September letzten Jahres ist die Gesichtserkennung in Google-Picasa integriert. Aber auch kleine Unternehmen bieten mit neuen Produkten wie dem ‚Photo Finder' eine Technologie [pf09], die mit erstaunlicher Erkennungsleistung Bildarchive und Plattfomen wie facebook durchsucht- mit dem Ziel, Personen in unterschiedlichen Aufnahmesituationen wiederzufinden. ICAO-kompatible Aufnahmen wie sie im elektronischen Reisepass erwartet werden sind das nicht – und es funktioniert dennoch (leidlich).

Was vor Jahren noch Utopie war und als paranoider Gedanke abgetan wurde, das ist heute Realität: Die verbesserte Leistung der Gesichtserkennung macht den Aufbau von Personen-Bewegungs-Profilen möglich. Hinzu kommt die Bildaufzeichnung im öffentlichen Raum, die mit der wohlgemeinten Absicht aufgestellt werden, von Straftaten abzuschrecken oder sie zu vereiteln. Die signaltechnische Qualität von Raumüberwachungskameras führt zu einer immer höheren Bildauflösung, so dass eine Verknüpfung mit den oben genannten Bildspeichern technisch möglich wird. Von informationeller Selbstbestimmung der betroffenen Person kann man in diesem Fall faktisch nicht mehr sprechen. Die verpflichtend vorgeschriebenen Hinweise auf installierte Überwachungskameras werden nur zu leicht in der auch im Straßenalltag vorhandenen Informationsflut übersehen. Die neuerlich wieder fortgesetzten StreetView-Aufnahmen auf deutschen Straßen regen die Phantasie der besorgten Datenschützer weiter an, auch wenn die Plattformbetreiber versichern, dass Gesichter in dem Erweiterungsdienst von Google Maps nicht kenntlich würden.

## 2 Flüchtige biometrische Gesichtsbilder

Mitunter wird durch den Einsatz von Biometrie ein neues Risiko des Identitätsdiebstahls vermutet [ttt08]. Kann die Biometrie als Beschleuniger eines Identitätsdiebstahl betrachtet werden? Und wenn das ein konkretes Risiko sein sollte - welche Handlungsempfehlungen ergeben sich dann aus den oben geschilderten profilbildenden Gegebenheiten?

- Erstens die Einsicht, dass persönliche Bilder nicht unbedacht in öffentlichen Internet-Bildspeichern wie facebook verteilt werden sollten; der Austausch der Erinnerungsphotos von der letzten Firmenfeier kann auch in zugangsgeschützten Bereichen oder verschlüsselt erfolgen, wenn kein Intranet zur Verfügung steht.
- Zweitens das Verständnis, dass zweidimensionale Bilder eine Repräsentation einer ‚flüchtigen' biometrischen Charakteristik darstellen. Flüchtig ist eine Charakteristik dann, wenn sie auch ohne explizite Einwilligung der betroffenen Person erfasst und verarbeitet werden kann [ross06]. Auch der an einem Glas hinterlassene analoge Fingerabdruck zählt dazu.

- Drittens die Hoffnung, dass zweidimensionale Gesichtsbilder in Zwei-Faktor-Authentisierungsverfahren die Sicherheit steigern können. So war es ein Ziel der Einführung biometrischer Pässe, die Bindung des Passinhabers an den Pass zu stärken und somit das Risiko der Weitergabe (Vermietung) eines Passes und Nutzung durch eine Dritte Person zu reduzieren. Es wird erwartet, dass durch die biometrische Verifikation ein Missbrauch durch Weitergabe deutlich reduziert werden kann [zier2007]. Eine solche technische Prüfung wird bereits heute an vielen Grenzkontrollpunkten in Portugal vorgenommen und mit dem Projekt easyPASS ab August 2009 auch am Frankfurter Flughafen getestet werden.
- Viertens die Gewissheit, dass zweidimensionale Gesichtsbilder wie andere flüchtige Modalitäten nicht alleinstehend für eine sichere unüberwachte Zugangskontrolle ausreichen. Das Anfertigen von Plagiaten ist schlicht zu einfach. Für die logische und physikalische Zugangskontrolle ergibt sich daher die Notwendigkeit zur Messung von nicht-flüchtigen biometrischen Charakteristiken wie der dreidimensionalen Gesichtsgeometrie [bus2008] oder den Fingervenen[hart2009], deren Gegenwart nicht durch ein einfaches Plagiat vorgetäuscht werden kann.

# 3 Identitätsdiebstahl

Die beiden Begriffe Biometrie und Identitätsdiebstahl werden oft in einem Zusammenhang benutzt ohne dabei jedoch Klarheit über die Bedeutung der Begriffe zu haben.

## 3.1 Klärung der Begrifflichkeiten

Die Internationale Standardisierungsorganisation (ISO) hat eine klare Definition des Terminus Biometrie erarbeitet: „*automated recognition of individuals based on their behavioural and biological characteristics*“ [iso-sc37]. Schwieriger ist die Definition der Identität, da dieser Begriff nicht nur bei der körperlichen Erkennung von natürlichen Personen sondern auch im Zusammenhang von Personengruppen und deren Gedanken- und Stimmungwelt verwendet wird. Hier formuliert die ISO: „*Structured collection of an entity's attributes, allowing this entity to be distinguished and recognized from other entities within given contexts*“, wobei unter entity (Entität) eine ausgeprägte Existenz verstanden wird, die in einem Kontext einzigartig ist [iso-sc27]. Entitäten können natürliche Personen sein, aber auch Organisationen sowie aktive und passive Objekte. Der Tatbestand eines Diebstahls ist hingegen klar im §242 des Strafgesetzbuchs definiert: „*Wer eine fremde bewegliche Sache einem anderen in der Absicht wegnimmt, die Sache sich oder einem Dritten rechtswidrig zuzueignen, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft.“*

### 3.1 Bewertung der Szenarien

Kommen wir zurück zur Betrachtung eines möglichen Identitätsdiebstahls. Zunächst wäre aus juristischer Sicht die Frage zu beantworten, ob das Sammeln von mehr oder weniger frei zugänglichen Bildern als Diebstahl im Sinne von §242 Strafgesetzbuch betrachtet werden kann. Wenn nicht - welcher Tatbestand ist gegebenenfalls zutreffender? Sicherlich ist die Verknüpfung von gesammelten Bildern und Überwachungsbildern ohne gesetzliche Grundlage als unrechtmäßig zu betrachten. Eine Einwilligung der betroffenen Personen liegt ja bei nicht-kooperativer Erfassung der Bilder nicht vor.

Unabhängig von der juristischen Bewertung für das oben beschriebene Gesamt-Szenario Raumüberwachung ergibt sich aus technischer Sicht jedoch als Ergebnis, dass Biometrie *nicht* als ein Beschleuniger von Identitätsdiebstahl betrachtet werden kann. Es wird in der Betrachtung deutlich, dass ein aufgezeichnetes zweidimensionales Bild nur *ein* Identitätsattribut einer Person ist – allerdings ein Attribut, das sonderlich flüchtig ist.

Ein Identitätsdiebstahl bedeutet aber doch mindestens die Kontrolle über einen umfangreichen oder vollständigen Satz von Identitätsattributen. Unter diesem Verständnis ist die - von der betroffenen Person unbemerkt durchgeführte - Beschaffung eines zweidimensionalen Lichtbildes daher kein Identitätsdiebstahl.

## 4 Identitätsmissbrauch

Ein Identitätsmissbrauch hingegen ist klar definierbar als Nutzung des Identitätsdiebstahls zum Schaden der betroffenen Person, wobei das vorrangige Interesse des Angreifers in aller Regel eine finanzielle Bereicherung ist. Das Risiko, Opfer eines solchen Ereignisses zu werden, ist in den vergangenen Jahren dramatisch gestiegen. Das Identity Theft Resource Center berichtet für das Jahr 2008 eine Zunahme von 47% im Vergleich zum Vorjahr [idtc2009a]. Die Liste der Einzelvorfälle dokumentiert zum Beispiel Kreditkartenbetrug, Kontenraub und Bankbetrug und zeigt die zur Beschaffung der notwendigen Informationen eingesetzte Spannbreite von Angriffen. Diese reichen von manipulierten Kartenlesern über Phishing-Angriffe bis hin zu ausgefeilten Social-Engineering-Angriffen, die zur unbedachten Preisgabe von sensitiven Daten motivieren. Diese Gefahren sind auch für Deutschland ein größer werdendes Problem, wie die Statistiken des Bundeskriminalamtes belegen [bka2008]. Hierzulande steigt die Zahl der Angriffe auf Geldautomaten um 50% pro Jahr. Der dadurch entstandene Schaden in 2007 wurde auf ca. 21 Millionen Euro beziffert. Hinzu kommt die zunehmende Manipulation von Point-of-Sales (POS)-Terminals zur Durchführung von Skimming-Angriffen. Diese Statistik lässt sich weiter fortführen – die Geschwindigkeit, mit der uns das Problem begegnet, wird jedoch schon mit diesen Zahlen deutlich. Es bleibt dabei den geschädigten Opfern auch nur ein schwacher Trost, wenn nach dem Diebstahl der Identitäts-Informationen der eigentliche Missbrauch im Ausland getätigt wird. Inländische Bankautomaten überprüfen die integrierten Sicherheitsmerkmale der Karte und können daher ein Duplikat vom Original unterscheiden.

## 5 Zusammenfassung

Identitätsdiebstahl wird ein zunehmend kritisches Problem, für das bald griffige Lösungen gefunden werden müssen. Der den Finanzbereich betreffende Anteil kann bald jeden Bürger betreffen. Der durch diese Art von Identitätsdiebstahl angerichtete Schaden ließe sich bremsen, wenn europaweit für großvolumige Transaktionen, neben den Faktoren Besitz (Original-Karte) und Wissen (Pin) auch die Präsentation und Überprüfung einer nicht flüchtigen biometrischen Charakteristik erforderlich wird. Die biometrischen Modalitäten der drei-dimensionalen Gesichtserkennung und der Venenerkennung sind zu diesem Zweck besonders geeignet.

## Literaturverzeichnis


[Heise06] Heiseticker: Google erweitert Picasa um Gesichtserkennung, http://www.heise.de/newsticker/meldung/76881, August 2006

[Heise09a] Heiseticker: "Antwortmaschine" Wolfram Alpha im ersten Test, http://www.heise.de/newsticker/meldung/137330, Mai 2009

[apc08] APC: Google Picasa gets face recognition, http://apcmag.com/Google_Picasa_gets_face_recognition.htm, September 2008

[FRVT2006] J. Philips: NISTIR 7408 - FRVT 2006 and ICE 2006 Large-Scale Results, März 2007

[pf09] Face.Com: Photo Finder on facebook, http://www.face.com/, April 2009

[Heise09b] Heiseticker: Google macht wieder Fotos für Street View, http://www.heise.de/newsticker/meldung/135281, Mai 2009

[ttt08] TeleTrust Whitepaper: Datenschutz in der Biometrie, http://www.teletrust.org/uploads/media/Datenschutz-in-der-Biometrie-080521.pdf, Mai 2008

[ross06] A. Rossnagel: Biometrie – Schutz und Gefährdung von Grundrechten, Tagungsband Biometrie und Datenschutz – der vermessene Mensch, Peter Schaar (Editor), Juni 2006

[zier2007] J. Ziercke: Stellungnahme zum Passgesetz, Expertenanhörung im Innenausschuss des Deutschen Bundestages, April 2007

[bus2008] C. Busch, A. Nouak: 3D-Gesichtserkennung für die unbeaufsichtigte Grenzkontrolle, in Tagungsband Sicherheit 2008, GI-LNI, April 2008

[hart2009] D. Hartung: Venenbilderkennung, in DuD 6/2009, Juni 2009

[iso-sc37] ISO/IEC JTC1 SC37 SD2 Harmonized Biometric Vocabulary, Feb. 2009

[iso-sc27] ISO/IEC JTC1 SC27 A Framework for Identity Management, June 2009

[idtc2009a] Identity Theft Resource Center: Security Breaches 2008, http://www.idtheftcenter.org/artman2/publish/lib_survey/Breaches_2008.shtml, März 2009

[idtc2009b] Identity Theft Resource Center: 2009 ITRC Breach Report, http://www.idtheftcenter.org/artman2/publish/lib_survey/ITRC_2008_Breach_List.shtml#, Mai 2009

[bka2008] Bundeskriminalamt: Aktuelle Herausforderungen in der Kriminalitätsbekämpfung, http://www.bka.de/pressemitteilungen/2008/pm080328.html, März 2008