Christoph Busch

Biometrie und Identitätsdiebstahl

Die beiden Begriffe Biometrie und Identitätsdiebstahl werden oft in einem Zusammenhang benutzt ohne dabei jedoch Klarheit über die Bedeutung der Begriffe zu haben. Die Internationale Standardisierungsorganisation (ISO) hat eine klare Definition des Terminus Biometrie erarbeitet: „*automated recognition of individuals based on their behavioural and biological characteristics*". 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. 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.*"

Der Zusammenhang zwischen Biometrie und Identitätsdiebstahl wird unter anderem hergestellt bei im Internet verteilten Gesichtsbildern (Facebook etc.) und deren Verknüpfung respektive Sammlung. 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. Wer diese Frage entlang der oben zitierten Definitionen beantworten möchte, kommt zu einem negativen Ergebnis. Dennoch ist sicherlich die Verknüpfung von gesammelten Bildern als unrechtmäßig zu betrachten. Eine Einwilligung der betroffenen Personen liegt ja nicht vor.

Unabhängig von der juristischen Bewertung kommt man für das Szenario der gegebenenfalls sogar im Übermaß gesammelten biometrischen Gesichtsbilder auch aus technischer Sicht zu dem 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 strukturierten Satz von Identitätsattributen. Unter diesem Verständnis ist die – von der betroffenen Person unbemerkt durchgeführte – Beschaffung eines zweidimensionalen Lichtbildes daher kein Identitätsdiebstahl.

Ein Identitätsmissbrauch hingegen ist 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. 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. 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. 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. Vorschläge dazu sind in den Beiträgen in diesem Heft formuliert.