

# Haben wir etwas zu verbergen?

Nach einer digitalen Diskussion mit einem Kollegen zum Thema Datenschutz im März 2006

## Prolog

Es ging um Datenmanagement und um Ereignisse, die darauf beruhten, dass mehrere Datenbanken nichts voneinander „wussten“.

## Ein Dialog

*Zeilen, die mit „>“ beginnen, sind Teilzitate des Kollegen.*

*>Na ja, ich denke dass ist eher ein typisches Beispiel  
>dafür, wie unfähig die Behörden sind und wie weit es*

Zunächst muss ich bemerken, dass natürlich alle Pauschalisierungen übersimplifizierend sind. :)

Und ich könnte auch zahlreiche Beispiele von Inkompetenz aus der Privatwirtschaft nennen. Inkompetenz ist nicht an die Art des Anstellungsverhältnisses gebunden.

*>dass es soweit kommen kann, wenn man auf die Bevölkerung  
>hört, die sich gegen eine zentrale Datenspeicherung wehrt.*

Die "Bevölkerung" (wer auch immer das sein mag) hätte auch gar nichts dagegen alles zentral zu speichern, wenn man so den landläufigen Meinungen zuhört. Eine zentrale Speicherung hätte aber zwei gravierende Nachteile, die durch die möglichen Vorteile meiner Einschätzung nach nicht aufgewogen werden:

1. Die menschliche Unfähigkeit würde sich potenzieren. Dezentrale Datenbanken hängen von den vielen Kompetenzen lokaler Administrationen ab, zentrale sind ein "single point of failure", in denen sich ein kleiner Fehler durch viele Anwendungen ziehen kann. Man hätte nicht unbedingt schneller verfügbare Daten, aber schneller sich ausbreitende Fehler.
2. Die zentrale Bereitstellung von Daten würde wie ein "Honigtopf" auf Interessenten wirken (Firmen, Behörden und die Organisierte Kriminalität), die sich dem notwendigen Datenschutz nicht verpflichtet fühlen. Dezentrale Vorhaltung verschiedener Datensegmente schützt vor allzu leichtem Missbrauch. Eine zentrale Bereitstellung wäre dagegen mit kleinem Aufwand schnell zu knacken und senkt die Hemmschwelle gegen Missbrauch erheblich. Und selbst Dir unterstelle ich, dass Du eine solche "zentrale Datenbank" in rechtlich gesicherten, vernünftigen Händen sehen möchtest. Das ist aber technisch und finanziell praktisch unmöglich, wie die Praxis ständig wieder zeigt.

Das Militär benutzt ein gutes Prinzip: "need to know basis". Jeder weiß nur soviel, wie er odr sie zur Erledigung seiner Aufgaben benötigt Alles

darüber hinaus ist unnützer Ballast und zudem noch gefährlich. Das gilt auch für Generale und andere Beamte.

*>Hätte man eine zentrale Stelle, die ALLE Daten einer  
>Person verwaltet (Adressen, Krankenkassendaten, Telefonanschlüsse,  
>Fahrzeuge, Arbeitgeber, Schulabschlüsse, Vorstrafen etc.),  
>würde so etwas NIEMALS passieren und die Behörden könnten  
>Milliarden einsparen.*

Das ist ein Trugschluss. Auch eine zentrale Stelle schützt nicht vor Inkompetenz. Eine Fehlbedienung hätte dann aber umfassende Folgen für die betreffende Person.

An sich schon problematisch genug, würde diese Lösung sogar an Brisanz zunehmen, wenn ein Betroffener überhaupt nichts über die Folgen falscher Verwendung oder den Falscheintrag seiner Daten erfährt (entweder, weil es niemand realisiert oder niemand realisieren will). Was sich dann zum Beispiel in der Ablehnung einer Bewerbung, der Verweigerung eines nötigen Kredits, der Verweigerung der Einreise in ein anderes Land oder in einer Nichtzulassung zu einer Ausbildungsstätte äußern kann.

*> So würde z.B. die GEZ sofort sehen wenn ich keine Gebühren  
> zahle, aber in einem Haus mit Kabelanschluss wohne. Außerdem*

Was nützt das? Ich wohne in einem Haus mit Kabelanschluss, besitze aber keinen Fernseher und kein Radio. Die juristische Unschuldsvermutung ist zwar schon an einigen Stellen korrodiert (Kopierabgaben auf CD- und DVD-Brenner und -Rohlinge zum Beispiel), aber immer noch Grundlage des Rechtssystems unseres Landes.

Eine solche Datenbank könnte präventiv oder auch erst nach Eintritt des Ereignisses benutzt werden. Letzterer Fall würde kaum abschrecken. Gegen schlaudere Ermittlungsmethoden finden sich auch schnell immer effektive Gegenmaßnahmen. Gerade im Bereich digitaler Anwendungen.

So ist das Protokoll des niederländischen RFID-Passes schon geknackt worden, bevor er regulär in Umlauf kam (<http://www.heise.de/newsticker/meldung/69127>). Ähnliches gilt auch inzwischen für den deutschen, in variiertes Form.

Und Prävention? Das ist höchst problematisch, denn an welchem Punkt soll die Prävention ansetzen? Soll sie passiv aufklären oder aktiv Einfluss nehmen? Und mit welchen "Mustern" soll eine aktive Prävention durchgeführt werden? Denn Muster sind dazu notwendig, z.B. wer zahlt typischerweise Kredite nicht zurück? Oder wer ist anfällig für Ladendiebstahlsdelikte?

Wusstest Du tatsächlich zuverlässige Muster für soziologische Phänomene, fielen Dir viele Leute um den Hals. Zum Beispiel die Banken, die verzweifelt nach so einem Muster für Kreditwürdigkeit suchen.

Wie ein lokaler Bankvorstand letztens in einem öffentlichen Vortrag in

Passau zugab, sind die bisherigen Muster, die seine Bank an deren umfangreiche Datenbestände anlegt, in ihrer Wirkung auch heute nicht viel besser (ca. 60% Treffer) als eine Münze zu werfen (50% Treffer). Und Banken haben erfahrungsgemäß neben einem sehr großen Datenbestand auch große Ressourcen zur Untersuchung solcher Probleme zur Verfügung. Wenn die es schon nicht ordentlich schaffen, wer dann?

Auch stimmen schon die technischen Voraussetzungen nicht, um überhaupt eine zuverlässige Datenbank zu erzeugen. Gehst Du nur von deutschsprachigen oder englischsprachigen Daten aus? Es gibt Eigennamen von Personen, Unternehmen und Dingen, die aus kyrillischer, hebräischer, arabischer, chinesischer, koreanischer, japanischer, thailändischer oder anderen Schriften stammen.

Sollte die Datenbank technisch nicht in der Lage sein, solche Eigennamen im Original aufzunehmen, kommen schon bei der Transposition in die lateinische Schrift Fehler vor, weil es entweder keine Normen dafür gibt oder die Eintragenden in diesen Normen nicht geschult sind. Und natürlich vertippen sich auch Beamte.

Und Du und ich möchten vor einem wichtigen Geschäftstermin sicherlich nicht aufgehalten oder gar verhaftet werden, nur weil ein US-Marshall sich bei meinem Namen vertippt und dann statt "Schönleber" einen "Schenleber" in der Datenbank findet, der vielleicht zur Fahndung ausgeschrieben ist? Weil der Beamte (oder die ihm zur Verfügung stehende Norm) keinen Unterschied zwischen den Buchstaben "ö" und "e" bei deutschen Namen hört? Das habe ich in ähnlicher Weise schon bei Bezahlvorgängen im Internet erlebt.

Fazit: Selbst wenn es technisch realisiert werden könnte, dass ein perfektes Datenmodell geschrieben würde, die Datenbank perfekt implementiert würde, sie perfekt gegen Angriffe geschützt wäre, so würden am Ende immer noch menschliche Fehler aller Art das alles wieder korrumpieren.

Wie die vielen Beispiele zeigen, die wöchentlich in den Medien zu erleben sind: Die Daten waren da, und sie waren auch relativ gut gepflegt. Man hat nur nicht sorgfältig genug gearbeitet. Das aber ist technisch nicht lösbar, das ist menschliche Eigenschaft.

*> Gläserner Bürger und Überwachung hin oder her: Wer nichts  
> zu verbergen hat, hat auch nichts zu befürchten und allen  
> anderen geschieht es recht.*

Das ist leider ein sehr leichtfertiger Schluss. Dazu zunächst eine polemische Antwort (1) und dann eine sachliche (2). :-)

1. Du hast nichts zu verbergen? Bitte veröffentliche doch dann an dieser Stelle Deine ec-Karten-PIN, Deine Zugangsnummer für die Uni-Bibliothek, Deine Passworte, Deinen Kontostand, Deinen Dispo, Deine laufenden Kredite, Deine Kreditkartennummer/n, Deine Krankheiten (chronische sind von besonderem Interesse, ich kenne da eine Versicherung). Dann möchte ich bitte ein Haar

von Dir für eine Gen-Analyse, Fingerabdrücke von Daumen und Zeigefinger Deiner beiden Hände, ein digitales Foto von Dir nach der Foto-Mustertafel "ePass" der Bundesdruckerei, Deine Kundennummern bei den von Dir frequentierten Unternehmen, dann eine Audio/WebCam in Deinem Schlafzimmer, Wohnzimmer und im Eingangsflur und Deine Telefonmitschnitte. Dann möchte ich einen Grundriss Deiner Wohnung mit Markierungen der Punkte, an denen sich Wertsachen befinden. Dazu bitte Eure nächsten Urlaubspläne, denn Ihr sollt nicht gestört werden, wenn dann jemand vorbei schaut und die Wertsachen untersucht. Dazu eine von Dir unterschriebene Genehmigung, dass ich das alles in Datenbanken meiner Wahl speichern und/oder verkaufen darf. Jegliche Einschränkung Deinerseits bedeutet, Du hast etwas zu verbergen. Vor wem auch immer.

2. Jede Person hat Dinge zu verbergen. Dazu muss es nicht mal einen Grund geben. Und niemand wird dadurch verdächtig oder suspekt. Wenn ich nicht will, dass jemand bestimmte Dinge von mir weiß, muss ich das nicht sagen. Es können mir Nachteile daraus erwachsen, wenn ich z.B. bei einem Kreditantrag die Schufa-Klausel streiche; dann gibt's eben kein Geld. Aber das ist dann meine Entscheidung. Das wurde auch durch das Bundesverfassungsgericht am 15.12.1983 (Az.: 1 BvR 209/83; NJW 84, 419) bestätigt (Recht auf informationelle Selbstbestimmung).

Würde man das verneinen, also den Leitsatz "Ich habe nichts zu verbergen" stringent zu Ende denken, müsste man in letzter Konsequenz zulassen, dass in jeder Wohnung und in allen Straßen und Gebäuden Kameras und Mikrophone installiert werden, um die 100%-ige Sicherheit zu gewährleisten Und dass jeder einen Chip implantiert bekommt, der jederzeit Aufenthaltsort und Identifikation mitteilt. Übrigens, das gibt es schon alles, in Firmen oder Behörden, sogar schon in manchen Ländern.

Ja, hätte ich beinahe vergessen: Dass außerdem andere Leute mit meinen Daten viel Geld verdienen, z.B. Whitepages wie Intelius (<http://www.bigfoot.com/>),

Zitat aus deren Werbung:

*"Intelius is searching billions of current utility company records, court records, county records, change of address records, property records, business records and a variety of other public records and publicly-available records to find what you are looking for."*

Einen vollständigen Datensatz einer beliebigen Person erhalte ich für 49,95 US\$, bezahlbar mit Kreditkarte online.

Noch Fragen, „Bürger“? :-)

Um es kurz zu formulieren: Datenmanagement bedeutet nicht, alle Daten in eine Datenbank zu stecken. Im Gegenteil. Es bedeutet, die zur Verfügung stehenden Daten effizient und effektiv zu einer Informationsmaische vorzubereiten, damit im entscheidenden Falle

(Unternehmensentscheidung, Fahndung, politische Planung,...) im rechtlichen Rahmen aus dieser Maische die richtigen Informationen destilliert werden können.

Das geht auch (oder evt. sogar nur) unter einer gut geplanten, dezentralen Datenaufbereitung unter Einhaltung notwendiger Einschränkungen. Wird die Datensammlung zu groß, versinkt nämlich die Nadel im Nadelhaufen oder es entstehen "virtuelle Artefakte", die keine reale Grundlage besitzen, aber zu realen, falschen Entscheidungen führen können (Im diskutierten aktuellen Falle entstand ein negatives Artefakt "nicht vorhanden", auf das sich dann jeder verließ).

Ganz vernachlässigt habe ich den Umstand, dass die meisten Firmen und Behörden tatsächlich zu dusselig sind, ihre Datenbanken so zu sichern, dass sie nicht von alleine ins Netz „auslaufen“. Datenschutz ist ja auch, wenn ich meiner Bank meine Daten anvertraut habe und sie dann am nächsten oder übernächsten Tag nicht gerade im Internet zu finden sind.

Ganz zum Schluss eine Denksportaufgabe:

Versuche, den Unterschied zwischen Datensicherheit, Datenschutz und Informationeller Selbstbestimmung herauszuarbeiten.

„Danke für die Beachtung aller Sicherheitsmaßnahmen!“ (aus: Dark Star)

## Und zum Schluss die obligatorischen Selbstkontrollfragen und Übungen: :-)

1. In welchen Büchern (oder Filmen) wird eine zentrale Datenspeicherung und die damit einhergehende Überwachung zum zentralen Thema genommen und *en detail* diskutiert? Wie realistisch sind solche Szenarien?
2. Sammle dazu real implementierte Beispiele und reale Planungen in (i) unserem Land und (ii) im Ausland aus öffentlichen Pressemeldungen.
3. Informiere Dich über das juristische Prinzip der Güterabwägung. Gewichte Vor- und Nachteile zu diesem Thema nach diesem Prinzip, und wäge nach selbst gefundenen Kriterien ab.
4. Informiere Dich über reale Situationen aus der Vergangenheit, in denen solche Verfahren bereits zum Einsatz kamen. Erläutere die Folgen, die diese Verfahren mit sich brachten. Würde eine solche Entwicklung heute/hier anders ablaufen? Begründe Deine Annahmen.
5. Diskutiere die technischen und administrativen Probleme, die solch ein zentralisiertes "data mining" und "data warehouse" mit sich bringen würde
6. Skizziere ein Datenmodell und ein Anwendungsfall-Diagramm für eine solche zentrale Datenbank.

## Ich hab' nichts zu verbergen!

Blutgruppe B, Herzinfarktrisiko 14%, KV-Datensatz (Genanalyse) liegt vor, Krankenversicherung: Standard, Zusatzversicherung angeboten (File 23A18)  
Risikoklasse 4 - (Nachuntersuchung erforderlich in Q8, Verdacht auf KV-Risiko Stufe 3)  
Drogenkonsum: Nicht aktuell.  
Alkoholkonsum mittel bis niedrig,  
Einkommen €1434,-, RV, PV, KS, VWL  
Kredit: DB, €40.000, Konto: €-729  
Zahlungsmoral: nachlässig, Versand auf Rechnung einstellen, Kundennr: 393848, Punkte: 2930,  
Umsatzpotential nicht ausgeschöpft.  
Interessensprofil Musik/Buch: liegt vor  
Interessensprofil Reisen: liegt vor,  
Bürgerklasse 3 (Normal, wiedervorlage, geplant 2009, ID-Code C89A839A) Soziales Umfeld: Thomas B., Kerstin A., Verena L. (siehe Datensatz B33421)  
Arbeitgeber K8273-23, Datenbankabgleich: OK  
Verspätungen: 4, Abmahnung: Nein, Auto: Ford Fiesta, TÜV, Teilkasko, Verkehrsdelikte: 2 (leicht) 0 (schwer)  
Risikostufe: 3, Tendenz fallend, Maut-ID A38-92384  
Fahrzeugsbewegungsdaten: liegen vor ab 04/2006  
Politische Ausrichtung: SPD (bis 2005), seit 2005 Nichtwähler, Teilnahme an AK-Demo 2005 (Video #0232-4)

...bis auf meine Privatsphäre.

[www.datenschutzzentrum.de](http://www.datenschutzzentrum.de)



(Quelle: Unabhängiges Landesdatenschutzzentrum Schleswig-Holstein)