DATENSCHUTZ

Luca Peter / Daniel Müller

1101010101010101010101010
10101010101010111
10101010101
1001011

10010101110101101010101011
10101101010011010 1
10101010101
1010101

Art der Arbeit: SVA
Oberthema: Alltägliches - Unalltägliches
Schule: Gewerbilch Industrielle Berufsschule Muttenz
Klasse: ISY 4c
Abgabedatum: 17. Dezember 2007
Klassenlehrer: Otto Höschle

Inhaltsverzeichnis

1. Einleitung

Im Rahmen unserer Informatikausbildung führen wir im letzten Jahr im Fach Algemeinbildung eine selbständige Vertiefungsarbeit (SVA) durch. Da wir bei der Wahl des Themas ziemliche Freiheiten hatten und beide über etwas schreiben wollten, was uns interessiert und eng mit unserer Gesellschaft verbunden ist, haben wir uns für das Thema Datenschutz entschieden.
Durch den zunehmenden Fortschritt der Technik sind wir im Alltag immer wieder mit neuen Technologien konfrontiert. Abläufe im Alltag sollen durch den technischen Fortschritt laufend vereinfacht, modernisiert und beschleunigt werden.
Der Computer und die stetig wachsende Vernetzung unserer Daten gewinnt in unserer Gesellschaft dadurch zunehmend an Bedeutung. Viele von uns benutzen ein Handy, besitzen eine Kreditkarte, zahlreiche Kundenkarten und nutzen regelmässig das Internet. Doch wer macht sich darüber Gedanken, was mit unseren Daten geschieht?
Ist wirklich alles so harmlos oder geben wir unbewusst immer mehr Daten von uns preis? Gerade Stichwörter wie „RFID“ und „Biometrie“, welche wir im Verlaufe unserer Arbeit selbstverständlich genauer erläutern werden haben derartige Fragen in uns aufkommen lassen. Wir hoffen, dass wir im Rahmen unserer Arbeit einige dieser Gefahren aufzeigen und das Interesse des Lesers an dieser Thematik wecken können.
Im nachfolgenden Teil werden wir erläutern, wie wir bei unserer Arbeit vorgegangen sind und danach auf den Grundlagenteil eingehen.
Der Hauptteil unserer Arbeit besteht darin, einige Technologien zu hinterfragen, ein Interview mit einem Experten durchzuführen und die Problematik bezüglich der Gefährdung unserer persönlichen Daten in der Gesellschaft aufzuzeigen. Bevor Sie unser persönliches Fazit finden, haben wir uns die Freiheit genommen, einen kleinen fiktiven Teil in die Arbeit einfliessen zu lassen, welcher sich auf zukünftige Entwicklungen in unserer Gesellschaft beziehen wird.

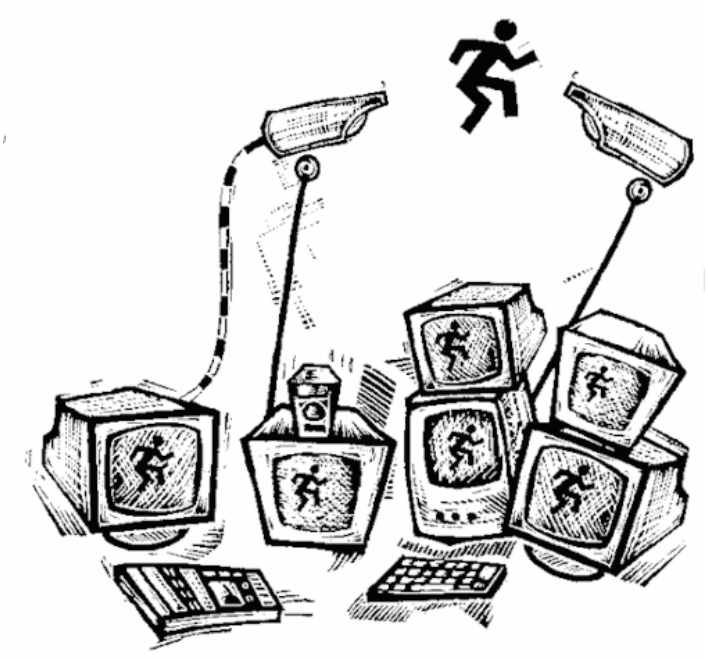

Abb. 1 Symbolische Darstellung eines gläsernen Bürgers

2. Vorgehensweise

Bevor wir mit unserer Arbeit gestartet sind und darauf los recherchiert haben, erstellten wir ein Mindmap[1], wo wir unseren Gedanken freien Lauf lassen konnten. Danach haben wir unsere Wahl begründet und ein Grobkonzept erstellt, damit wir einen kleinen Leitfaden hatten an dem wir uns für die Gliederung der Arbeit orientieren konnten. Den grössten Teil unserer Arbeit haben wir mit Hilfe von Internetrecherchen durchgeführt. Die uns zur Verfügung gestellten ABU-Stunden nutzten wir, um Aufgaben zu verteilen, Recherchen zu vertiefen und Informationen zusammenzufügen. Dabei haben wir unsere Quellenangaben[2] laufend festgehalten.

3. Grundlagen

In der Einleitung sind Sie vielleicht bereits schon dem einen oder anderen Begriff begegnet, der Ihnen unklar war.
In diesem Kapitel werden Sie einige Auszüge aus dem Schweizer Datenschutzgesetz finden, wobei wir uns auf die allgemeinen Bestimmungen beschränkt haben. Weiter werden wir in diesem Teil auf Definitionen und Begriffe eingehen um das Verständnis für unsere Arbeit zu erleichtern.

3.1 Datenschutz und Datensicherheit

Da die Begriffe Datenschutz und Datensicherheit sehr ähnlich klingen, können diese auch gerne mal verwechselt werden, obwohl sie ganz unterschiedliche Bedeutungen aufweisen. Damit die Leser unserer Arbeit nicht in Versuchung kommen diese Begriffe zu verwechseln, wollen wir gleich zu Beginn dieses Kapitels Klarheit schaffen

> In den Bereich Datenschutz fällt der Schutz personenbezogener Daten vor Missbrauch. Auch wurde dieser für Schutz wissenschaftlicher und technischer Daten gegen Verlust, Veränderung und Diebstahl der Daten gebraucht. Heute wird er grundsätzlich nur noch für ersteres verwendet.[3]

> Datensicherheit oder Informationssicherheit beschreibt die Eigenschaften eines Systems, welches Daten lagert und verarbeitet. Die Verarbeitung, Speicherung sowie die Kommunikation müssen so realisiert werden, dass die Vertraulichkeit, Verfügbarkeit und die Integrität der Daten sichergestellt sind. Auch müssen Aspekte wie Gefahren, Schäden o.ä. berücksichtigt werden.[4]

Wie wir also den beiden Definitionen entnehmen können, geht es beim Datenschutz darum, dass der Mensch grundsätzlich selbst entscheiden kann, wem wann welche seiner persönlichen Daten zugänglich sein sollen und dass diese vor Missbrauch geschützt sind. Bei der Datensicherheit hingegen geht es primär nicht um Menschen, sondern darum, dass die Datensicherung und Verfügbarkeit von Daten auf einem Informationssystem gewährleistet wird.

[1] Siehe Anhang
[2] Siehe Kapitel 9. Abbildungsverzeichnis und Quellenangaben
[3] Siehe http://de.wikipedia.org/Datenschutz
[4] Siehe http://de.wikipedia.org/Datensicherheit

3.2 Schweizer Datenschutzgesetz

1. Zweck

Das Schweizerische Datenschutzgesetz[5] trat am 1. Juli 1993 in Kraft und bezweckt den Schutz der Persönlichkeit und der Grundrechte von Personen, über die Daten bearbeitet werden. Zu diesen Personen gehören Sie und Ich.

2. Geltungsbereich

Es gilt für das Bearbeiten von Daten „natürlicher und juristischer Personen“[6] durch private Personen und Bundesorgane.
Es ist nicht anwendbar auf:

a.
Personendaten, die eine natürliche Person ausschliesslich zum persönlichen Gebrauch bearbeitet und nicht an Aussenstehende bekannt gibt.
b.
Beratungen in den Eidgenössischen Räten und in den parlamentarischen Kommissionen.
c.
Hängige Zivilprozesse, Strafverfahren, Verfahren der internationalen Rechtshilfe sowie staats- und verwaltungsrechtliche Verfahren mit Ausnahme erstinstanzlicher Verwaltungsverfahren;
d.
Öffentliche Register des Privatrechtsverkehrs.
e.
Personendaten, die das Internationale Komitee vom Roten Kreuz bearbeitet.

3. Begriffe

Die folgenden Begriffe und deren Bedeutungen sind wortwörtlich aus dem Datenschutzgesetz zitiert und erläutern das Verständnis nachfolgender Paragraphen:

a.
Personendaten (Daten): alle Angaben, die sich auf eine bestimmte oder bestimmbare Person beziehen;
b.
betroffene Personen: natürliche oder juristische Personen, über die Daten bearbeitet werden;
c.
besonders schützenswerte Personendaten: Daten über:
- die religiösen, weltanschaulichen, politischen oder gewerkschaftlichen Ansichten oder Tätigkeiten,
- die Gesundheit, die Intimsphäre oder die Rassenzugehörigkeit,
- Massnahmen der sozialen Hilfe,
- administrative oder strafrechtliche Verfolgungen und Sanktionen;

d.
Persönlichkeitsprofil: eine Zusammenstellung von Daten, die eine Beurteilung wesentlicher Aspekte der Persönlichkeit einer natürlichen Person erlaubt;

[5] Siehe: http://www.admin.ch/ch/d/sr/c235_1.html
[6] Wenn im Recht von Personen (oder Privatpersonen) die Rede ist, so sind damit nicht nur **natürliche Personen**, also Menschen gemeint, sondern auch **juristische Personen**. Dies sind vom Recht geschaffene, künstliche Gebilde wie z.B. Vereine oder Aktiengesellschaften, die wie eine Menschliche Person Rechte und Pflichten erwerben, Verträge abschliessen und Geschäfte führen können.

e.
Bearbeiten: jeder Umgang mit Personendaten, unabhängig von den angewandten Mitteln und Verfahren, insbesondere das Beschaffen, Aufbewahren, Verwenden, Umarbeiten, Bekanntgeben, Archivieren oder Vernichten von Daten;
f.
Bekanntgeben: das Zugänglichmachen von Personendaten wie das Einsichtgewähren, Weitergeben oder Veröffentlichen;
g.
Datensammlung: jeder Bestand von Personendaten, der so aufgebaut ist, dass die Daten nach betroffenen Personen erschliessbar sind;
h.
Bundesorgane: Behörden und Dienststellen des Bundes sowie Personen, soweit sie mit öffentlichen Aufgaben des Bundes betraut sind;
j.
Inhaber der Datensammlung: private Personen oder Bundesorgane, die über den Zweck und den Inhalt einer Datensammlung entscheiden;
k.
formelles Gesetz:

- Bundesgesetze und referendumspflichtige allgemeinverbindliche Bundesbeschlüsse,
- für die Schweiz verbindliche Beschlüsse internationaler Organisationen und von der Bundesversammlung genehmigte völkerrechtliche Verträge mit rechtsetzendem Inhalt.

4. Grundsätze

Es gibt drei wesentliche Grundsätze, welche das Bearbeiten von Personendaten betreffen. Personendaten dürfen nur rechtmässig beschafft werden, ihre Bearbeitung hat nach Treu und Glauben zu erfolgen und muss verhältnismässig sein. Weiterhin dürfen Personendaten nur zu dem Zweck bearbeitet werden, der bei der Beschaffung angegeben wurde, aus den Umständen ersichtlich oder gesetzlich vorgesehen ist.

5. Richtigkeit der Daten

Wer Personendaten bearbeitet, hat sich zu vergewissern, dass diese der Richtigkeit entsprechen. Jede Person hat das Recht zu verlangen, dass unrichtige Daten berichtigt werden.

6. Bekanntgabe ins Ausland

Die gesammelten Informationen über Personen dürfen nicht ins Ausland weitergegeben werden, da ein Datenschutz fehlt, der dem unseren gleichwertig ist.
Datensammlungen, welche ins Ausland bekanntgegeben werden wollen, müssen dem Schweizerischen Datenschutzbeauftragten vorher gemeldet werden, wenn für die Bekanntgabe der Daten keine gesetzliche Pflicht besteht oder die betroffenen Personen davon keine Kenntnis haben.

7. Datensicherheit

Die Personendaten müssen durch angemessene technische und organisatorische Massnahmen gegen unbefugtes Bearbeiten geschützt werden. Nähere Bestimmungen zu den Mindestanforderungen werden durch den Bundesrat erlassen.

8. Auskunftsrecht

Jede Person kann vom Inhaber einer Datensammlung Auskunft verlangen, ob Daten über sie verarbeitet werden. Der Inhaber muss der Person mitteilen was für Daten über sie vorhanden sind und welchem Zweck sie dienen. Wenn die Daten durch einen Dritten verarbeitet werden ist der Inhaber auskunftspflichtig.

9. Einschränkung des Auskunftsrecht im Allgemeinen

Der Inhaber der Datensammlung kann die Auskunft verweigern, einschränken oder aufschieben, soweit:

- ein formelles Gesetz es vorsieht;
- es wegen überwiegender Interessen eines Dritten erforderlich ist.

Ein Bundesorgan kann zudem die Auskunft verweigern, einschränken oder aufschieben, soweit:

- es wegen überwiegender öffentlicher Interessen, insbesondere der inneren oder äusseren Sicherheit der Eidgenossenschaft, erforderlich ist;
- die Auskunft den Zweck einer Strafuntersuchung oder eines andern Untersuchungsverfahrens in Frage stellt.

10. Einschränkung des Auskunftsrechts für Medienschaffende

Der Inhaber einer Datensammlung, die ausschliesslich für die Veröffentlichung im redaktionellen Teil eines periodisch erscheinenden Mediums verwendet wird, kann die Auskunft verweigern, einschränken oder aufschieben, soweit:

- Die Personendaten Aufschluss über die Informationsquellen geben;
- Einblick in Entwürfe für Publikationen gegeben werden müsste;
- Die freie Meinungsbildung des Publikums gefährdet würde.

11. Register der Datensammlungen

Das vom Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten geführte Register kann von jeder Person eingesehen werden. Jegliche Datensammlungen müssen beim Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten durch die Bundesorgane zur Registrierung angemeldet werden.

„Private Personen, die regelmässig besonders schützenswerte Personendaten oder Persönlichkeitsprofile bearbeiten oder Personendaten an Dritte bekannt geben, müssen Sammlungen anmelden wenn für das Bearbeiten keine gesetzliche Pflicht besteht und die betroffenen Personen davon keine Kenntnis haben.“
Jede Datensammlung muss vor der Erstellung angemeldet worden sein.

„Der Bundesrat regelt die Anmeldung der Datensammlungen sowie die Führung und die Veröffentlichung des Registers. Er kann für bestimmte Arten von Datensammlungen Ausnahmen von der Meldepflicht oder der Registrierung vorsehen, wenn das Bearbeiten die Persönlichkeit der betroffenen Personen nicht gefährdet.
Die Anmeldung von Datensammlungen wird vom Bundesrat geregelt. Für bestimmte Arten von Sammlungen kann er Ausnahmen vorsehen, solange das Bearbeiten der Daten die Persönlichkeit der betroffenen Personen nicht gefährdet.

3.3 Biometrie

Biometrie ist ein Stichwort, welches in unserer Gesellschaft immer häufiger auftaucht. Beispielsweise stand in den Medien vor nicht allzu langer Zeit der neue Schweizer Reisepass zur Diskussion. Abgesehen davon, dass dieser mit einer neuen Technologie ausgestattet ist, doppelt so viel kostet und im Gegensatz zum bisherigen Pass nur halb so lange gültig sein wird, gibt es da noch ein weiteres gravierendes Detail. Dieser Pass soll biometrische Daten über den jeweiligen Bürger speichern. Doch was genau verstehen wir unter biometrischen Daten?
Dieses Kapitel soll darüber Klarheit verschaffen und in einem weiteren Schritt aufzeigen, wie eine Biometrische Fingerabdruckerkennung funktioniert.

> Biometrie wird definiert als Wissenschaft der Vermessung von Körpern und Lebewesen. Biometrie erfasst mit Hilfe mathematisch-statistischer Methoden physische oder verhaltenstypische Merkmale von Lebewesen und wertet diese aus. Das Wort Biometrie wird von den griechischen Wörtern Leben (Bios) und Mass (Metron) hergeleitet. In der Informationstechnologie bedeutet Biometrie das Erkennen von Benutzern an ihren individuellen Merkmalen.[7]

Folgende biologische Merkmale können z.B. zur Identifikation verwendet werden:

- Fingerabdruck
- Handabdruck
- Hand- und Fingergeometrie
- Gesicht
- Iris
- Netzhaut
- Stimme
- Unterschrift

Abb. 2 Fingerprintsensor

3.3.1 Beispiel anhand der Fingerabdruckerkennung

Um die Frage zu klären, ob Fingerabdrücke einzigartig sind, bin ich auf folgendes Zitat gestossen:

> Jeder Mensch hat ein völlig individuelles Fingerbild. Selbst eineiige Zwillinge können anhand ihrer Fingerbilder eindeutig unterschieden werden. Die einzelnen Merkmale eines Fingerbildes wie Gabelungen, Schleifen und Wirbel nennt man Minutien (Minuzien [lat.]: Kleinigkeiten). Diese Minutien bleiben während des ganzen Lebens unverändert und werden deshalb für den Vergleich herangezogen.[8]

[7] Siehe: http://www.neuer-reisepass.de/biometrie.htm
[8] Siehe: http://www.heumann-webdesign.de/pages/biometrie/verfahren/finger/bv-fing.html

Ein Spezialscanner erzeugt ein Digitalbild eines Fingerabdrucks, indem die Fingerspitze mit Licht bestrahl wird. Die erhöhten Bereiche reflektieren dabei mehr Licht als die dazwischen liegenden Täler des Fingerabdrucks.

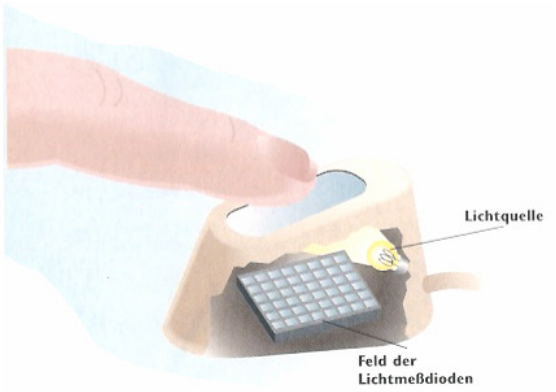

Abb. 3 Querschnitt eines Fingerabdruckscanners

Fingerabdruck-Identifizierungssoftware (FID) analysiert die Erhebungen, indem sie nach zwei spezifischen Merkmalstypen sucht. Das ist zum einen der „Kern“ oder Mittelpunkt des Abdrucks, und zum anderen die kleinen Details oder „Minutien“ – die Punkte, an denen die Erhebungen enden oder sich teilen.

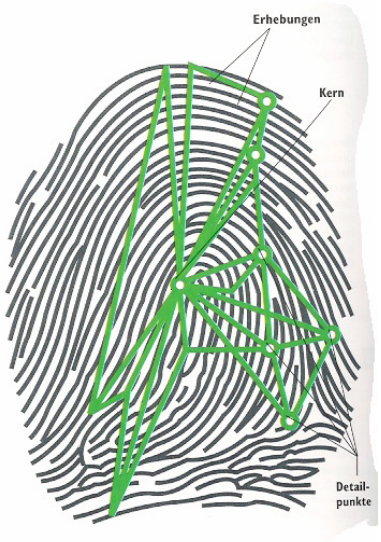

Abb. 4 Minutien

Die FID- Software berechnet die Abstände und Winkel zwischen den Detailpunkten.
Auch wenn der Finger nicht ganz in der Mitte liegt oder sich während des Scannvorgangs dreht, ändern sich die Verhältnisse zwischen den hier dargestellten grünen Punkten kaum.

Da aufgrund einer Schnittwunde oder Abweichungen anderer Ursache mitunter nicht alle Detailpunkte erfasst werden könnten, kann die Software als bestmögliche Option die Wahrscheinlichkeit prüfen, ob der Abdruck einem anderen Abdruck entspricht. Stimmt ein bekannter Abdruck in einem vertretbaren Rahmen mit einem anderen Fingerabdruck überein, so erlaubt die Software Zugriff auf den je weiligen Gegen-stand, wie z.B. den Computer oder die verschlossene Tür, die er überwacht.

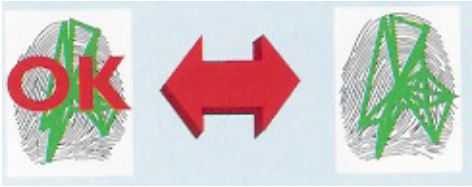

Abb. 5 Fingerabdruckprüfung

3.4 RFID Grundlagen

RFID steht für **R**adio **F**requenz **Id**entifikation, was so viel heisst wie Identifizierung per Funk. Das RFID-System besteht aus einem **RFID-Transponder** mit dem **RFID- Tag** und dem **RFID-Lesegerät**. Der Transponder enthält einen Microchip und eine Antenne. RFID-Tags sind Chips, welche **gespeicherte Daten** enthalten. Sie werden z.B. zur Kennzeichnung an Waren, Paletten und Schachteln befestigt.

Energieversorgung brauchen die Chips in der Regel nicht.

Hierbei unterscheidet man zwischen aktiven und passiven Transpondern. Sobald ein passiver Transponder in das elektromagnetische Resonanzfeld des Lesegeräts kommt, entzieht der Transponder Energie aus dem elektromagnetischen Feld. Es ist also kein Akku und keine Batterie notwendig. Die gesamte **Energieversorgung** liefert das Lesegerät, wobei bei aktiven Transpondern eine zusätzliche Stromversorgung notwendig wäre. ☞ Siehe Abb.7

Transponder gibt es in sehr vielen verschiedenen Bauformen. Am bekanntesten sind die Etiketten zum Aufkleben auf Waren. Es gibt sie aber auch eingegossen, in Glaskapseln und in robusten Formen für Container.

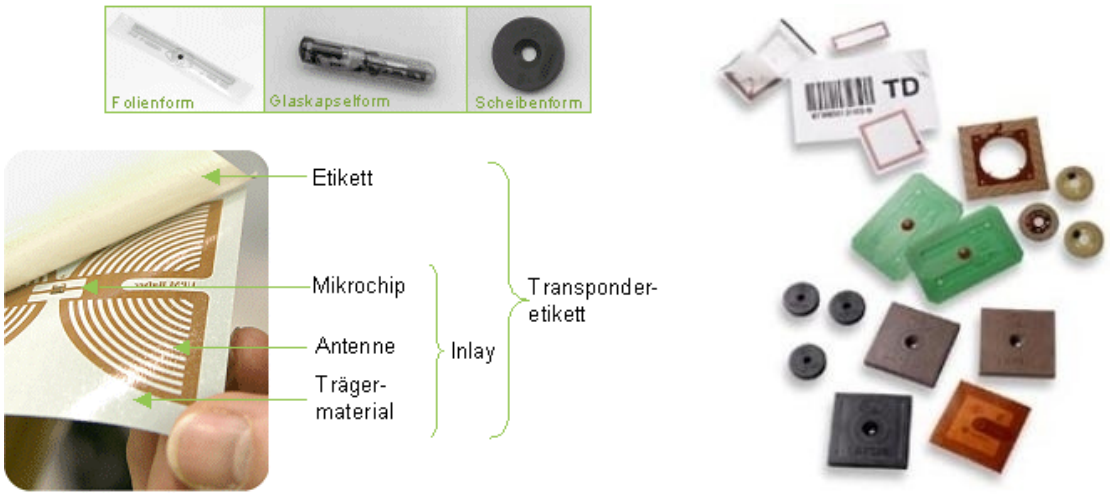

Abb. 6 Vielfalt der RFID Transponder

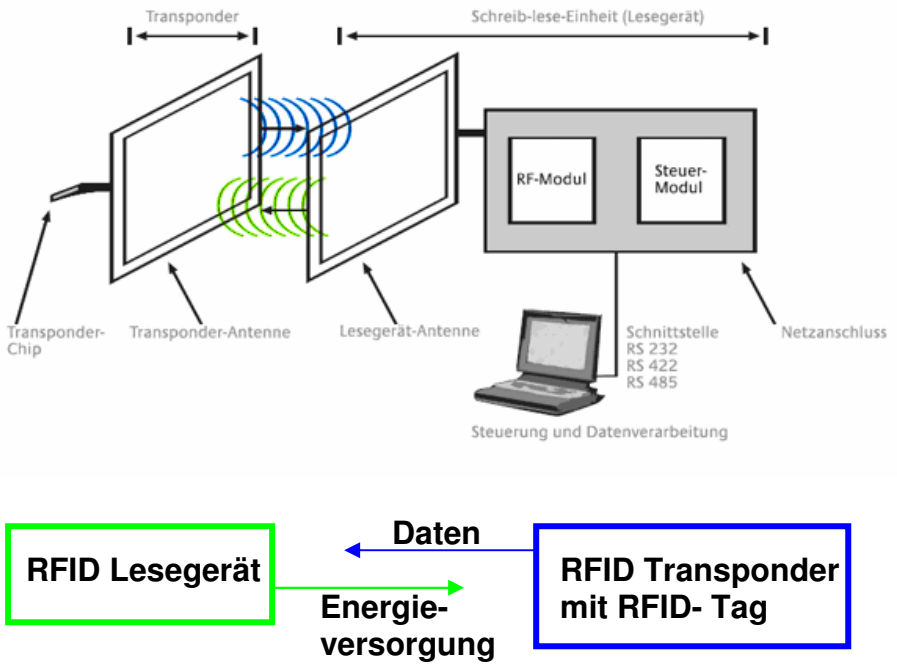

Abb. 7 Schematischer Aufbau eines RFID Systems

3.5 Schweizer Datenschutzverantwortlicher

In der Schweiz gibt es einen Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB). Zurzeit hat dieses Amt Hanspeter Thür inne.

Auf der Homepage des EDÖB[9] werden wir darüber aufgeklärt, welche Hauptaufgaben dieses Amt in der Schweiz umfasst:

- Aufsicht über Bundesorgane
- Aufsicht über Privatpersonen
- Beratung von privaten Personen
- Unterstützung und Beratung der Organe des Bundes und der Kantone
- Stellungnahme zu Rechtsvorlagen des Bundes
- Zusammenarbeit mit in- und ausländischen Datenschutzbehörden
- Information der Öffentlichkeit
- Führung und Veröffentlichung des Registers der Datensammlungen

Um diese Teilbereiche abzudecken kann der EDÖB entweder selber oder auf Meldung Dritter Sachverhalte abklären und Empfehlungen erlassen.

Im Privatbereich übernimmt der EDÖB eine beratende Funktion. Hauptsächlich erläutert er das Datenschutzgesetz und Verordnungen und bietet u.a. Hilfe bei der Registrierung von Datensammlungen. Auch kann er bei rechtlichen und technischen Fragen angefragt werden.

[9] Siehe http://www.edoeb.admin.ch/org/00447/index.html?lang=de

4. Umfrage

Gleich zu Beginn unserer Arbeit haben wir auf der privaten Domain von Luca eine kleine anonyme Umfrage ins Internet gestellt, wo wir den Leuten die Frage stellten, ob sie sich im Alltag beobachtet fühlen.
Luca hat diese Umfrage darauf in seinem Freundeskreis sowie in diversen Internetplattformen verbreitet.

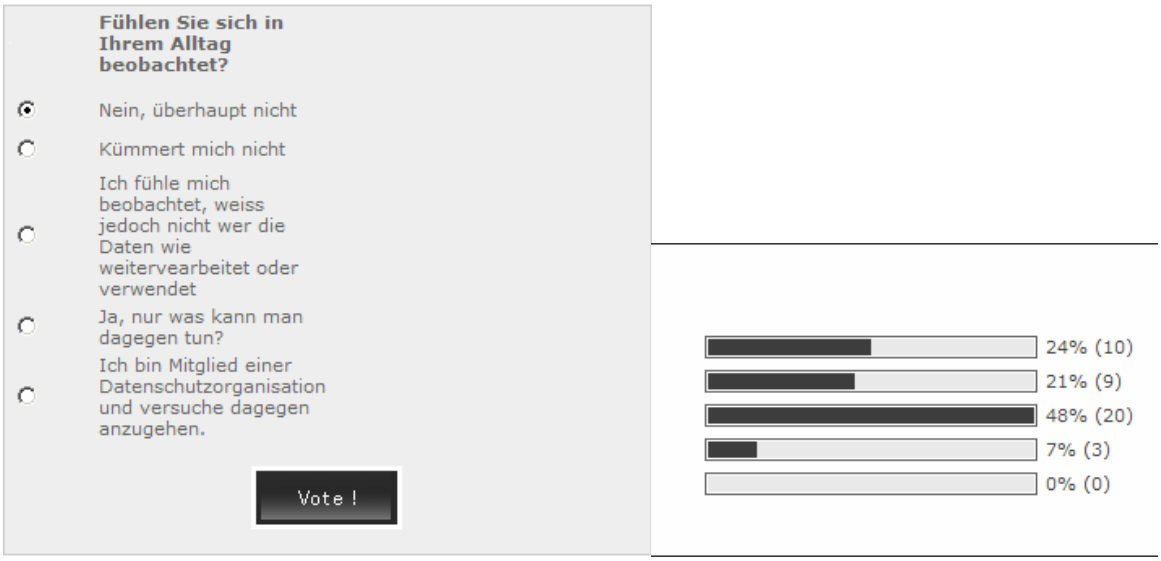

Abb. 8 Umfrage

Die Auswertung[10] (Stand 08.12.07) sieht wie folgt aus:

- Beinahe die Hälfte der Befragten gab an, dass sie sich im Alltag beobachtet fühlen, aber nicht wissen, wer die Daten wie weiterverarbeitet oder verwendet.
- Rund ein viertel der Befragten fühlt sich im Alltag nicht überwacht
- Rund ein fünftel kümmert es nicht, ob sie beobachtet werden
- Lediglich eine Minderheit von 7% gab an, dass sie sich beobachtet fühlen und mehr darüber erfahren möchten, wie man sich schützen kann
- Keiner der Befragten war Mitglied einer Datenschutzorganisation.

5. Aktuelle Beispiele

In diesem Kapitel werden wir auf einige aktuelle Technologien und Gegebenheiten in unserer Gesellschaft eingehen. Da wir den Rahmen unserer Arbeit jedoch nicht sprengen wollen und zwecks Vorgaben des SVA-Reglements auch nicht dürfen, beschränken wir uns in diesem Kapitel auf die Thematik der Kundenkarten, RFID, Datamining und den neuen Schweizer Pass.
Danach werden wir wie in der Einleitung bereits angetönt noch auf einen technologischen Aspekt eingehen, welcher uns in Zukunft betreffen könnte.

[10] Siehe http://www.easy-poll.com/sonda.vote.2.29334

5.1 Kundenkarten

Wer kennt sie nicht?. Kundenkarten sind heute weit verbreitet.
Wer beispielsweise im Migros oder Coop an der Kasse ansteht wird mit grösster Wahrscheinlichkeit beim Bezahlen nach der „Supercard“ oder „Cumulus“ Karte gefragt. Hat man keine, so kommt man sich schon beinahe wie ein „Outsider“ vor.
Zugegeben, verlockend klingt das System schon. Beim Bezahlen kurz die Karte an den Scanner halten und schon erhält man Punkte, von denen man später beispielsweise von Vergünstigungen, Aktionen und Prämien profitieren kann.

Abb. 9 Kundenkarten

Nebst allen Vorteilen, welche eine solche Karte bietet, muss man aber bedenken, dass man nebst dem Einbuchen von Bonuspunkten auch Daten über das Einkaufsverhalten preisgibt. Gewöhnt man sich also daran eine solche Karte regelmässig zu nutzen, entsteht mit der Zeit ein Käuferprofil. Der Detailhändler kann dadurch das Sortiment den örtlichen Bedürfnissen so wie den Kunden entsprechend besser anpassen. Käuferprofile können aber auch missbraucht werden. Kundendaten könnten beispielsweise an Adresshandelsagenturen und dann weiter an Werbefirmen verkauft werden. Diese haben dann die Möglichkeit, die Werbung an einen gewissen Kundenkreis zu verschicken oder die Werbung einzelnen Käuferprofilen anzupassen. Wir wollen nun herausfinden, an wen Migros und Coop diese Informationen weitergibt und besuchen deren Internetseiten[11].

Coop sowie Migros geben auf ihrer Internetseite bekannt, die Kundendaten nur für eine gewisse Zeit zu speichern und ausschliesslich an Partnerfirmen weiterzugeben.

Migros-Partner sind:

- Migrol
- Migros Bank
- Do it+garden
- Obi, Micasa
- SportXX
- M-Electronics
- Migros Klubschule
- Ex libris, Hotelplan
- Eurocenters, Switzerland Travel Centre
- Mobility Carsharing
- Leshop.ch

[11] Siehe http://www.migros.ch
http://www.coop.ch

Partnerfirmen von Coop sind:

- Coop Restaurant
- Coop City
- Coop Bau+Hobby, Lumimart
- Coop Vitality-Apotheke
- Coop Pronto
- Bank Coop
- Christ
- IST- Coop travel
- Interdiscount
- TopTip
- Import Parfumerie
- Swisscom Fixnet
- Gidor Coiffure
- Pneu Egger
- Viseca (Kreditkartenmarkt)
- Hertz

Auszug aus den Datenschutzbestimmungen[12] von Coop:

> Ihre Daten werden nur innerhalb der Coop-Gruppe und an Supercard Partnerfirmen (Firmen ausserhalb der Coop-Gruppe, welche Superpunkte ausgeben oder Gutscheine als Supercard Treue-Prämien verschicken) weitergegeben. Diese Firmen haben das Recht die Daten für eigene Marketingzwecke zu benutzen und können die erhaltenen Kundendaten via professionelle Adresshändler mit zusätzlichen Merkmalen (wie Haushaltsgrösse, Hausbesitz, Alter, Einkommensklasse etc.) ergänzen. Ihre Daten werden ferner an Firmen weitergegeben, welche Ihre Daten im Rahmen eines Auftragsverhältnisses bearbeiten, **wobei ein Datentransfer ins Ausland** (Holland und Deutschland) in Einzelfällen **erfolgt**. Es wird sichergestellt, dass keine über den konkreten Kundenauftrag hinausgehende Verwendung der Daten durch die bearbeitende Partnerfirma stattfindet und diese die Daten weder für sich verwendet, noch einem Dritten weitergibt.

Auszug aus den Datenschutzbestimmungen[13] von Migros:

> Personen, die uns bei ihrer Anmeldung zu M-CUMULUS erlaubt haben, ihre Adresse zu verwenden, erhalten Angebote und Informationen von Firmen der Migros Gemeinschaft. Wann immer wir Sie anschreiben, vermerken wir, dass wir dies aufgrund Ihrer Erlaubnis anlässlich der Anmeldung zu M-CUMULUS tun. Falls Sie darauf verzichten möchten, weitere Angebote und Informationen von uns zu erhalten, teilen sie uns dies mit. Selbst-verständlich respektieren wir Ihren Wunsch gerne. Die CUMULUS-Infoline erreichen Sie unter 0848 85 0848. Sie können die Anpassung auf www.M-CUMULUS.ch unter Ihr Konto auch gleich selbst vornehmen.
>
> Übrigens: Sie können unbesorgt sein, Ihre Adresse wird weder verkauft, noch Firmen ausserhalb der M-Gemeinschaft zugänglich gemacht.

[12] Siehe http://www.supercard.ch/scin/dataSecurity.do
[13] Siehe http://migros.ch/DE/M-CUMULUS/Ueber_mcumulus/Datenschutz/Seiten/Datenschutz.aspx

Als nächstes schauten wir nach, wie lange Coop bzw. Migros die gesammelten Daten speichert.

Auszug aus den Datenschutzbestimmungen[14] von Coop:

> Die Details Ihrer Bestellungen/Einkäufe (Warenkorb) können in Bezug auf Einkaufshäufigkeit und -betrag ausgewertet werden. In Bezug auf deren Inhalt erfolgt eine Auswertung nur in anonymisierter Form. Von Gesetzes wegen muss aber eine Kopie des Kassenbons (inkl. Supercard-Nummer) während 10 Jahren aufbewahrt werden. Auch diese Kopie wird nicht zu einer individualisierten Warenkorbanalyse benutzt.
> Die Daten ihrer Bestellungen/Einkäufe werden periodisch saldiert und später gelöscht. Im weiteren sind wir aufgrund gesetzlicher Bestimmungen verpflichtet, gewisse Unterlagen (z.B. strafrechtlich relevante Akten) bis zu 10 Jahren aufzubewahren.

Auszug aus den Datenschutzbestimmungen[15] von Migros:

> Kassenzetteltotale werden maximal 3 Jahre aufbewahrt. Die detaillierten Einkaufsdaten von CUMULUS-Teilnehmern welche beim Einkaufen Ihre Karte vorgewiesen haben, werden 15 Monate lang aufbewahrt. Die detaillierten Einkaufsdaten zeigen, welche Artikel in der Migros eingekauft wurden. Sie sind auch auf www.M-CUMULUS.ch unter Ihr Konto abrufbar. Dort können Sie jederzeit die über Sie gesammelten Einkaufs- und Personendaten aufrufen.

5.2 EPC Netzwerk im Supermarkt

Gleich anschliessend an das Kapitel der Kundenkarten, wollen wir uns mit dem Thema RFID im Supermarkt befassen. Dazu sollte man wissen, dass man plant, den heutigen sehr weit verbreiteten und bekannten Strichcode (EAN)[16], durch einen neuen Code, den so genannten „EPC“ zu ersetzen. Lange Wartezeiten an der Kasse fallen weg, da die Produkte nicht mehr gescannt werden müssen.
Klingt doch gut, wenn man bedenkt, wie doch heute in unserer Gesellschaft alles so schnell gehen muss. Oder steckt da vielleicht doch noch mehr dahinter?

EPC steht für **E**lectronic **P**roduct **C**ode. Der Electronic Product Code spielt im Zusammenhang mit den RFID-Tags eine wichtige Rolle. Es handelt sich dabei um eine weltweit überschneidungsfreie Ziffernfolge, mit der jedes Produkt auf der ganzen Welt eindeutig gekennzeichnet und somit jederzeit identifiziert werden kann.

Der Aufbau sieht dabei sieht folgendermassen aus:

- Der Datenkopf (Header) klassifiziert, welche EPC-Version genutzt wird und welche Informationsart der Artikelnummerierung verwendet wird.
- Der EPC-Manager stellt die Kennzeichnungsnummer des Nummerngebers, z.B. des Herstellers dar
- Die Objektklasse bezeichnet die Objektnummer, z.B. eine Artikelnummer
- Die Seriennummer dient zur Identifikation des Objektes

[14] Siehe http://www.supercard.ch/scin/dataSecurity.do
[15] Siehe http://migros.ch/DE/MCUMULUS/Ueber_mcumulus/Datenschutz/Seiten/Datenschutz.aspx
[16] Die **EAN** steht für **International Article Number** (früher **European Article Number**) und ist eine Produktkennzeichnung für Handelsartikel

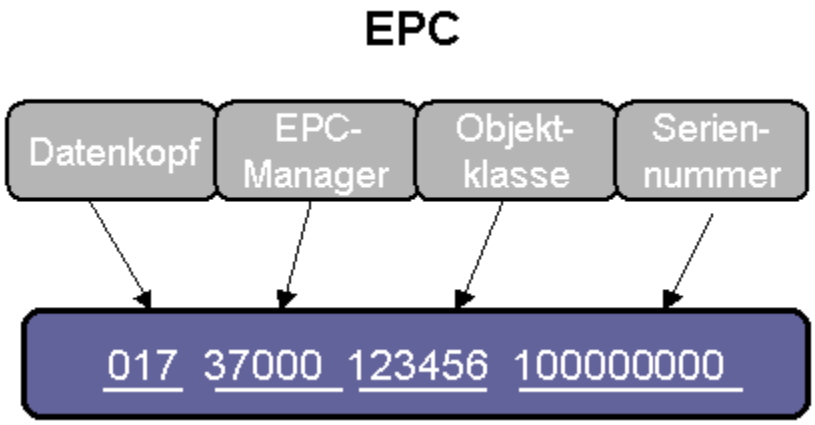

Abb. 10 Aufbau des Electronic Product Code

Die EPC-Nummer trägt keine weiteren Daten, die Produkteigenschaften abbilden.
Daten wie z.B. Herstellung des Produktes, wohin es geht, wie lange es bereits im Regal gelegen hat etc. könnten aber problemlos mit Datenbanken verknüpft werden.

Abb. 11 Der Aufbau des EPC ermöglicht eine Identifikation jedes einzelnen Artikels

Der Walmart[17] in Amerika, sowie der Future Store[18] in Deutschland nutzen bereits ein solches System. Datenschützer befürchten nun, dass durch dieses System beispielsweise Bewegungsprofile erstellt werden könnten. In Kombination mit einer Kundenkarte weiss das System nicht nur, was im Warenkorb liegt, sondern auch wer den Wagen schiebt. Durch die Kundenkarte könnte auch festgestellt werden, wer den Supermarkt betritt und wann wieder verlässt, sofern eine entsprechende Einrichtung installiert werden würde. Datenschützer gehen auch davon aus, dass die winzigen Funketiketten auch problemlos in Kleidungsstücke und Schuhe eingenäht werden könnten, ohne dass die Käufer etwas davon wissen. Datenschützer fordern, dass die Funketiketten beim Bezahlen daher zwingend deaktiviert werden müssen. Weiterhin liessen sich noch gezielter Käuferprofile erstellen, da das System erlaubt, noch mehr und präzisere Daten festzuhalten.
Auf der nächsten Seite wollen wir uns eine Grafik ansehen, die verdeutlicht, wie ein EPC Netzwerk in einem Supermarkt etwa aussehen könnte.

[17] Siehe http://www.zdnet.de/news/business/0,39023142,39128876,00.htm
[18] Siehe http://www.future-store.org/servlet/PB/menu/1007054/index.html

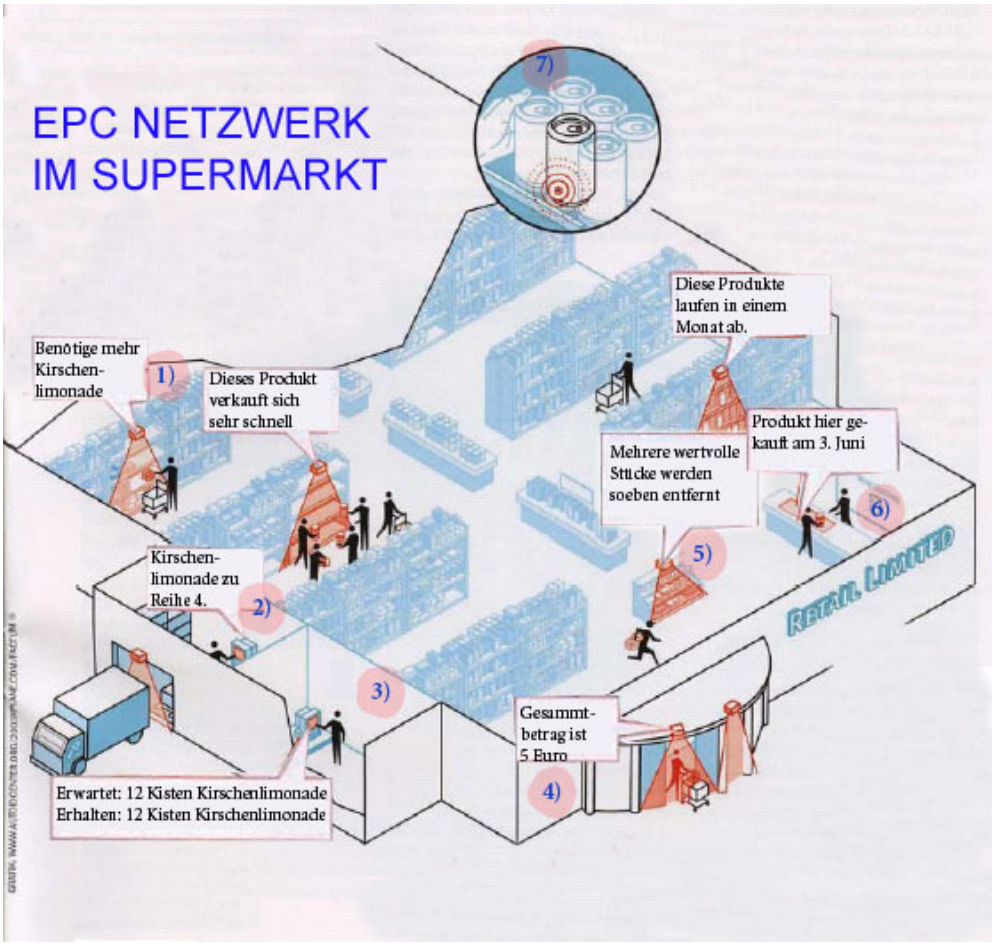

Abb. 12 EPC Netzwerk im Supermarkt

5.2.1 Beschreibung der Grafik (EPC Netzwerk)

1) Denkende Regale

Die Angestellten wissen sofort, wenn es einen Ansturm auf Erdnüsse aufgrund einer Sportübertragung im Fernsehen gibt. Sie können das Lager sofort auffüllen. Der Ladenverantwortliche wird alarmiert, wenn verderbliche Waren vor dem Ablaufen sind.

2) Vereinfachung im Vorratsraum

Die Angestellten können rasch und auf einfache Weise sämtliche Produkte im Lager lokalisieren, selbst solche, die auf gemischten Paletten liegen. Der Detaillist nutzt das System, um die Menge festzustellen, die Lage und den Bestimmungsort aller Produkte. Damit kann die Warenhausfunktion im Lager auf ein Minimum reduziert werden.

3) Einfache Lagerbewirtschaftung

Manager können überprüfen woher die Ware kommt, wann sie ankommen sollte und sobald eingetroffen, ob die Lieferung in Ordnung ist.

4) Sicherheit

EPC Lesegeräte erfassen alles, auch versteckte Produkte und Gegenstände - zumindest im Einkaufswagen. Die Kunden gehen ein und aus ohne Schlange zu stehen

5) Diebstahl Sicherung

Da die Produkte mit Transpondern ausgestattet sind, wird das Stehlen schwieriger. Die Produkte können laufend identifiziert und verdächtige Aktivitäten dem System gemeldet werden.

6) Rücksendungen bearbeiten

Die Mitarbeiter können ein Produkt scannen, um festzustellen, ob die zurückgegebene Flasche aus Ihrem Laden stammt, wann sie verkauft wurde, für welchen Betrag sie verkauft wurde oder ob sie gestohlen wurde. Es ist keine Quittung mehr nötig.

7) So funktioniert es

Jede Ware enthält einen Mikrochip mit einem individuellen Code, einem Electronic Product Code (EPC). Der RFID Chip erlaubt ein präzises Mitverfolgen des Weges, den ein Produkt macht. Kisten und Paletten können ihre eigenen elektronischen Etiketten tragen.

5.3 Datamining

Datamining ermöglicht es, in Datenbeständen mit Hilfe statischer Verfahren Regeln und Muster, bzw. statistische Auffälligkeiten aufzuspüren und diese auszuwerten.
Genutzt wird es vor allem von Firmen, welche Werbung produzieren. Mit Datamining können also Veränderungen im Kaufverhalten von Kunden- sowie Kundengruppen registriert werden, welche dann in neue Geschäftsstrategien miteinbezogen werden. Auch kann so abweichendes Verhalten einzelner Personen erkannt werden.

Die folgende Liste zeigt drei weit verbreitete Anwendungsmöglichkeiten von Datamining auf:

- Kundensegmentierung im Marketing (gezielte Werbemassnahmen)
- Warenkorbanalyse (Produktplatzierung im Supermarkt)
- Kampagnenmanagement (Selektion von Zielgruppen für Marketingaktionen)

Als typisches Beispiel für Datamining könnte man die Firma amazone nennen.
Das Empfehlungssystem von amazone.com verwendet beispielsweise Informationen früherer Einkäufe, um Empfehlungen für zukünftige Einkäufe abzugeben oder zukünftiges Verhalten der Kunden vorherzusagen.

5.4 Biometrischer Pass

Dieses Kapitel soll über den neuen Schweizer Reisepass informieren.
Auf der offiziellen Internetseite[19] lesen wir folgendes nach:

> Biometrische Daten im Pass sind nichts Neues. Bereits der Pass 85 und der Pass 03 enthalten biometrische Daten: Foto, Grösse und Unterschrift der Person, auf deren Namen er lautet. Die Neuerung, welche die aktuelle Technologie nun ermöglicht, besteht darin, dass diese Daten auf einem Chip abgespeichert werden. Zusätzlich zu den bisher im Pass enthaltenen Daten zur Person wird auf dem Chip ein digitales Foto im jpeg-Format abgespeichert, das mit dem im Pass abgebildeten identisch ist. In naher Zukunft, sollen gemäss den Standards der Europäischen Union Pässe ausgestellt werden, die darüber hinaus auch zwei Fingerabdrücke enthalten.

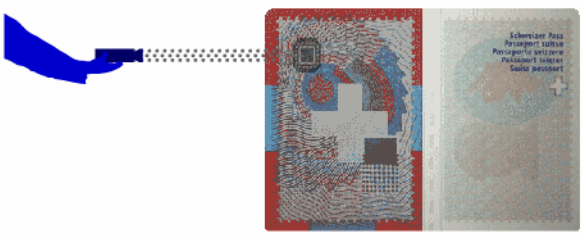

Abb. 13 Der neue Pass06 mit eingebautem RFID Chip

Weil es sich im Pass06 um elektronische Daten handelt, können diese in einem automatischen Vorgang mit den Daten derjenigen Person verglichen werden, die den Pass vorweist. Aufwändige Datenschutz- und Sicherheitsmassnahmen verhindern, dass die Daten unberechtigterweise ausgelesen werden.

> Die Daten, die auf dem Chip im Pass 06 gespeichert sind, können - mit der inzwischen weit verbreiteten Technologie der Radio Frequency Identification (RFID) - kontaktlos über eine kurze Distanz ausgelesen werden. Der grosse Unterschied zu herkömmlichen RFID-Produkten besteht jedoch in den umfangreichen Datenschutz- und Sicherheitsmassnahmen, die beim Pass getroffen werden. So werden die gespeicherten Daten zum einen so abgelegt, dass sie nach der Herstellung des Passes nicht mehr verändert werden können («read-only»). Zudem kann anhand einer elektronischen Signatur jederzeit deren Authentizität überprüft werden.

Um ein unbefugtes Auslesen der Daten zu verhindern, sei der Pass durch eine maschinenlesbare Zone (MRZ) gesichert. Diese Zone kann nur mit geöffnetem Pass gelesen werden.

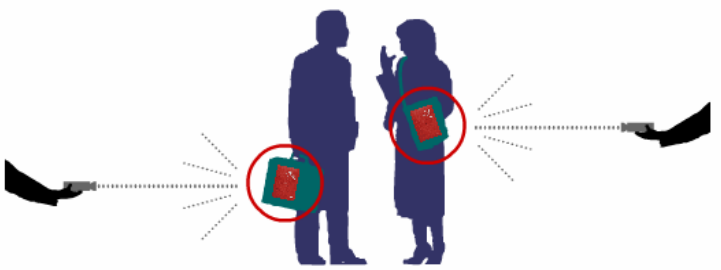

Abb. 14 Bei geschlossenem Pass können die Daten nicht ausgelesen werden

Jeder, der sich schon mit Sicherheitssystemen auseinandergesetzt hat, weiss dass es keine 100%ige Sicherheit gibt.

[19] Siehe http://www.schweizerpass.admin.ch/

Äusserst bedenklich ist beispielsweise eine Publikation[20], welche darüber berichtet, wie ein Forscher die neuen Pässe knackte.

> Er nannte die derzeitige E-Pass-Architektur einen "Hirnschaden". Aus seiner Sicht sind RFID-Pässe eine immense Geldverschwendung, da sie in keinerlei Hinsicht die Sicherheit erhöhen, erklärte er gegenüber dem Magazin Wired. Es habe ihn nur zwei Wochen gekostet, die angeblich fälschungssicheren Ausweise zu hacken und herauszufinden, wie sich die elektronischen Daten eines RFID-Passes auslesen, klonen und auf einen anderen Chip übertragen lassen. Dies sei auch mit Smartcards möglich, die dann wiederum für Zutrittsberechtigung genutzt werden können.

6. Interview

Herr Sloot, Sie haben sich schon beruflich mit Datenschutz auseinandergesetzt. Wer sind Sie und welche Aufgaben umfasste Ihre Arbeit?

Mein Name ist René Sloot. Neben dem Schulunterricht an der GIBMuttenz arbeite ich in einem Heim für Behinderte, wo ich die komplette Wartung von Netzwerk und Serverbetrieb übernehme. Ausserdem bin ich Chefexperte an den Lehrabschlussprüfungen der Informatiker in Basel. Vor einiger Zeit habe ich noch für den EDSB in Bern gearbeitet.

Was war Ihr Auftrag beim EDSB?

Die grössten Probleme beim Datenschutz kommen oft nicht von ausserhalb, sondern sind innerhalb eines Unternehmens anzutreffen. Dies betrifft z.B. Datendiebstahl und das Beschädigen und Verändern von Daten. Zusammen mit dem EDSB habe ich an einem Paket gearbeitet, welches anhand von Berechtigungsstufen und Verschlüsselung die vorher genannten Szenarien verhindern soll. Das Paket wurde aber nie fertig gestellt.

Zu Beginn unserer SVA haben wir eine kleine Umfrage ins Internet gestellt, wo wir die Frage gestellt haben, ob sich die Leute im Alltag überwacht fühlen.
Wie würden Sie spontan auf diese Frage antworten?

Nein, ich fühle mich nicht im Geringsten überwacht. Jetzt ist aber zwischen zwei Varianten zu unterscheiden. Zum einen wäre dies „wer hat was wann gemacht“ oder geht es um Prävention? Wenn ich in einem Einkaufszentrum bin und dort eine Kamera sehe, fühle ich mich nicht überwacht. Wenn ich jedoch wüsste dass diese Videos noch über ein Jahr aufbewahrt und diese dann noch weiterverarbeitet oder weitergereicht werden, dann erst hätte ich ein Problem damit.

[20] Siehe http://www.silicon.de/enid/client_server_host/21295

Denken Sie, dass wir im Alltag zu viele Informationen über uns preisgeben? Falls ja, wo denken Sie, dass wir Spuren hinterlassen und wie könnten wir uns dagegen schützen?

In der heutigen Zeit kann man einen Grossteil der Daten überhaupt nicht schützen. Ich sehe Tag für Tag, dass die Leute Informationen zu ihrer Person unbewusst herausgeben – Name, Geburtstagsdatum, Adresse etc. Vor allem tun sie dies, wenn es etwas zu gewinnen gibt. Sie können meistens nicht beurteilen, ob die Firma nun vertrauenswürdig ist oder nicht.

Ich hatte selber zwei Abos bei CHIP und einen Newsletter abonniert. Habe letzte Woche alles gekündet. Geworben wurde der Newsletter als normaler Newsletter mit Informationen zu CHIP, bekommen habe ich jedoch nur Werbung und das von mehr als nur einer Firma. Fazit: Daten werden weitergegeben. Dem müssen sich viele einfach bewusst werden. Niemand liest Geschäftsbedingungen, in welchen meistens versteckt darauf hingewiesen wird, dass die Daten an Dritte weitergegeben werden.

Beim Datenschutz geht es primär darum, dass der Mensch grundsätzlich selbst entscheiden kann, wem wann welche seiner persönlichen Daten zugänglich sein sollen und dass diese vor Missbrauch geschützt sind. Denken Sie, dass dieser Grundsatz in der Schweiz gewährleistet wird?

Einerseits wird der ganze Datenschutz restriktiv gehandhabt, andererseits nehmen es die Datenschutzbeauftragten zu locker. Ich selber könnte für einen Nachbarn beim Steueramt anrufen und nach dessen Daten fragen. Ein bisschen schlau anstellen und ich hab sie. In der Schweiz wird relativ leichtsinnig mit Daten umgegangen. Als Beispiel medizinische Personendaten: Ein Arzt darf die Informationen nur weitergeben, wenn er meine Zustimmung hat. Wird diese Weisung in der Realität eingehalten? Diese Informationen dürfen ohne meine Zustimmung nicht von Arzt A zu Arzt B gelangen – wird aber gemacht. Ich finde medizinische Daten sowie die eines Betreibungsamtes dürfen nicht für die Öffentlichkeit offengelegt werden. Egal unter welchen Umständen. Ausserdem gibt es ein Problem bei den Betreibungen. Jedermann kann mich betreiben – auch wenn die Betreibung storniert wird, der Eintrag bleibt bestehen, was z.B. die Suche einer Wohnung behindern kann.

Wie stehen Sie den heute sehr weit verbreiteten Kundenkarten gegenüber? Nutzen Sie beispielsweise auch eine Coop Profit oder Cumulus Karte?

Ja, ich benutze sie. Habe die Supercard und auch die Cumulus. Mir ist es grundsätzlich egal, ob die Firmen wissen, was ich bei ihnen einkaufe.
Es stört mich doch nicht, wenn die Migros weiss, dass ich bei ihnen einen Staubsauger gekauft habe. Stören würde mich jedoch, wenn die Migros erfahren würde, was ich bei Coop einkaufe. Eine Vermischung der Daten sowie das Weiterreichen wären auch nicht positiv für die Privatperson.

Die Technologie RFID sollte im Alltag vieles erleichtern. Ist Ihnen dieser Begriff bekannt? Falls ja, welche Einsatzbeispiele von RFID kennen Sie und wo sehen Sie die Gefahren?

Ja, dieser Begriff ist mir bekannt.
Karstadt in Deutschland vertreibt schon viele Produkte in welchen RFID installiert ist.

Ein Beispiel in der Schweiz wäre sicherlich Manor. Manor lehnt es jedoch ab RFID in Produkten zu integrieren. Es wird nur in den Lagerhallen benutzt, um zu wissen, wo sich gerade ein Laster mit welchem Ladegut befindet.

Was halten Sie von der Erfassung biometrischer Daten und wie stehen Sie dem neuen Schweizer Reisepass gegenüber?

Grundsätzlich ist es notwendig eine Fälschungssicherheit bei Pässen einzusetzen. Aber ob es wirklich nötig ist, die biometrischen Daten zu erfassen und diese im Pass zu integrieren, ist fraglich. Ausserdem: es wird doch nach einer gewissen Zeit sicher möglich sein, diese Daten als Drittperson auszulesen.

Wir sind bei unserer Arbeit noch einen Schritt weiter gegangen und haben uns auch über zukünftige Technologien Gedanken gemacht. Dabei sind wir auf eine Entwicklung namens „Verichip" gestossen. Es handelt sich dabei um ein Chipimplantat für Menschen, auf dem beispielsweise die gesamte Krankenakte gespeichert werden kann. Könnten Sie sich vorstellen auch eines Tages einen solchen Chip unter der Haut zu tragen oder geht diese Entwicklung Ihrer Meinung nach zu weit?

Hier ein kleines Beispiel: In Barcelona gibt es in einem Nachtclub im olympischen Dorf schon Verichips. Diese werden den Stammgästen unter die Haut implantiert. Auch hier tritt wieder dasselbe Problem auf: die Daten können sicher - die Frage ist wann - durch Dritte gelesen werden. Momentan muss man sicher noch nahe beim Lesegerät sein. Doch wie sieht es in 10 Jahren aus?

Ich selber würde mir nie einen solchen Chip implantieren lassen, rein aus Angst davor, dass es zu weit gehen könnte und die Daten an die falschen Personen geraten.

An dieser Stellte möchten wir uns nochmals ganz herzlich für das Interview mit Herrn Sloot bedanken.

7. Bedenkenswertes

Bevor wir unsere Arbeit abschliessen, kommen wir noch zu einem Teil, der Sie vielleicht zum Nachdenken anregen könnte. Es mag vielleicht etwas ketzerisch klingen, aber könnten Sie sich vorstellen, dass wir eines Tages kein Bargeld, Ausweise, Kreditkarten und sonstige Personalien mehr bei uns tragen müssten?
Halten Sie es für möglich in naher oder ferner Zukunft einer Nummer zugeordnet und in einer grossen Datenbank gespeichert zu sein?
Eine Entwicklung namens „VeriChip" aus den USA hat derartige Fragen in uns aufkommen lassen. Im nachfolgenden Kapitel wollen wir darauf eingehen, was man unter diesem Chip genau versteht und auf ein aktuelles Einsatzbeispiel eingehen.

7.1 VeriChip

Der „VeriChip" von der Firma Applied Digital Solutions[21] ist ein Chipimplantat für Menschen in Reiskorngrösse. Es handelt sich dabei um einen RFID-Transponder in einem etwa 12mm langen Glaszylinder mit 2mm Durchmesser. Seine Grösse erlaubt es, ihn auch in ambulanter Behandlung einzusetzen. Interne Energie braucht der Chip nicht, denn er lässt sich lesen, sobald er von einem Scanner erkannt wird.
Die Reichweite hängt von der Stärke des elektrischen Impulses von aussen ab und kann durchaus einige Meter betragen.

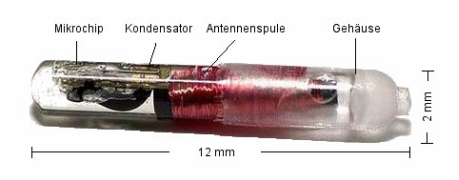

Abb. 16 Verichip stark vergrössert

Abb. 15 Chip im Vergleich mit Reiskorn

7.1.2 Aktuelles Einsatzbeispiel

Wer zu den VIP-Mitgliedern im „Baja Beach Club“[22] in Barcelona gehört, muss keine Geldbörse mehr mit sich herumtragen. Sämtliche Drinks werden bequem über den Oberarm abgerechnet. Der Baja Beach Club ist damit die erste Diskothek weltweit, die auf ein solches System zurückgreift.

> Zum siebten Jahrestag seines Baja Beach Clubs im spanischen Barcelona wollte Conrad Chase dem Publikum etwas Besonderes bieten. Nicht nur eine VIP-Lounge liess der Clubbetreiber einrichten, passend dazu präsentierte Chase auch ein neues Eintrittssystem. Stammgäste der Diskothek können sich künftig einen Microchip in den Oberarm implantieren lassen. Der Vorteil: Bei Besuchen des Etablissements brauchen die Chipträger künftig weder ihren Ausweis einzustecken, noch ihr Portemonnaie mitzunehmen. Auf dem Microchip werden nicht nur relevante Personendaten gespeichert. Die Träger können Geld einzahlen und auf ihrem "VeriChip" gutschreiben lassen.[23]

Abb. 17 Person lässt sich Verichip implantieren

Abb. 18 Verichip Identifikationsprüfung

[21] Website der Firma Applied Digital Solutions: http://www.adsx.com
[22] Website des Baja Beach Club Spanien: http://www.bajabeach.es/
[23] Siehe dazu Telepolis Artikel: http://www.heise.de/tp/r4/artikel/17/17707/1.html

8. Persönliches Fazit von Luca und Daniel

Daniel

Mir hat es Spass gemacht, eine Arbeit über das Thema Datenschutz zu verfassen.
Ich konnte dabei das Eine oder Andere vertiefen und neue Erkenntnisse gewinnen.
Aus persönlicher Sicht wurde mir klar, dass wir im Alltag sehr viele Spuren hinterlassen und eigentlich keine Gedanken darüber verlieren. Viele dieser Spuren betreffen Abläufe in unserem Alltag, welche bereits normal geworden sind. Zudem stelle ich fest, dass wir uns in einem Zeitalter befinden, in dem durch die zunehmende Vernetzung von Computern immer mehr Informationen gesammelt werden. Informationen sammeln ist grundsätzlich noch nichts Schlimmes, aber es kommt immer darauf an, wohin diese Informationen fliessen und was aus ihnen gemacht wird. Die Vorstellung, dass man per Knopfdruck sämtliche Informationen über uns abrufen kann, halte ich für gefährlich. Wenn ich Technologien wie RFID betrachte, habe ich den Eindruck, dass es früher oder später genau in diese Richtung gehen wird.
Im letzen Kapitel dieser Arbeit haben wir erfahren, dass es bereits Chipimplantate für Menschen gibt und diese Technologie bereits als Zahlungsmittel in einem Club in Spanien verwendet wird. „Da hört für mich der Spass auf!“
Ich rate daher allen, neue und gerade derartige Entwicklungen in unserer Gesellschaft zu hinterfragen.

Luca

Den Entscheid, dieses Thema zu wählen, haben wir erst 2 Wochen nach Beginn der Arbeit an der SVA gefällt – und dieser hat sich auch ausgezahlt. Die Arbeit mit Daniel hat mir viel Freude bereitet da er sich sehr passioniert mit dem Thema auseinandergesetzt hat. Für mich persönlich war die Arbeit sehr interessant, wenn man bedenkt, dass dieses Thema Tag für Tag unser Leben tangiert.
Ich finde es wichtig, dass die Leute sich besser informieren in der heutigen Zeit. Immer und überall werden unsere Daten aufgenommen – wie mit diesen dann weiter gearbeitet wird ist leider nicht immer genug transparent. Darum sollten die Menschen mit ein bisschen Skepsis dem Datenschutz entgegentreten damit das Ganze nicht den falschen Weg einschlägt.

9. Abbildungsverzeichnis und Quellenangaben

Abb1: http://www.raw.at/galerie/images/comix/ueberwachung.gif
Abb2: http://www.itwissen.info/media/lex_pics/small/hb10f13.png
Abb3: Eingescannte Grafik aus Quelle[1]
Abb4: Eingescannte Grafik aus Quelle[1]
Abb5: Eingescannte Grafik aus Quelle[1]
Abb6: http://www.tecchannel.de/imgserver/bdb/346500/346565/original.jpg
Abb7: http://gs1germany.de/common/grafiken/epcglobal/rfid_epc/transponderaufbau.gif
Abb8: Screenshot unserer Umfrage auf http://www.kackvogel.ch
Abb9: http://www.bkb.ch/karten-supercard.jpg
http://www.migrol.ch/images/g_heizoel_cumulus02.gif
Abb10: http://gs1-germany.de/common/grafiken/epcglobal/rfid_epc/aufbau_des_epc.gif
Abb11: http://www.epc-forum.de/epc/index.html

Abb12: Eingescannte Grafik aus Quelle[2]
Abb13: Screenshot von http://www.schweizerpass.admin.ch/
Abb14: Screenshot von http://www.schweizerpass.admin.ch/
Abb15: http://www.dergrossebruder.org/miniwahr/2006/03/28/verichip.png
Abb16: http://business.tomshardware.de/hardware/20060321/images/aufmacher.jpg
Abb17: http://www.heise.de/tp/r4/artikel/17/17707/17707_1.jpg
Abb18: http://www.heise.de/tp/r4/artikel/17/17707/17707_2.jpg

Literatur und Quellenangaben

[1] White, Ron: *So funktionieren Computer*
Markt + Technik, 2000 ISBN: 3-8272-5972-X

[2] Factum-Magazin: Sprechender Staub 8/2003
http://www.factum-magazin.ch NO ISBN

Internet

http://de.wikipedia.com
http://www.heise.de
http://www.telepolis.de
http://www.heumann-webdesign.de/pages/biometrie
http://www.admin.ch
http://www.neuer-reisepass.de
http://www.schweizerpass.admin.ch/
http://www.easy-poll.com
http://www.kackvogel.ch
http://www.edoeb.admin.ch/
http://www.coop.ch
http://www.supercard.ch
http://www.migros.ch
http://www.zdnet.de/
http://www.future-store.org
http://www.adsx.com
http://www.bajabeach.es

10. Anhang

Im Anhang finden Sie folgende Dinge:

- Begründung der Themenwahl
- Arbeitsplanung
- Unser persönliches Mindmap zum Thema Datenschutz

11. Erklärung

Hiermit bestätigen wir, dass wir diese Arbeit ohne fremde Hilfe erstellt haben.

Luca Peter **Daniel Müller**