Absehbare Risiken und Wirkungen beim RFID-Einsatz

Jan E. Hennig, Peter B. Ladkin, Bernd Sieker
{jhennig|ladkin|bsieker}@rvs.uni-bielefeld.de

21. Dezember 2004

Inhaltsverzeichnis

1 Einleitung

RFID steht für Radio Frequency Identification und ist eine Technologie zur automatischen Datenerfassung per Funk. RFID-Tags sind „funkende Etiketten“, die eine Codenummer an ein Lesegerät übermitteln. Es gibt RFID-Tags ohne eigene Energieversorgung, die ihre Energie aus der elektromagnetischen Strahlung des Lesegerätes beziehen. Das gesamt Tag ist so klein, dass es unsichtbar in Gegenstände oder deren Verpackung eingebaut werden kann.

RFID-Technologie wird derzeit im großen Stil als *das* revolutionäre Hilfsmittel der Warenlogistik propagiert und steht am Beginn ihrer Einführung. Bisher wurden Schwerpunkte bei der Entwicklung der technischen Möglichkeiten selbst gesetzt dabei wurde jedoch kaum auf die Verträglichkeit der Technologie und die soziale Akzeptanz geachtet.

Gerade dabei jedoch existieren Probleme, die ein Risiko für die Technologie selbst und die sie einsetzenden Unternehmen, die RFID-Anwender, darstellen. Wir versuchen, über die kausale Wirkungskette einen Überblick über Risiken beim Einsatz der RFID-Technologie zu geben. Vollständigkeit jedoch können und wollen wir beim derzeitigen Forschungsstand nicht garantieren.

Wir verwenden in dieser Arbeit durchgehend den Begriff *Risiko* nach der Definition von Ulrich Beck [1].

2 Grundlagen und Risikoebenen

Risiken bestehen auf mehreren Ebenen. Sie begründen sich und folgen direkt oder indirekt aus der derzeitigen RFID-Technologie selbst und deren Einsatz (siehe Abb. 1). An von den Risiken Betroffenen sind zu nennen:

- **einzelne Bürger**

  Bürger, die als Kunden oder Nutzer mit RFIDs ausgestattete Produkte kaufen bzw. nutzen und bei sich tragen

- **alle Bürger und die Gesellschaft als Ganzes**

- **der RFID-Anwender und die Regierung**

  Personen, Firmen und Institutionen sowie Regierungen, die RFID-Technologie einsetzen

- **Hersteller und Entwickler der RFID-Technologie**

Darüber hinaus gibt es ein Risiko für die Einführung der Technologie als Ganzes.

Am weitesten publiziert sind Probleme, die einzelne Bürger unmittelbar betreffen. Entwickler der RFID-Technologie vom AutoID-Center des MIT schreiben dazu in einer Akzeptanzstudie [2], dass sie zwar viele Vorteile für eine RFID-Anwendung in der Logistik sehen, jedoch die Bürger als Kunden oder Nutzer von mit RFID-Tags ausgestatteten Produkte nur negative Auswirkungen zu spüren bekämen. Diese Studie stellt ein Waagenmodell, vor bei dem ein Kunde für sich positive und negative Auswirkungen miteinander abwägt und sich daraus seine Ansicht bildet. Bei anderen Technologien wie beispielsweise Mobilfunk gibt es sowohl für Bürger positive (Erreichbarkeit, Bequemlichkeit) als auch negative (Überwachbarkeit, Verfolgbarkeit) Auswirkungen, die die Technologie ausgewogen erscheinen lassen. Bei RFID-Technologie sieht die Studie jedoch keine Ausgleichsmöglichkeit durch für den Bürger positive Eigenschaften. Die Sicht des Bürgers kann, sobald er von einer für ihn negativen Eigenschaft erfährt, nur weiter ins Negative abrutschen, jedoch keinen Ausgleich finden.

Eine derartige Sicht wirkt sich auch auf den RFID-Anwender aus — spätestens, wenn seine Kunden verunsichert sind und sich lieber ein Geschäft suchen, welches keine RFID-Technologie einsetzt. Fühlen sich viele Bürger betroffen, wirken sich die Einzelmeinungen in der allgemienen sozialen Akzeptanz der Technologie aus.

Derzeit werden von verschiedenen Bürgerrechtsorganisationen Risiken für den einzelnen Bürger formuliert und publiziert. Mit verschiedenen dieser Risiken beschäftigen wir uns in Kapitel 4.1. die darauf folgenden Kapitel widmen sich den direkten und indirekten Auswirkungen dieser Risiken und der Risiken aus dem RFID-Einsatz selbst auf RFID-Anwender, Regierung und Gesellschaft sowie auf die RFID-Hersteller und -Entwickler. (4.2, 4.3, 4.4, 4.5). Zuvor aber stellen wir vor, wodurch sich beim Einsatz von RFID-Technologie Risiken von neuer Qualität ergeben.

3 Risiken von neuer Qualität

RFID-Tags ähneln den derzeit verwendeten Barcodes, weisen aber einige Eigenschaften auf, die für eine Risikobeurteilung dieser Technik zentral sind. Beispiele der Eigenschaften und sich daraus ergebende Chancen:

- Hatten bisherige Barcodes einen Adressraum, der es im wesentlichen nur ermöglichte, Art der Ware und Warengruppe zu speichern, so erlauben RFID-Tags auch *weltweit gültige* Individual-IDs, die global einen *einzigen* Gegenstand bezeichnen (Container, Ware z.B. Auto oder Elektrorasierer, Scheck-Karte oder Personalausweis).

- Erfolgte des Auslesen von Barcodes im Allgemeinen *mit Zustimmung* der Besitzer, können ungeschützte RFIDs auch unbemerkt gelesen werden.

- Beim bargeldlosen Einkauf können bei Einsatz einer Datenbank-Verknüpfung alle weiteren Auftreten des RFID-Tags mit dem Käufer in Zusammenhang gebracht werden. Wird gleichzeitig mit einem Satz von RFID-Tags auch ein Tag gelesen, das auf einem Ausweis angebracht ist, so können diese ebenfalls individualisiert werden.

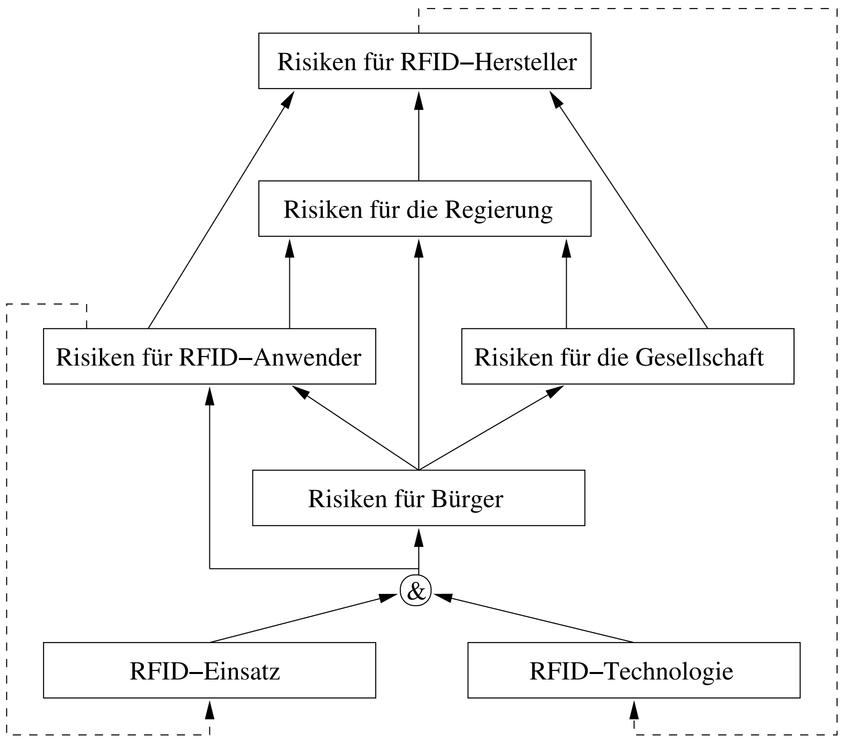

Abbildung 1: Risikofortpflanzung nach Ebenen bei derzeitiger RFID-Technologie

- Die leichte und schnelle Möglichkeit, eine Vielzahl von RFID=Tags lesen zu können, legt den Einsatz von umfassenden, verknüpften Datenbanken nahe, die durch diese Informationsfülle neue Wissensqualität generieren können.

Diese Eigenschaften beschreiben wichtige Chancen der RFID-Technologie und sind ein wesentlicher Grund für deren derzeit priorisierte Entwicklung. Zugleich sind mit diesen Eigenschaften aber auch Risiken verknüpft. Die folgenden vier Beispiele stehen jeweils für eine der oben genannten Chancen und den damit verbundenen Risiken. Weitere Risiken sind erkennbar und werden derzeit bereits von verschiedenen Bürgerrechtsgruppen formuliert.

- Werden von einem Anwender trotz gegenteiliger öffentliche Erwartung RFIDs mit Individual-IDs eingesetzt, kann dies zu Boykott-Aufrufen und erheblichen finanziellen Nachteilen beim Hersteller der Ware führen.

- Die Möglichkeiten des unbemerkten Auslesens von RFID-Informationen (auch durch Mauern) bergen die Gefahr von Industriespionage und Möglichkeiten für Organisationen oder Firmen, Informationen aus der geschützten Privatsphäre des Endverbrauchers zu erhalten.

- Durch die Verknüpfung eines Gegenstandes mit einer Person bestehen Risiken für die gesetzlich geschützte informelle Selbstbestimmung der Individuen. Missachtung von datenschutzrechtlichen Bestimmungen können für die Unternehmen unerwünschte Konsequenzen nach sich ziehen.

- Die einfache Datensammlung und Speicherung in komplexen verknüpften Datenbanken ermöglicht es verschiedenen Institutionen oder Organisationen, ihre Daten abzugleichen oder übergreifende Datenbank-Verknüpfungen zu erzeugen. So gewinnen sie relevante neue Wisseninhalte und damit Wettbewerbsvorteile zum Nachteil andere Organisationen oder des Endverbrauchers.

Auf jedem RFID-Tag in der Logistik wird mindestens eine weltweit einmalige ID gespeichert, die nicht gelöscht oder verändert werden kann. Das internationale Konsortium *EPCglobal* reguliert die Verteilung dieser IDs, so dass die Einmaligkeit sichergestellt ist.

Für einige Anwendungen kann zusätzliche Information gespeichert werden, z. B. eine Kundennummer oder ein Preis, um damit Scannern, die nicht an einer zentralen Datenbank angeschlossen sind, weitere Informationen zu liefern.

In der Regel wird ein Scanner an eine Datenbank angeschlossen sein; in diesem Falle reicht die ID aus, um Verknüpfungen mit weiteren Daten herzustellen.

Die EPC-konforme ID kennzeichnet jedes einzelne Exemplar, und nicht nur einen Produkttyp, so dass bereits mit der ID allein eine eindeutige Identifizierung und Wiedererkennung möglich ist.

Hieraus ergibt sich gegenüber herkömmlicher Technologie eine neue Qualität:

- Die eindeutige Seriennummer (*EPC*) bezeichnet nicht nur jedes Produkt, sondern jedes einzelne Exemplar davon, dessen Weg verfolgt werden kann, solange das Tag lesbar bleibt. Bisherige Produkt-IDs kennzeichnen nur den Produkttyp, aber keine Einzelexemplare.

- Da zur Datenübertragung elektromagnetische Wellen eingesetzt werden, ist, anders als z. B. beim Strichcode, keine direkte Sichtverbindung zum Auslesen notwendig. Bisherige Technologien sehen bei RFID-Technologie keine Möglichkeit vor, das Auslesen eines Tags zu verhindern.

  Jedes Tag in Reichweite eines Scanners übermittelt seine Daten an diesen, unabhängig davon, ob dies erwünscht oder erlaubt ist. Ein Auslesen kann so auch unbemerkt vom Besitzer des Tags und ohne dessen Einwilligung erfolgen. Beim Strichcode kann im Gegensatz dazu das Vorhalten des Etiketts vor den Scanner als Einwilligung zum Lesen gewertet werden.

  Man kann sowohl RFID-Tags als auch die Scanner verstecken und die Tags verdeckt auslesen, was mit herkömmlicher Technologie nicht möglich ist. Ein Schutz vor unbefugtem Auslesen ist nicht oder nur technisch aufwendig möglich.

- Durch die einfache Infrastruktur (kleine, billige Tags, preiswerte Scanner, schnelles Lesen ohne Aufwand) können in zentralen Datenbanken sehr einfach weitaus größere Datenmengen über Kaufverhalten, Bewegungen von Personen, etc. gesammelt werden als bisher.

- Daten, die ursprünglich anonym, d. h. nicht personenbezogen sind, wie die ID auf einem RFID-Tag, werden personenbezogen, wenn in der Datenbank eine Verknüpfung hergestellt wird, die bestimmte Tags mit einer bestimmten Person verknüpft. Bereits beim ersten Kontakt mit dem Gegenstand ist die Verknüpfbarkeit gegeben.

- Durch weltweit verteilte Datenbanken mit einheitlichem zentralen Zugriff, wie z. B. den Object Name Service (*ONS*), können verknüpfte Informationen einfach zur Verfügung gestellt werden.

- RFID-Technologie erleichtert in großem Umfang die Erfassung, Kombinierung und Weiterverarbeitung vielfältiger alltäglicher Daten. Dadurch ermöglicht sie die Erstellung von Bewegungs-, Konsum- und Interessenprofilen.

Aus diesen neuen Qualitäten leiten sich direkt die einzelnen Risiken ab.

4 Risiken im Einzelnen

4.1 Risiken für Bürger

Für Personen, die mit RFID-Tags ausgestattete Gegenstände bei sich führen, ergeben sich unmittelbare Bedrohungen ihrer Privatsphäre und denkbare Szenarien verschieder Verstöße gegen Datenschutzgesetze.

Zweck von Produkten ist es, gekauft und nach Hause getragen zu werden, im Falle von Kleidung tragen Menschen das Produkt auch nach dem Kauf noch längere Zeit bei sich bzw. an sich.

Hierdurch lassen sich die Menschen, die diese Produkte bei oder an sich tragen, auch an anderen Orten identifizieren. Beim Mitführen mehrerer Tags ist eine erhöhte Sicherheit bei der Wiedererkennung gewährleistet. Dies stellt eine technikimmanente Bedrohung der Privatspäre und des Datenschutzes dar. Durch verdecktes Auslesen an verschiedenen strategischen Punkten können z. B. Bewegungsprofile erstellt werden.

Das Bundesverfassungsgericht hat in einem Urteil zur Volkszählung 1983 das „Recht auf informationelle Selbstbestimmung“ direkt aus dem Grundgesetz abgeleitet, dieses Recht wird durch Einsatz der RFID-Technik beim derzeitigen Stand der Technik verletzt.

Durch Datenschutzprobleme, Probleme durch Ermöglichen von automatischer, passiver (schweigsamer) Personenverfolgbarkeit und allgemein im Problembereich des Privatsphärenschutzes ergeben sich vielfältige Risiken für einzelne Individuen. Dieser schweigsame Charakter für die normalen menschlichen Sinne führt dazu, dass ein Betroffener nichts tun kann, um beispielsweise herauszufinden, ob er gerade verfolgt wird oder nicht

Risiken existieren also durch die Möglichkeiten:

- Menschen identifizieren
- Menge anwesender Produkte identifizieren
- Einzelprodukte identifizieren
- Langzeitige Strahlungseffekte
  - für Ladenmitarbeiter
  - unvorgesehene Interaktionen mit implantierten medezinische Geräte in Kunden

Risiken für einzelne Bürger sind bereits in einigen Texten publiziert worden. An dieser Stelle verweisen wir daher auf [4, 6] und [8].

4.2 Risiken für die Gesellschaft

Aus den Risiken für jeden einzelnen Bürger folgt direkt die Wirkung der Technologie in der Gesellschaft: die soziale Akzeptanz.

Das größte Hindernis für die soziale Akzeptanz stellt die Eigenschaft der RFID-Technologie dar, jedes einzelne mit RFID-Tags ausgestattete Produktexemplar der realen Welt eindeutig bestimmen zu können und diese Zuordnung in der virtuellen Welt für Datenverknüpfungen sehr einfach zu gestalten. Während dies in der Logistik einer kleinen Revolution gleichkommt, sind die sozialen Auswirkungen ebenfalls immens, allerdings mit anderem Vorzeichen: Menschen können nun über die mitgeführten Produkte identifiziert und verfolgt werden und es können Konsum-, Interessens-, und Verhaltensprofile angelegt werden ohne das Wissen des Individuums darüber und ohne die Möglichkeit zum Widerspruch.

Regierungen, die RFID-Technologie benutzen, und die Gesellschaft als Ganzes können in Mitleidenschaft gezogen werden durch unüberlegten Einsatz dieser neuen Technologie.

RFID beinhaltet also Risiken für die Gesellschaft selbst. Es ist noch nicht absehbar, wie die Gesellschaft mit den Risiken umgehen wird.

Beispiele für Akzeptanzprobleme sind:

- Machtkonzentration durch Datenfülle in zentralisierten Datenbanken wird ausgeweitet: bestehende Datenbanken werden mit Hilfe von RFID-Technologie mit individuellen Daten gefüttert.
- Bereits das Vermuten von Überwachung führt zu Verhaltensänderung [9]
- Es kann ein de-facto Zwang zur Nutzung von RFID-Technologie entstehen, wenn die Nichtnutzung greifbare Nachteile hat
- Weitgehende Automatisierung von Verwaltungsprozessen ohne menschliche Kontrolle
- Weitgehendes Verlassen auf die Technik
- Weitere Strahlungsbelastung durch RFID-Scanner

4.3 Risiken für RFID-Anwender

Wenn es nicht gelingt, die Risiken bereits vor Einführung der RFID-Technologie zu identifizieren und beherrschbar zu machen, droht eine unzureichende öffentliche Akzeptanz. Tritt aber ein geschlossener Widerstand gegen eine Technologie auf, so kann deren Einführung erheblich verzögert oder verhindert werden (vgl. derzeitiger Ausstieg aus der Kernenergie oder die Debatte um eine Stammzellen-Nutzung). Investitionen können verloren gehen oder es wird ein erheblicher nachträglicher Verbesserungsaufwand nötig. Investoren können zur Zielscheibe des öffentlichen Protestes werden und erhebliche Image- oder Finanzschäden erleiden.

Ein Beispiel für Haftungsfragen: Eine Firma mit Sitz in Deutschland setzt RFID-Technologie ein. Sie kooperiert dabei mit einem Datenverarbeitungspartner aus dem Ausland. Jener wird nicht unbedingt das Datenschutzrecht von Deutschland berücksichtigen. Insbesondere können so Personen aus anderen Ländern über Datenbankinferenz an eigentlich geschützte Daten gelangen. Dies ist hier gesetzeswidrig, wird aber ermöglicht über die Kooperation mit den Datenverarbeitungspartner im Ausland. Die deutsche Firma ist jedoch in Deutschland haftungspflichtig.

Aus den Risiken für einzelne Bürger erwächst ein generelles Problem für die Akzeptanz der RFID-Technologie. In der Folge ergeben sich Risiken für die Personen, Firmen und Institutionen, die RFID-Technologie einsetzen.

Ungenügende Akzeptanz aber führt dazu, daß die Technologie sich nicht durchsetzen kann, oder verboten wird. Dieses ist hauptsächlich ein finanzielles Risiko für jeden RFID-Technologie-Anwender, aber auch ein Risiko für das jeweilige Image von Produkt und Unternehmen.

Obwohl die Kunden die primär betroffene Gruppe darstellen, können auf den Einzelhändler, der mit RFID-Tags ausgestattete Ware verkauft oder seinen Kunden Kundenkarten mit RFID-Tag aushändigt, Schadenersatzforderungen seiner Kunden zukommen.

Denkbar sind Klagen der Kunden wegen Verletzung ihrer Rechte; geschäftsschädigend wirkt sich hier bereits der Verdacht eines Rechtsverstoßes aus, durch Androhung einer Klage und Mundpropagande kann das Unternehmen in der Bevölkerung einen schlechten Ruf bekommen.

Das Problem einer Gefährdung durch den Einsatz von RFID-Technologie ist weitgehend unbekannt bzw. unerforscht. Es besteht ein Risiko für Hersteller, Händler, Regierungen, etc., die RFID-Technologie einsetzen wollen. Dieses Risiko ist im jetzigen Zustand nicht abzuschätzen, und teilweise besteht gar kein Bewusstsein um dieses Risiko. Händler haben ein Interesse an Schutz vor den realen Gefahren (insbesondere finanziellen Risiken). Gesetze können ein Unternehmen vor Regressansprüchen schützen, sowohl gegenüber seinen Aktionären als auch gegenüber der Konkurrenz, wenn es datenschutzrechtlich unbedenkliche Verfahren *verlangt*. Eine reine Selbstverpflichtung der Industrie wird nicht ausreichen, wie bereits in der Praxis laufende Beispiele zeigen:

Prominentes, in Deutschland angesiedeltes Beispiel ist die Metro AG. Sie mußte nach Bürgerprotesten in Rheinberg [10] ihre zuvor heimlichen Tests von RFID-Chips in Payback-Kundenkarten abbrechen [11, 12] und neben dem weltweiten Imageschaden [13] 10000 Karten umtauschen.

Weitere Beispiele für Akzeptanzprobleme:

- Verbrechen die mittels eines RFID-Tracking verübt werden können. Ein Beispiel hierfür wäre, dass ein Gewalttäter zur Ausübung seiner Neigungen seinem Opfer über die in ihren Schuhen eingebrachten RFID-Tags leicht verfolgen und so ihre Gewohnheiten herausfinden kann. Dies wirft Fragen nicht nur in direkten Bezug zum Täter auf, sondern auch Haftungsfragen für den RFID-Anwender, der nicht für ein Ausschalten dieser Gefahr gesorgt oder nicht ausreichend auf die RFID-Tags hingewiesen hat.
- Kunden meiden das Geschäft, das RFID-Technologie einsetzt, wenn sie RFID als will unerwünscht Technologie ansehen. Dieser Effekt vervielfacht sich durch Mundpropaganda
- Imageschädigung durch Verlust des Vertrauens der Kunden in das Unternehmen
- Versprechen eines „großen“ Unternehmens, dass alles richtig läuft ist für viele Kunden nicht ausreichend, sie vertrauen einem großen Konzern nicht automatisch.
- Schon der Verdacht einer Verletzung der Privatsphäre des Kunden durch das Unternehmen kann schädliche Folgen haben

- Die Supermarktkette Wal-Mart hat Mitte 2003 einen Testlauf fürr den Einsatz von RFID-Technik gestoppt und alle bis dahin installierten RFID-Komponenten wieder entfernt nachdem Verbraucherschützer befürchteten, „die Technik könne missbraucht werden, zum Beispiel um Kunden zu überwachen und von ihnen Bedürfnisprofile zu erstellen.“ [14]
- Die Supermarktkette Tesco hat in ihrer Niederlassung in Cambridge zusammen mit Gillette Rasierklingenverpackungen mit RFID-Tags ausgestattet und die RFID-Tags als Auslösemechanismus für eine Kamera benutzt. [15] Dies und weitere Vorfälle u.a. in Australien [16] hat inzwischen zu weltweiten Proteste und einer Kampagne „Boycott Gillette“ geführt [17]
- Der Kleidungshersteller Benetton hat RFID-Tags direkt in die Kleidung eingewebt und dieses zunächst geheim gehalten. Nach dem Auffinden von RFID-Tags wurde ein Boykottaufruf gestartet. [18]

4.3.1 Haftungskosten

Für einen RFID-Anwender bestehen also Risiken bei Haftungskosten für den Verstoß gegen bestehende zivile Richtlinien, wie dem Datenschutz. Zu schützende Informationen von nichtgeschützten Datenquellen können durchaus für Verbrechen genutzt werden, die so über RFID *mitverursacht* und vielleicht sogar erst ermöglicht werden. Die Frage, wie in einem solchen Fall die Haftungspflicht genau ausfällt, ist noch ungeklärt.

Haftungsrisiken bestehen auch durch die mögliche Mitverursachung oder Ermöglichung von Gewaltakten. Über ein bekanntes, mitgeführtes RFID-Tag kann eine entsprechende Vorrichtung automatisch als Auslöser beispielsweise für einen Terroranschlag dienen.[8] Nicht unbedingt weniger dramatisch für die betroffene Person wäre es, wenn ein Gewalttäter eine Person über die mitgeführten RFID-Tags verfolgen und dann seine Neigungen ausleben kann.

4.3.2 Industriespionage

Für einen RFID-Anwender aus der Industrie besteht neben dem Haftungsrisiko auch ein Risiko durch mögliche Industriespionage. Dies existiert beispielsweise dadurch, dass sein Warenbestand von Konkurrenten ebenfalls sehr leicht mit mobilen Lesegeräten erfaßt werden kann. Bringt ein Anwender gar weitere Daten auf einem RFID-Tag unter und werden die RFID-Tags nicht sicher deaktiviert, so kann ein Konkurrent auch durch die von gemeinsamen Kunden von Anwender und Konkurrent in dessen Lesebereich mitgeführte RFID-Tags an wichtige oder aufschlußreiche Daten des RFID-Anwenders gelangen. Weitere Szenarien sind denkbar.

4.3.3 Verwendbarkeitsreduktion

Nicht nur Haftungsfragen und Fragen der Industriespionage werden aufgeworfen, auch der RFID-Einsatz selbst kann vielleicht nicht so sicher erfolgen, wie sich ein RFID-Anwender dies vorstellt. Durch die Befürchtungen in der Bevölkerung genährt sind inzwischen mögliche RFID-Störsender in die Schlagzeilen geraten, voran die von RSA Security propagierten Blockertags [19, 20]. Auch wenn diese nicht das Potential zum vollständigen Datenschutz der Bürger mit sich bringt kann es durch die Verwendung derartiger Gegenmaßnahmen dazu kommen, dass sich die Verwendbarkeit der RFID-Technologie für den RFID-Anwender rediziert, hier beispielsweise insofern, dass nicht sichergestellt werden kann, dass seine RFID-Tags immer gelesen werden können.

4.4 Risiken für die Regierung

Auch für Regierungen als mögliche RFID-Anwender bestehen Risiken:

Rückhalt und Unterstützung in der Bevölkerung geht durch verschiedene Maßnahmen verloren, es kommt zu Protesten [21]:

- Die Regierungen verschiedener Länder, mit den USA in der Vorreiterrolle, sind auf dem Wege, biometrische Merkmale in Pässen und Ausweisen einzuführen. Das Auslesen soll mit Hilfe der RFID-Technologie erfolgen. Dabei werden die Daten ungesichert gespeichert und jedem RFID-Lesegerät preisgegeben [22].

- Durch Maßnahmen wie das Erhöhen der Fälschungssicherheit von Ausweisdokumenten mit RFID-Chips wird nicht die Sicherheit vor beispielsweise terroristischen Anschlägen erhöht, obwohl dies in den Medien oft vermischt wird. Alle bekannten Attentäter vom WTC-Anschlag waren mit legalen, nicht gefälschten Dokumenten unterwegs. Ein Vertrauen auf erhöhte Sicherheit durch derartige Maßnahmen kann sich als fataler Irrtum herausstellen. Diese Diskrepanz der Regierungsmaßnahmen schädigt zudem ihren Ruf.
- durch RFID können sehr viele individuelle Daten erhoben und leicht verarbeitet werden. Die erhobenen Daten lassen sich für eine Rasterfahndung verwenden. Rasterfahndung gilt als unwirksam, sie ist diskriminierend und verdächtigt unbescholtene Bürger nur aufgrund bestimmter Musterkombinationen.[23] Polizei und Verwaltung werden so zunehmend als reine Überwacher angesehen [24].

4.5 Risiken für RFID-Hersteller und -Entwickler

Mittelbar können sich auch Risiken für die Hersteller und Entwickler von RFID-Technologie ergeben:

- Es besteht das Risiko des Nichtdurchseztens der Technologie aufgrund vorgenannter Probleme
- bestehende RFID-Anwender können sich aus den derzeit laufenden Feldtests zurückziehen
- potentielle RFID-Anwender schrecken vor dem Einsatz von RFID zurück
- dadurch gehen die Investitionen der RFID-Hersteller und -Entwickler verloren

Beispiele für das Scheitern von neuen Technologieanwendungen aufgrund der fehlenden gesellschaftlichen Akzeptanz gibt es bereits auf anderen Gebieten, wie z.B. dem der Kernenergie.

Grundsätzlich wirken sich also alle Risiken für RFID-Anwender, Regierung und Gesellschaft auch auf die RFID-Hersteller und -Entwickler aus. Sie sind abhängig davon und haben viel Geld investiert dafür, dass die RFID-Technologie tatsächlich angewendet wird. Bei den Entwicklern ergibt sich diese Notwendigkeit aus den Gebühren zur Nutzung ihrer Patente, für die Hersteller direkt aus der Notwendigkeit, RFID-Tags und -Scanner verkaufen zu wollen.

Ein jedes Risiko, das den Einsatz der Technologie gefährdet, ist somit gleichzeitig ein Risiko für Hersteller und Entwickler. Nichtgefährdende, aber in ihrer Wirkung den Einsatz behindernde Risiken wirken sich auf Hersteller und Entwickler ebenfalls behindernd aus. Übrige Risiken sind für eine Risikobetrachtung für RFID-Hersteller und -Entwickler hingegen nicht interessant.

5 Lösungsansätze

Mögliche Lösungsmöglichkeiten sind folgende:

1. **Nichteinsetzen der Technik**

   Obwohl dies die Probleme lösen würde, kann es zum derzeitigen Zeitpunkt nicht ernsthaft in Betracht gezogen werden, da viele Unternehmen die Technik entwickelt haben und sie viel Energie darauf verwenden werden, sie zum Einsatz zu bringen. Jedoch besteht diese Möglichkeit und es muß mit ihr gerechnet werden: Prominentes Beispiel ist die Kernenergie deren Einsatz nach dem Willen der Gesellschaft mangels Akzeptanz nun nach einer Übergangszeit in Deutschland generell verboten wird.

2. **Keine Menschen betroffen**

   In Bereichen, in denen sichergestellt ist, dass keine Menschen in direkten Kontakt mit funktionsfähigen RFID-Tags kommen, kann die Technik in ihrer derzeitigen Entwicklungsform voraussichtlich ohne derzeit erkennbare Probleme eingesetzt werden. Dies könnte beispielsweise beim automatischen Gepackmanagement im internationalen Luftverkehr sein, wenn die RFID-Tags nach Erreichen des Zielflughafens sicher vom Gepäck entfernt werden. Eine weiterreichende Verwendung und besonders die weiterhin bestehende Auslesbarkeit der RFID-Tags hingegen kann unter Securitybetrachtungen nicht ohne weitere Einschränkungen erfolgen.

3. **trivialer legislativer Ansatz, Rechtssicherheit**

   RFID-Technologie gesetztlich vom Datenschutz und vom Schutz der Privatsphäre auszunehmen ist nicht möglich, da solche Gesetze mit bestehenden Gesetzen und dem Grundgesetz kollidieren würden. Juristisch gibt es derzeit keine Lösung und es ist auch keine Lösung abzusehen.

   Wie so oft bei der Einführung einer neuen Technologie herrscht auch bei RFID Rechtsunsicherheit darüber, inwieweit sie verantwortlich gemacht werden können für Eingriffe in die Privatsphäre ihrer Kunden. Eine solche Situation muß von Unternehmen besonders vor- und umsichtig behandelt werden.

4. **Kombination aus technischer Lösung und Gesetzen**

   Der einzig praktikable und gangbare Weg scheint zu sein. technische Lösungen vorzusehen, die die Privatsphäre aller Bürger schützt, und dies leistet, ohne Nachteile für den Bürger mit sich zu bringen und ohne von diesem zusätzliche Anstrengungen zu verlangen.

   Es gibt verschiedene Ansätze, den Schutz der Privatsphäre zu verbessern, sogenannte *Privacy Enhancing Technologies*. Eine Untersuchung unserer Arbeitsgruppe [8] hat gezeigt, dass zwar einige der Ansätze recht weit gehen, aber alle einige Fragen unbeantwortet lassen.

5. **Problembewusstsein schaffen**

   Es gilt sich mit dem Problembewußtsein für die mit RFID-Technologie verbundenen Risiken auseinanderzusetzen, sowohl mit der Wahrnehmung in der Bevölkerung als auch bei der Risikoabschätzung der Unternehmen, die RFID-Technologie herstellen und einsetzen wollen. Gerade für letztere ist das Risiko vorhanden, aber anscheinend ist es vielen nicht bewusst, und es ist auch vom Umfang her noch gar nicht abschätzbar.

6. **Folgekostenabschätzung**

   Es muss klar sein, welche Folgekosten sich aus eventuellen Rechtsstreitigkeiten durch Datenschutzverletzungen für Anwender von RFID-Technologie ergeben könnten, aber auch, welche zusätzlichen Kosten entstehen, wenn RFID-Technik so erweitert wird, dass unerwünschte Eingriffe in die Privatsphäre durch technische und legislative Maßnahmen unmöglich gemacht werden.

6 Schlußfolgerungen

Es gibt Lösungsansätze, die versuchen, die Grundrisiken bei den Bürgern gering zu halten und dadurch die Folgerisiken ebenfalls auszuschalten. Wie wir in [8] gezeigt haben, sind diese Ansätze jedoch noch nicht ausgereift.

Nicht nur in der Zwischenzeit bis derartige Ansätze um- und eingesetzt werden, sondern auch zur Berwertung jener Ansätze ist es aber unausweichlich, dass die Risiken für alle Parteien identifiziert, benannt und analysiert werden. Eine umfassende Risikoanalyse im Bereich der RFID-Anwendung wurde bislang jedoch noch nicht durchgeführt. Dies aber stellt nun den nächsten notwendigen Schritt für die RFID-Technologie dar.

Literatur

[1] Beck, Ulrich: *Risikogesellschaft. Auf dem Weg in eine andere Moderne.*, Suhrkamp Verlag, Frankfurt a.M., 1986, ISBN 3-518-13326-8

[2] Helen Duce: *Executive Briefing – Public Policy: Understanding Public Opinion*, AutoID-Centre Cambridge, 1. Februar 2003, `http://cryptome.org/rfid/cam-autoid-eb002.pdf`

[3] Dr. Finking im Auftrag des Bundesministeriums für Bildung und Forschung: *Bekanntmachung von Förderrichtlinien des Bundesministeriums für Bildung und Forschung zum Rahmenprogramm Mikrosysteme (2004-2009). Thematischer Schwerpunkt „Mikrosystemtechnik für Smart-Label-Anwendungen in der Logistik (MST-Smart-Label)"*, 22.09.2004, `http://www.bmbf.de/foerderungen/3109.php`

[4] Jan E. Hennig: *Preserving Privacy in RFID Deployment*, 23. März 2004, `http://www.rvs.uni-bielefeld.de/cms/publications/RVS-Occ-04-01`

[5] EU Directorate D – Communication Networks, Security & Software, Applications – ICT for Business: *Wide consultation on wireless tags research needs and workshop*, 20. April 2004,
http://www.cordis.lu/ist/directorate_d/ebusiness/workshop.htm

[6] RVS-Gruppe, Universität Bielefeld: *Statement on Digital Wireless Technologies Prepared for the EU 6th Framework Consultation*, 8. April 2004,
http://www.rvs.uni-bielefeld.de/cms/publications/specialreports/statement-digital-wireless

[7] European Telecommunications Standards Institute (ETSI): *RFID and Telecommunication Services Workshop*, 25. Mai 2004, http://portal.etsi.org/docbox/ERM/open/RFIDWorkshop

[8] Jan E. Hennig, Peter B. Ladkin, Bernd Sieker: *Privacy Enhancing Technology Concepts for RFID Technology Scrutinised*, 28. Oktober 2004,
http://www.rvs.uni-bielefeld.de/cms/publications/RVS-RR-04-02

[9] Dr. Benda, Dr. Simon, Dr.Hesse, Dr. Katzenstein, Dr. Niemeyer, Dr. Heußner, Niedermaier, Dr. Henschel: *„BVerfGE 65, 1 - Volkszählung: Urteil des Ersten Senats vom 15. Dezember 1983 auf die mündliche Verhandlung vom 18. und 19. Oktober 1983 - 1 BvR 209, 269, 362, 420, 440, 484/83 in den Verfahren über die Verfassungsbeschwerden“*, http://www.datenschutz-berlin.de/gesetze/sonstige/volksz.htm

[10] FoeBuD e.V.: *Demo in Rheinberg 28.2.2004*,
http://www.foebud.org/rfid/photo_album/rheinberg/photoalbum_view

[11] Metro AG: *Positionspapier: Thema: Einsatz von RFID im Future Store in Rheinberg – RFID in Kundenkarten: Test beendet*, 28. Februar 2004,
http://www.future-store.org/servlet/PB/menu/1002376_l1/index.html

[12] Christian Klaß: *FoeBud: Metro verzichtet auf RFID-Chip in Kundenkarte*, 27. Februar 2004,
http://www.golem.de/0402/29985.html

[13] CASPIAN: *The METRO „Future Store“ Special Report – Backlash: German Consumers Demand an End to RFID Experiments!*, 2004,
http://www.spychips.com/metro/protest.html

[14] Andreas Wilkens: *Wal-Mart stoppt RFID-Versuch*, Heise Newsticker, 9. Juli 2003,
http://www.heise.de/newsticker/meldung/38420

[15] Oliver Lau: *Tesco überwacht Kunden per RFID*, Heise Newsticker, 22. Juli 2003,
http://www.heise.de/newsticker/meldung/38783

[16] CASPIAN: *RFID Tags Confirmed in Australian Mach3 Razor Packages – Angry Aussies may be next to protest spy chips*, 22. Dezember 2003, http://www.spychips.com/RFID_Australia.htm

[17] CASPIAN Project Boycott Gillette: *GILLETTe's spy shelf photographs CUSTOMERS!!*, July 2003,
http://www.boycottgillette.com/spychips.html

[18] CASPIAN Project Boycott Benneton: *Send Benneton a message: Don't buy clothing with tracking devices!*, ohne Datumsangabe, http://boycottbenetton.org/

[19] Jan E. Hennig: *Was sind RFID Blocker-Tags? Sollte ich mir sowas besorgen?*, 27. März 2004,
http://www.foebud.org/rfid/blockertags/de

[20] Britta Oertel, Michaela Wölk, Lorenz Hilty, Andreas Köhler: *Risiken und Chancen des Einsatzes von RFID-Systemen*, Bundesamt für Sicherheit in der Informationstechnik, ISBN 3-922746-56-X

[21] Lukas Gundermann: *Bürgerrechtsorganisationen legen Positionspapier zu RFID vor*, 20. November 2003,
http://www.datenschutz.de/news/detail/?nid=1087

[22] Karsten Violka: *Bürgerrechtler: RFID-Reisepässe für US-Bürger ohne Datenschutz*, Heise Newsticker, 27. November 2004, http://www.heise.de/newsticker/meldung/53709

[23] *Ombudsmann kritisiert 607 Überprüfungen im Haus / „Angst, Rückzug und Schweigen“*, 13.11.2001, ohne Nennung eines Autors,
http://www.islam.de/?site=articles&archive=folgen-fuer-muslime&article_number=671

[24] Der Spiegel online: *Big Brother Award 2003*, 24. Oktober 2003,
http://www.spiegel.de/netzwelt/politik/0,1518,271027,00.html

[25] Claudia Fischer: *Die BigBrotherAwards 2003 – Kategorie Verbraucherschutz*, BigBrotherAwards.de,
http://www.bigbrotherawards.de/2003/.cop/

[26] Richard Sietmann: *Mehr Fragen als Antworten – RFID-Studie des Bundesamtes für Sicherheit in der Informationstechnik – Die BSI-Studie zu den Risiken und Nebenwirkungen der RFID-Technologie bleibt hinter dem Stand der öffentlichen Diskussion zurück*, c't Magazin für Computer und Technik Ausgabe 25/2004 Seite 48ff., ISSN 0724-8679

[27] Verein zur Förderung des bewegten und unbewegten Datenverkehrs (FoeBuD) e.V. *Homepage*, gegründet 1987, `http://www.foebud.org`

[28] FoeBuD. e.V.: *Aktuell – 17. November: BSI äußert sich zu RFID*, `http://stoprfid.foebud.org/htm/aktuell.html`

[29] Dirk Henrici, Paul Müller: *Hash-based Enhancement of Location Privacy for Radio-Frequency Identification Devices using Varying Identifiers*, Januar 2004, `http://www.icsy.de/~archiv/DPArchiv.0080.pdf`

[30] Dirk Henrici, Paul Müller: *Tackling Security and Privacy Issues in Radio Frequency Identification Devices*, April 2004, `http://www.icsy.de/~archiv/DPArchiv.0086.pdf`

[31] Dirk Henrici, Jochen Müller, Paul Müller: *Sicherheit und Privatsphäre in RFID-Systemen*, Juni 2004, `http://www.icsy.de/~archiv/DPArchiv.0096.ps.gz`

[32] Sarah Spiekermann, Oliver Berthold: *Maintaining privacy in RFID enabled environments – Proposal for a disable-model*, April 20, 2004, `http://www.vs.inf.ethz.ch/events/sppc04/papers/sppc04_spiekermann.pdf`

[33] Sarah Spiekermann, Uta Jannasch: *RFID Technologie im Einzelhandel der Zukunft: Datenentstehung, Marketing Potentiale und Auswirkungen auf die Privatheit des Kunden*, April 2004, `http://www.wiwi.hu-berlin.de/iwi/internetoekonomie/deutsch/publikationen/index.php`

[34] Sarah Spiekermann: *Zwischenbericht 2004 Projekt InterVal*, August 2004, `http://www.wiwi.hu-berlin.de/iwi/internetoekonomie/deutsch/publikationen/040815_interval_zwischenbericht.pdf`

[35] Stephan J. Engberg, Morten B. Harning, Christian D. Jensen: *Zero-knowledge Device Authentication: Privacy & Security Enhanced RFID preserving Business Value and Consumer Convenience Protocols.*, September 2004, `http://dev.hil.unb.ca/Texts/PST/pdf/engberg.pdf`

[36] Stephan J. Engberg: *A new Approach to RFID Privacy Zero Knowledge Device Authentication*, April 2004, `http://obivision.com/Papers/EU_RFID_Workshop_20040420_obi.pdf`

[37] Stephan J. Engberg: *Privacy through virtual identities in Infrastructure*, November 2002, `http://obivision.com/Papers/Ist_Living_with_Security_20021106.pdf`