

# Datenschutzkonzept und Risikoanalyse

## 1. Chancen und Risiken von RFID-Systemen

RFID steht für Radio Frequency Identification (selten: Radiofrequenz-Identifikation). Diese Technologie ermöglicht es, Daten mittels Radiowellen berührungslos und ohne Sichtkontakt zu übertragen.<sup>1</sup> Eine RFID-Systeminfrastruktur umfasst einen Transponder, ein Sende-Empfangs-Gerät sowie ein im Hintergrund wirkendes IT-System. Herzstück der Technologie ist ein Transponder – ein winziger Computerchip mit Antenne. Er ist in ein Trägerobjekt integriert, beispielsweise in ein Klebeetikett oder eine Plastikkarte. Auf dem Chip ist in der Regel ein Nummerncode gespeichert. Dieser enthält Informationen, die in einer Datenbank hinterlegt sind. Dadurch erhält jeder Gegenstand mit RFID-Transponder eine unverwechselbare, weltweit eindeutige Identität.

Die Anwendungsszenarien von RFID-Systemen sind vielfältig und reichen von der Unterstützung im Bereich Logistik bis hin zur bargeldlosen Zahlungsmethode in Szene-Bars. Transponder gibt es in verschiedenen Ausführungen. Da sind zum einen die passiven Aufkleber, die nicht über eine eigene Stromversorgung verfügen und ihre Energie vom Lesegerät beziehen. Wird das Lesegerät in die Nähe eines Transponders geführt, wird ein Strom induziert, der es dem Chip ermöglicht, seine weltweit eindeutige Seriennummer per Funk mitzuteilen. Solche Transponder finden sich in Bibliotheksbüchern, auf Parfümverpackungen und generell auf Produkten, die eine gewisse Preisgrenze überschritten haben und automatisiert verpackt, verschifft oder katalogisiert werden.

RFID-Transponder müssen aber nicht zwangsläufig auf der Oberfläche angebracht werden. Das kontaktlose Auslesen auf Distanz erlaubt es, RFID-Tags auch im Inneren von Objekten – aber auch von Lebewesen – einzusetzen. Implantierbare Glaszylinder werden eingesetzt, wenn Haus- oder Nutztiere markiert werden sollen oder Stranddiscothèque-Besucher in Badehose ihren Cocktail bezahlen wollen. In Spanien konnten sich Freiwillige zu diesem Zweck einen solchen reiskorngroßen Glaszylinder in das Gewebe oberhalb des Trizeps einsetzen lassen.<sup>2</sup> An der Bar des »Baja Beach Club« in Barcelona erlauben entsprechenden Lesegeräte und ein im Hintergrund arbeitendes IT-System, auf dem die Kundendaten gespeichert sind, das bargeldlose Bezahlen per »Handauflegen«.

Ein anderes Chancen- und Risikofeld der RFID-Technik betrifft das Thema Umwelt, sowohl im Sinne des Umweltschutzes als auch im Sinne von Umweltbeobachtung. RFID-Technik wird in Österreich zur Zeit für das Umweltmonitoring eingesetzt: die Bäume der Stadt Wien sind mit einem Transponder ausgestattet und erlauben so eine individuelle Pflege.

„Alle Bäume einer Stadt sollten regelmässig auf ihren Zustand von der Wurzel bis zur Krone hin begutachtet werden. In Österreich z. B. ist gem. Önorm L 1122 eine jährliche Kontrolle anzustreben. Daraufhin sind entsprechende Arbeitsaufträge zu erstellen. Baumkennzeichnungen durch Lagepläne sind sehr mühsam und äußerst arbeitsintensiv. Mit der Kennzeichnung durch Transponder bekommen die Bäume eine elektronische Nummer. Diese ID wird jetzt mühelos mit einem Handgerät gelesen und zusammen mit den baumpflegerischen Maßnahmen in einem Tablet-PC dokumentiert. Nach Begutachtung vor Ort können weitere Arbeiten papierlos festgehalten werden, die neben der Pflege des Baumes der Verkehrssicherungspflicht und der Verbesserung des Baumumfeldes dienen. Als weitere Nutzung kann die Bodenanalyse eines jeden Baumes in einem

<sup>1</sup> Eine gute Einführung sowie Vertiefung in das Thema findet sich in Klaus Finkenzeller: RFID-Handbuch. Grundlagen und praktische Anwendungen von Transpondern, kontaktlosen Chipkarten und NFC, Hanser Verlag, München, 2008.

<sup>2</sup> Susanne Donner: Der Chip, der unter die Haut ging, November 2009, <http://www.heise.de/tr/artikel/Der-Chip-der-unter-die-Haut-ging-836048.html>, letzter Abruf am 28. Februar 2010.

Bewässerungssystem gespeichert werden. Das Bewässerungssystem mixt dann einen speziellen ‚Cocktail‘ aus Wasser, Dünger etc. für jeden Baum.“<sup>3</sup>

RFID-Systeme bieten eine bequeme Alternative zur Beobachtung von Umwelteinflüssen auf Mensch, Tier und Pflanze. Aber solche Systeme sind ebenfalls Bestandteil dieser Einflüsse: Giftstoffe in den Transpondern und die immer größere Verbreitung tragen zur Umweltverschmutzung bei. Die Materialien eines RFID-Systems sind unter anderem Kupfer, Silizium, Plastik aber auch Klebstoffe. Also problematische Stoffe, deren Entsorgung umweltschutzrechtlich relevant sind. In einer Studie des Umweltbundesamt von 2009 kommen die Autoren zu dem Schluss:

„Insgesamt entscheidet das Zusammenspiel von RFID-Tags, Verpackung/Objekt und Entsorgungssystem über die Auswirkungen der RFID-Technologie auf das Entsorgungssystem. Es bestehen große Unsicherheiten über die tatsächlichen zukünftigen Auswirkungen der RFID-Technologie auf das Entsorgungssystem. Es konnte gezeigt werden, dass die Bandbreite realistischer Entwicklungen von ‚vernachlässigbar‘ bis hin zu ‚konkreter Bedrohung von Recyclingprozessen und –verfahren‘ reicht. Zusammenfassend ist festzustellen, dass die durch ein hohes Aufkommen von RFID-Tags im Entsorgungssystem zu erwartenden Probleme beherrschbar sind, wenn vorsorgende Maßnahmen ergriffen werden.“<sup>4</sup>

Es wird sich zeigen, ob alternative Materialien oder Mehrwegtransponder entwickelt werden können, wie es die Autoren dieser Studie sich wünschen würden. Der Verzicht auf RFID stellt keine ernsthafte Option dar, da RFID verstärkt für die Authentizität von offiziellen Dokumenten eingesetzt wird. In der Bundesrepublik Deutschland ist jeder nach November 2005 ausgestellte Reisepass mit einem RFID-Chip versehen. Obwohl hinter vorgehaltener Hand jedem bekannt war, dass diese Maßnahme alleine der Wirtschaftsförderung dienen sollte, wurde die erschwerte Fälschbarkeit eines Passes durch den Einsatz von RFID als Begründung angeführt. Auch Hersteller von Luxusmarken setzen verstärkt RFID-Transponder ein, die teilweise sogar in das Produkt eingearbeitet sind.<sup>5</sup>

Bei elektronischen Tickets als einem weiten Anwendungsfeld gibt es demzufolge auch zwei Möglichkeiten, RFID einzusetzen: einerseits als Sicherheitsmerkmal auf einem gedruckten Ticket, andererseits auch als kompletter Papiertickersatz. Bei der Fußballweltmeisterschaft 2006 wurde der Einsatz von RFID als Sicherheitsmerkmal getestet, eine endgültige Auswertung ist offen. Die Akzeptanz bei den Besuchern war jedoch verhalten. Auch die Einschätzung des ehemaligen Datenschutzbeauftragten von Schleswig-Holstein, Helmut Bäumler, lässt tief blicken:

„Welche Person ist im Stadion, das will man fest stellen können. Und so sehr ich Verständnis dafür habe, dass man Fußball-Rowdies rechtzeitig abwehren und erkennen möchte: Hier sieht man ganz genau, wohin diese Technik führt, nämlich zur Überwachung von Menschen. Beim nächsten mal geht's nicht um Fussballspiele, sondern um eine Demonstration gegen Umweltverschmutzung oder was auch immer, das zieht dann Kreise. Das Fußball-Beispiel zeigt, es geht eigentlich im Hintergrund um die Überwachung von Menschen.“<sup>6</sup>

Positiv kann die RFID-Technik aber auch dazu eingesetzt werden, um beispielsweise individuelle Fahrpreise zu ermitteln, so dass man nur die tatsächlich gefahrene Strecke bezahlen muss. Auch kleinere Zahlvorgänge könnten durch den Einsatz eines solchen eTickets vorgenommen werden. Die Octopus-Karte in Hongkong wird von über neun Millionen Personen nicht nur für den Fahrkartenerwerb genutzt, sondern auch für den Einkauf bei Fast-

---

3 EURO I.D. Identifikationssysteme GmbH & Co. KG: Bäume der Stadt Wien, <http://www.euroid.com/unsere-projekte/baeume-der-stadt-wien.html>, letzter Zugriff am 25. Februar 2010.

4 Lorenz Erdmann, Lorenz Hilty: Einfluss von RFID-Tags auf die Abfallentsorgung, Umweltbundesamt, 2009, <http://www.umweltbundesamt.de/uba-info-medien/dateien/3845.htm>, letzter Zugriff am 25. Februar 2010. S. 12ff.

5 RFID im Blick: Luxus-Schmuckhändler setzt auf RFID-Technologie von Motorola, <http://www.marktplatz-ifu-im-blick.de/201001051716/luxus-schmuckhler-setzt-auf-ifu-technologie-von-motorola.html>, 5.1.2010, letzter Zugriff am 25. Februar 2010.

6 Interview mit dem Sender NDR im Jahre 2004, zitiert nach: FoeBuD e. V.: Wo gibt es RFID?, <http://www.foebud.org/ifu/wo-gibt-es-ifu/>, 2.12.2008, letzter Zugriff am 25. Februar 2010.

food-Läden oder in Cafés. Obwohl die Karten nicht personalisiert sind, werden sie aufgrund ihrer Eindeutigkeit auch zur Zutrittskontrolle in bestimmte Gebäude verwendet.

Als Zutrittskontrolle haben sich RFID-SmartCards auch in Deutschland längst durchgesetzt. Sie verfügen über einen integrierten Schaltkreis und können damit Rechenoperationen durchführen, also beispielsweise Prüfsummen berechnen oder verschlüsselte Daten verifizieren. Ein Zutrittsberechtigter kann sich mit der Karte vor dem System authentifizieren. Generell gibt es kognitive, possessive, existentielle und qualitative Methoden der Authentifizierung.<sup>7</sup> Durch Kombination dieser vier Methoden kann eine erhöhte Zutrittskontrolle sichergestellt werden. Der Besitz einer RFID-Karte (possesiv) in Verbindung mit einer PIN (kognitiv) kann in den meisten Fällen eine ausreichende Überprüfung eines Zugangsberechtigten darstellen.

In einem anderen Einsatzszenario könnte man sich abschließend vorstellen, eine Art von medizinischer Krankenakte implantiert stets bei sich zu haben, damit im Notfall wichtige Daten bereitstehen, also damit beispielsweise der Sanitäter vor Ort über Medikamentenunverträglichkeiten des ohnmächtigen Patienten informiert werden kann. Medizinische Notfälle werden gerne als positives Beispiel angeführt, obwohl zahlreiche praktische Probleme, wie beispielsweise eine Standardisierung der Daten oder die Form des Hinweises eines solchen Dokuments, nicht geklärt sind. Die Kehrseite der Medaille eines solchen Notfallausweises ist darüber hinaus sehr dunkel. Es kann technisch bislang nur unzureichend sichergestellt werden, dass allein Berechtigte diese Daten auslesen können. Außerdem bestehen große Vorbehalte gegenüber Implantaten. Und nicht zuletzt gilt es, den Datenschutz zu wahren, zumal wenn es sich um sehr persönliche, intime Daten handelt.

## 2. Allgemeine Datenschutzprobleme mit RFID

Unter Datenschutz (engl. data privacy) versteht man den Schutz von personenbezogenen und personenbeziehenden Daten vor Missbrauch durch Dritte. Das Bundesverfassungsgericht prägte in seinem berühmten Volkszählungsurteil von 1983 den Begriff der informationellen Selbstbestimmung und formulierte daraus ein Grundrecht.<sup>8</sup> Das Bundesdatenschutzgesetz beginnt mit den Worten: »Zweck dieses Gesetzes ist es, den Einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird.« Und dieses Persönlichkeitsrecht leitet sich direkt aus dem zweiten Artikel des Grundgesetzes der Bundesrepublik Deutschland ab. Der Begriff Datensicherheit taucht im Bundesdatenschutzgesetz nur ein einziges Mal in §9 auf und beschreibt die technischen Maßnahmen, die ergriffen werden müssen, damit der Datenschutz gewahrt werden kann. Dabei muss Datensicherheit nicht in jedem Fall dem Datenschutz dienen, denn unter Datensicherheit wird jede Art der vertraulichen, zuverlässigen und integren Aufbewahrung von Daten verstanden; auch jener Daten, die weder personenbezogen noch -beziehbar sind. Datensicherheit betrachtet lediglich Daten, wohingegen der Datenschutz die Person im Blick hat. Die Integrität und der Zugriffsschutz kann durch Verschlüsselung gewährleistet werden.

Es gibt zahlreiche RFID-Systeme, die mit verschlüsselten Daten arbeiten, darunter auch das bekannte MIFARE Classic der Firma NXP Semiconductors (vormals Philips). Die zwischen Transponder und Lesegerät anfallenden Daten werden mit einem proprietären Verschlüsselungsverfahren vor dem unberechtigten Zugriff geschützt. Jedoch sind proprietäre Verfahren in den meisten Fällen unsicher. Ohne die Möglichkeit einer unabhängigen Überprüfung durch sachverständige Dritte kann eine (Abhör-)Sicherheit unmöglich gewährleistet werden. Und so verwundert es auch nicht, dass es Forschern gelungen ist, diese Sicherungsmaßnahme zu knacken. NXP schreibt zu diesem Forschungsbericht auf ihrer Website:

The Radboud University Nijmegen has presented a publication during a conference on October 6th, with information on how the protocol and algorithm were reverse engineered and the description of some practical attacks which can be carried out with limited means. Henryk Plötz and others have also posted documents on the internet containing detailed information which significantly facilitate attacks on cards and infrastructures

---

<sup>7</sup> Kognitiv könnte beispielsweise die Kenntnis eines Passworts sein, possessiv nennt sich das Besitzen eines physischer Schlüssels, existentiell meint den Themenkomplex der Biometrie und eine qualitative Methode ist z. B. die Unterschrift.

<sup>8</sup> BVerfG, Urteil v. 15.12.1983, Az. 1 BvR 209, 269, 362, 420, 440, 484/83.

using MIFARE Classic. NXP is trying to prevent these publications but due to the nature of internet it is to be expected that such an effort does not meet much success.“<sup>9</sup>

Die Firma versucht also nicht, ihre Produkte zu verbessern, sondern lediglich, die Berichterstattung in ihrem Sinne zu manipulieren. Nicht nur aus diesem Vorfall kann generell die Lehre gezogen werden: nicht erhobene Daten sind am besten vor Missbrauch geschützt.

### **3. Datenschutzkonzept für RFID-Installationen in Museen**

Das Recht des Besuchers auf informationelle Selbstbestimmung verlangt, dass die Betreiber eines Systems zur Datenverarbeitung den Besucher darüber informieren, ob und welche Daten von ihm erhoben werden. Im Falle von der Funktechnologie RFID gilt dies in einem sehr starken Maße: diese Technik wird meistens verborgen betrieben, so dass potentiell betroffene Personen keine Kontrolle darüber haben, wann und welche Daten erhoben werden. Die gesamte Technik ist geradezu darauf angelegt, vollständig transparent hinter den Kulissen zu arbeiten. Daran ist per se nichts datenschutzrechtlich Bedenkliches auszusetzen, allerdings sind sich weder Entwickler, noch Betreiber oder gar die Nutzer eines solchen IT-System des gewaltigen Potentials solcher Datenmengen bewusst. Mit Hilfe immer mehr und immer genaueren Daten lassen sich Bedürfnisse einer erfassten Person immer besser auch ohne deren Hilfe feststellen und gegebenenfalls automatisiert befriedigen. Die Beratung beim Stöbern in einer Online-Buchhandlung beispielsweise wird von Softwareprogrammen übernommen („Kunden, die das RFID-Handbuch gekauft haben, kauften auch RFID für Dummies“). Problematisch wird es dann, wenn diese süße Unmündigkeit nicht selbst gewählt, sondern einem ohne Wahlmöglichkeit von Seiten der Technik geradezu aufgedrückt worden ist.

Ein RFID-System besteht bekanntlich aus weit mehr als aus Transpondern und Lesegeräten, es benötigt immer auch ein im Hintergrund arbeitendes IT-System für die Speicherung und Verarbeitung der anfallenden Daten. Die Datenschutzprobleme bestehender IT-Systeme sind bekannt, bestehen aber nach wie vor. Die zahlreichen Datenskandale der jüngsten Zeit zeigen, dass es umfassende Datensicherheit nicht gibt. Daten wecken Begehrlichkeiten, daher sollte die Datensparsamkeit die oberste Maxime bei der Verarbeitung von personenbeziehbaren Daten sein. Allein nicht erfasste Daten sind sichere Daten, könnte man verkürzt sagen. Auf diese, nicht-RFID-spezifischen Datenschutzprobleme wird an dieser Stelle nicht weiter eingegangen.

Mit der Allgegenwärtigkeit der uns umgebenden Technik entsteht eine neue Qualität der Datenerfassung. Egal ob freiwillig in sozialen Netzwerken oder gezwungenermaßen mit der Nutzung von Telekommunikationstechniken: die Menge an personenbezogener und personenbeziehbarer Daten erlaubt einen präzisen Rückschluss auf die Verhaltensweisen der totalüberwachten Personen zu. Die daraus resultierende Angst vor einem Kontrollverlust beim Umgang mit der verborgenen Funktechnik RFID ist daher nur allzu verständlich. Dabei zeigen die Erfahrungen im Projekt »Poseidon«, dass diesen Ängsten durch Offenheit und Aufklärung begegnet werden kann.

Staatliche Museen genießen ein hohes Vertrauen, das ihnen von den Besuchern entgegengebracht wird. Wird den Besuchern am Eingang beispielsweise ein RFID-Chip ausgehändigt können diese – und damit potentiell auch die Besucher – über die fortlaufende Seriennummer identifiziert werden. Das Museum muss daher sicherstellen, dass zu keinem Zeitpunkt, auch und insbesondere nach dem Ausstellungsbesuch, eine Zuordnung von persönlichen Informationen des Besuchers zu den Seriennummern auf dem Chip vorgenommen werden kann. Dies kann technisch oder dialektisch erfolgen. Technisch gibt es zwei Möglichkeiten, einen RFID-Chip zu deaktivieren: physisch und logisch. Physikalische Deaktivierung bedeutet in der Regel die Zerstörung der Antenne oder die Überlastung des Chips durch ein starkes elektromagnetisches Feld. Das Museum könne also beispielsweise einen entsprechenden »Datenschutz-Automaten« am Ende der Ausstellung aufstellen, der für die physische Zerstörung des Transponders sorgt. Er könnte ihn aber auch logisch deaktivieren, etwa durch das Senden eines speziellen Befehls zum Chip, eines sogenannten kill-Befehls. In den RFID-Spezifikationen ist ein solcher Befehl explizit

---

9 NXP Semiconductors: Security of MIFARE Classic, [http://www.mifare.net/security/mifare\\_classic.asp](http://www.mifare.net/security/mifare_classic.asp), letzter Zugriff am 25. Februar 2010.

vorgesehen, allerdings liegt es an den Herstellern der Systeme, ihn auch zu implementieren. Im Rahmen unseres Projektes entschieden wir uns allerdings dafür, den Besucher in den Datenschutzprozess einzubeziehen.

Mit dialektischer Verhinderung des Datenmissbrauchs soll gemeint sein, dass der Besucher über den Einsatz der RFID-Technik umfassend aufgeklärt wird. Dazu gehört einerseits ein Hinweis auf dem Träger des RFID-Chips, nämlich, dass es sich um einen RFID-Chip handelt und andererseits eine Datenschutzerklärung, die sinnvollerweise auf eine Tafel im Eingangsbereich sowie auf einer Webseite stehen kann. Die Erfahrung in der Wechselausstellung »Koscher & Co« des Jüdischen Museums Berlin, in der von Anfang Oktober 2009 bis Ende Februar 2010 mit Hilfe von RFID-Löffeln Rezepte gesammelt werden konnten, zeigte, dass die Methode der Besucheraufklärung für alle Beteiligten die positivsten Resultate erzielte. Im Rahmen der Besucherevaluation wurden ausgewählte Besucher über ihre Einschätzung von Chancen und Risiken der RFID-Technik befragt. Dabei wurde explizit auf deren alltäglichen Einsatz Bezug genommen. In der Bundesrepublik Deutschland besitzen sämtliche Reisepässe, die nach November 2005 ausgestellt worden sind einen RFID-Chip. Die Steuermarke beim Haustier ist längst einem implantierten Glaszylinder gewichen, der ebenfalls über einen solchen Chip verfügt. Die meisten Besucher kamen also mit einem Chip in den Kontakt und in dem meisten Fällen standen sie zwar dem Einsatz der Technik unkritisch gegenüber – allerdings beklagte ein Großteil der Leute den Kontrollverlust über ihre Daten. Ist der technische Ablauf sachverständig und klar erklärt, steigt die Akzeptanz der RFID-Technik bei den Nutzern. Das verwundert nicht, wenn man sich den Aufschrei in Gedächtnis ruft, den die Supermarktgruppe WalMart provozierte, als sie, unangekündigt und vor den Kunden geheim gehalten, alle Produkte mit RFID-Transpondern versahen. Schnell war die Rede von »Schnüffelchips« und dem »gläsernen Kunden«. Die Profilbildung von Personen wird von der Allgemeinheit kritisch gesehen. Dies liegt nicht zuletzt daran, dass moderne Gesellschaften von einer Gleichheit im Sinne einer Chancengleichheit der einzelnen Mitglieder ausgehen. Es wird dabei übersehen, dass diese Gleichheit eine vor dem Gesetz, also gegenüber dem Staat ist und eben nicht eine Gleichheit der Bedürfnisse meint.

Ein kontextsensitives Informationssystem sollte genau auf diese unterschiedlichsten Anforderungen eingehen und jeweils unterschiedlich aufarbeiten. Dabei müssen Chancen und Risiken stets gegeneinander abgewogen werden. Dem Museum ist sich der ihm obliegende Verantwortung gegenüber den Besuchern aber auch gegenüber der Nachwelt bewusst. Die Zeiträume, in denen die Museumsleitung rechnet, sind ungleich höher als in der freien Wirtschaft. Die Funktionsfähigkeit der eingesetzten technischen Systeme muss für mindestens zehn Jahre gewährleistet sein, daher zögern die meisten noch, im großen Stil neue Techniken (wie RFID) einzusetzen, da sich diese so stark weiterentwickeln.

Generell unterscheidet man beim Einsatz von RFID in Museen, wer von dem Einsatz profitieren sollte: der Besucher oder die Museumsleitung. Der mit Zusatzinformationen angereicherte Besuch bedeutet einen Mehrwert für den Besucher, eine Analyse des Besucherstroms und der Zufriedenheit der Besucher ist für die Besucherforschung und somit für die Museumsleitung interessant. Im günstigsten Fall lassen sich beide Interessen zugleich vertreten.

#### **4. Das Szenario in der Wechselausstellung »Koscher & co«**

„Eine Ausstellung bittet zu Tisch! Und der ist im Jüdischen Museum Berlin reich gedeckt: »Koscher & Co. Über Essen und Religion« spannt den Bogen von den uralten Kulturen Mesopotamiens bis in die unmittelbare Gegenwart der jüdischen Küche. Die Kaschrut, das jüdische Speisegesetz, und alles, was mit Essen im Judentum bis zum heutigen Tag zu tun hat, ist Thema der Ausstellung. Zugleich sucht sie den Vergleich mit anderen Weltreligionen, vor allem mit Christentum, Islam und Hinduismus.

Dass Nahrungstabus, die Unterscheidung von »rein« und »unrein«, Opferhandlungen, Tischsitten, Zeremonien, besondere Festtagsspeisen, religiöse Vorstellungen und Rituale das Verhältnis der Menschen zur Nahrung auch dort beeinflussen, wo sie sich dessen gar nicht bewusst sind, zeigt die Ausstellung – und warum das Tafelfreude und Gaumenlust nicht schmälert.

Zu sehen sind antike Marmorstatuetten, prachtvoll illustrierte Handschriften vom Mittelalter bis in die frühe Neuzeit, opulente Stillleben, bei deren Anblick einem buchstäblich das Wasser im Munde zusammenläuft, aber auch Stahl- und Plastikgerätschaften aus der modernen koscheren Küche. Interaktive Medieninstallationen laden schließlich dazu ein, das eigene Wissen zu erproben: an flüsternden Tischen und frommen Küchenherden mit kritischen Kommentaren aus dem Off.<sup>10</sup>

Ein Bestandteil der erwähnten interaktiven Medieninstallationen ist die Installation »à la carte«. Die Wechselausstellung führt den Besucher durch zehn Räume, die einem bestimmten Thema zugeordnet sind. In jedem Raum befindet sich eine »à la carte«-Medienstation, die der Besucher als Teller wahrnimmt.

### Technischer Aufbau der Installation »à la carte«



Der Besucher erhält am Eingang zur Ausstellung einen mit einem RFID-Chip versehenen Löffel aus Kunststoff mit einer kleinen Gebrauchsanweisung, wie er mit dessen Hilfe Rezepte sammeln kann. Die RFID-Chips besitzen über die einprogrammierte ID hinaus einen aufgedruckten und somit für den Besucher

lesbaren »Löffelcode«. In jedem Raum der Wechselausstellung befindet sich Medienstationen, die aus einem Teller bestehen, unter denen sich jeweils ein RFID-Lesegerät befindet, der wiederum an einen kleinen Computer angeschlossen ist. Auf der Unterseite der Teller wurde ein Symbol eingraviert, das sich auf den Raum bezieht und zunächst nicht sichtbar ist. Wird nun der Löffel in die Nähe des Tellers gebracht, typischerweise in den Bereich zwischen 1 cm und 6 cm über der Oberfläche, erkennt das Lesegerät unterhalb des Tellers die Anwesenheit eines Chips und der angeschlossene Computer sendet ein Signal an eine LED, so dass der Teller von unten beleuchtet wird und ein Symbol offenbart. Der Löffelcode wird zusammen mit einem Datumsstempel auf dem Computer gespeichert und über ein internes Netzwerk auf einem zentralen Server gespeichert. Durch das (optische wie akustische) Feedback und den Hinweis auf die Installation, hat der Löffelbesitzer den Eindruck, ein Rezept gesammelt zu haben. Da nicht registriert wird, wie lange sich ein Besucher in der Ausstellung aufhält und demzufolge nicht erfasst wird, wann der Besuch abgeschlossen ist, werden die Daten eines jeden Tages erst nach Ausstellungsende ausgewertet. Die Software führt nun die Daten aller zehn Medienstationen zusammen und kann somit bestimmen, an welchen Stationen in welchen Räumen der Löffel aufgelegt worden ist.

### Kontextbasiertes Auswählen der Rezepte

Wenn es nur um ein schlichtes Rezeptesammeln ginge, würde sich eine technisch weniger aufwändige Lösung anbieten, beispielsweise mit Hilfe von Sammelkarten, die der Besucher in jedem Raum aus einem Spender entnehmen könnte. Das Besondere an dieser Installation ist, dass zu jedem Raum mehrere Rezepte zugeordnet sind und die Software kontextsensitiv entscheidet, welches Rezept der Besucher schließlich erhält. Im konkreten Fall sind es drei Rezepte pro Thema und Raum, die in die Kategorien »5 Sinne«, »5 Zutaten« und »5 Minuten« eingeordnet wurden. Die Zuordnung eines jeden Besuchers zu einem bestimmten Profil wird kontextsensitiv über die Auswertung der besuchten Stationen ermittelt. Das System erfasst darüber hinaus für interne Zwecke den Zeitstempel, zur Profilbildung wird er hingegen nicht benutzt, um dem Besucher nicht das Gefühl zu geben, das Museum würde die Aufenthaltsdauer kontrollieren. Wählt sich der Rezeptsammler am nächsten Tag auf die Website der Ausstellung ein, sieht er sowohl sein Profil, als auch die von ihm gesammelten Rezepte der jeweiligen Kategorie.

Die Wechselausstellung besitzt eine eigene Website und ein Unterpunkt ist der Hinweis auf die Installation »à la carte«. Dort besitzt der Internetnutzer (und früherer Besucher der Ausstellung) die Möglichkeit, seinen »Löffelcode« einzugeben, um die gesammelten Rezepte abzurufen. Es gibt insgesamt 30 Rezepte, jeweils 10 in einer der Kategorien »5 Sinne«, »5 Zutaten« und »5 Minuten«. Der Besucher hat unter Umständen nicht alle Medienstationen benutzt, aus welchen Gründen auch immer, er bekommt demzufolge nur die Rezepte aus den Räumen zu sehen, die er auch tatsächlich gesammelt hat. In diesem personalisierten Bereich der Website wird er

<sup>10</sup> Text der Sonderwebsite zur Wechselausstellung entnommen, <http://www.jmberlin.de/koscher/>, August 2009.

darüber aufgeklärt, aus welcher Kategorie er nun Rezepte lesen und herunterladen kann. Falls ihn die beiden anderen Kategorien oder die von ihm nicht gesammelten Rezepte interessieren, kann der Nutzer mit einer spielerischen Hürde ebenfalls auf die restlichen Rezepte zugreifen: Dazu bewegt er einen auf der Website gezeichneten Löffel auf einen ebensolchen Teller – und schon hat er Zugriff auf alle Rezepte.

Der personalisierte Bereich der Website ist nicht durch ein Passwort geschützt und da der »Löffelcode« lediglich aus einer hexadezimalen Zahl besteht, müssen wir davon ausgehen, dass es Internetnutzer gibt, die zwar nicht in der Ausstellung waren, jedoch den Code erraten und somit Zugriff auf die Rezepte haben. Daher können die zusätzlich auf der Website gesammelten Rezepte und das gewählte Profil nicht dauerhaft gespeichert werden. Bei jedem Einwählen auf der Site werden also zunächst nur die Rezepte angezeigt, die tatsächlich während des Ausstellungsbesuchs gesammelt wurden.

## **5. Fazit**

Abschließend lässt sich feststellen, dass die Akzeptanz des Einsatzes von RFID in Museen im Vergleich zu anderen Szenarien sehr hoch ist. Am Ende der Wechselausstellung »Koscher & co« verzeichnete das Jüdische Museum Berlin über 33.000 eingesetzte RFID-Löffel. Die Besuchercommentare im Gästebuch und auf der Website sowie die Reaktion der in der Evaluation befragten Besucher bestätigen das Vorgehen, die Besucher aktiv über den Einsatz der RFID-Technik aufzuklären. So aufgeklärte Besucher sind in der Lage, unabhängig von ideologischem Ballast über diese pervasive Technik zu urteilen.

Das Projekt Poseidon ist froh, dass das Urteil so positiv ausfiel.