Interview

„Passwortschutz heißt der Königsweg“

Privacy by Design – Mit diesem Ansatz lassen sich Datenschutzprobleme bereits von vornherein ausschließen, sagt Professor Dr. Sarah Spiekermann im Interview mit „RFID im Blick“. Sie plädiert: Privatsphäre sollte technisch gewährleistet werden.

■ *Professor Dr. Spiekermann, Sie plädieren beim Verbraucherschutz für das Prinzip „Privacy by Design“, warum?*

Aus meiner Sicht sollte man nicht nur über den Datenschutz diskutieren, sondern über den Erhalt von Privatsphäre insgesamt. Und dieser kann technisch zu einem hohen Grad gewährleistet werden, indem Systeme von vornherein so konzipiert werden, dass sie dem Menschen mehr Kontrolle geben und nur dort Daten verarbeiten und speichern, wo dies zur Erfüllung der primären Geschäftszwecke erforderlich ist. Wenn sich Betreiber und Hersteller von RFID-Systemen bereits in einem frühen Stadium über datenschutzgerechte Systeme Gedanken machen, haben wir die besten Voraussetzungen, eine langfristig verbraucherfreundlichere technische Umgebung zu schaffen. Zum Vergleich: Warum hat Apple keine Probleme mit Virenangriffen? Weil das System von vornherein anders ausgelegt wurde!

■ *Welche konkreten Maßnahmen können den technischen Datenschutz unterstützen?*

Tag-Entwickler und Standardisierungsinstitutionen wie GS1 sollten endlich anfangen, ernsthaft darüber nachzudenken, wie eine Deaktivierung von passiven RFID-Chips kosteneffizient und prozesstechnisch sinnvoll umgesetzt werden kann. Der zweite Punkt ist die Frage nach dem Umfang der Datenspeicherung. Allein durch den Verzicht auf sekundengenaue Reader-Timestamps können viele gefürchteten Trackingszenarien bereits vereitelt werden. Drittens kann sich der Handel dazu verpflichten, keine fremden Tags zu verarbeiten und zu speichern; was im PIA Framework übrigens festgehalten worden ist. Überhaupt sind im Anhang des PIA-Frameworks über 20 Maßnahmen aufgelistet, an denen sich RFID-Operator orientieren können, um den Verbraucherschutz ihrer Anlagen zu optimieren. Neben technischen Gestaltungsmöglichkeiten sind hier auch Governance-Maßnahmen beschrieben, wie Managementprozesse oder die Kundeninformation mittels Logo. Schließlich gibt es viele kreative Möglichkeiten, ein Produkt so zu gestalten, dass sich das Datenschutzproblem von selbst löst. Zum Beispiel Tags, die in ein separates Etikett eingearbeitet sind, welches der Kunde einfach abreißt. Oder Tags in einer Schuhsohle, deren Antennen beim Laufen abbrechen.

„Man sollte nicht über Datenschutz diskutieren, sondern über den Erhalt von Privatsphäre.“

Univ.-Professor Dr. Sarah Spiekermann ist seit 2009 Vorständin des Instituts für BWL & Wirtschaftsinformatik an der Wirtschaftsuniversität Wien. Die habilitierte Wirtschaftsinformatikerin ist Expertin im Bereich E-Marketing und Verbraucherschutz im Ubiquitous Computing.

Professor Dr. Sarah Spiekermann

■ *Warum ist ‚RFID und Privacy‘ ein so sensibles Thema, während das Internet ein teilweise noch rechtlich unregulierter Raum ist?*

Die RFID Technik ist neben Mobilfunk, Videoüberwachung und dem Internet heute eine der vier großen Bereiche, in denen sich unsere gesellschaftlicheVorstellung von Privatsphäre wandelt; in denen sie aber durch wirtschaftliche Interessen auch bedroht ist. RFID hat dabei leider eine besondere Eigenschaft: die Unsichtbarkeit. Dass die Technologie Objekte durch Materialien hindurch unbemerkt aus der Distanz auslesen kann, insbesondere im UHF Bereich auch aus erheblichen Distanzen heraus, ruft bei Menschen ein Gefühl des Kontrollverlustes hervor und weckt so besonders große Ängste. Das Internet oder das Handy lassen sich ausschalten, bei RFID geht dies bisher jedoch nicht. Wir haben herausgefunden, dass über 70% der Verbraucher aus diesem Grund RFID Tags am Ladenausgang am liebsten killen wollen, egal wie schön die Joghurtbecher hinterher mit dem intelligenten Kühlschrank kommunizieren könnten. Aufgrund dieser erheblichen Verbraucherängste steht die EU unter Regulierungsdruck.

■ *Der neue Personalausweis mit RFID-Chip kann zukünftig auch als digitale Identität für Internetgeschäfte eingesetzt werden. Inwieweit liegt die Verantwortung für persönliche Daten auch bei dem Verbraucher?*

Beim Personalausweis kommt das Auslesen der Tags aus der Distanz nicht Maße zum Tragen, da der Verbraucher selbst die Kontrolle hat. Er legt den Personalausweis selbst auf den Reader. Bei passiven Tags im UHF-Bereich – und um diese geht es oft wenn über Privatsphäre diskutiert wird – hat der Verbraucher diese Kontrolle hingegen nicht, es sei denn man setzt ein Passwortverfahren ein. Dies ist aus meiner Sicht daher auch langfristig der Königsweg; selbst wenn ich zugestehe, dass dabei das Passwortmanagement ein ungelöstes Problem ist. Die Bemühungen und Investitionen zur Verbesserung der Technik sollten jedoch auf jeden Fall dahin gehen, dass die Tags am Kassenausgang nur „schlafen gelegt“ werden und im Nachhinein wieder durch den Besitzer angeschaltet werden können. Zum Beispiel, um zusätzliche After-Sales-Services wie Garantieabwicklungen etc. zu nutzen.

■ *Also, opt-out wäre Ihrer Ansicht nach kein ausreichendes Verfahren?*

Nein. Um das Szenario zu verhindern, das jeder jeden in der Ladenpassage auslesen kann, sollte „opt-in“ als Standardeinstellung für alle Systeme gelten. Noch sind die Technologien für dieses langfristige Szenario nicht verfügbar, aber die Investitionen sollten klar dahin gehen. Es ist doch ein Unding, dass der GS1-Standard bisher nicht vorsieht, ein Kill-Kommando durch die Supply-Chain bis zur Kasse mitzureichen. Hier müssen sich die entsprechenden Standardisierungsbehörden Gedanken machen.