

■ Als Industrie und Handel Ende 2005 mit dem „Internet der Dinge“ eine Kampagne zur Ablösung des Barcodes durch RFID (Radio-Frequency-Identification) begannen, beobachtete die Europäische Kommission diese Entwicklung mit Sorge. Insbesondere die Möglichkeiten der unbemerkten Auslesung und hiermit einhergehender Profilbildung, ließ die Kommission schließlich tätig werden. Um eine gesetzliche Festlegung abzuwenden, bot

sie der Industrie 2009 an, im Rahmen der Selbstregulierung für einen angemessenen Datenschutz in RFID-Anwendungen Sorge zu tragen. Hierzu sollte ein Verfahren vorgeschlagen und abgestimmt werden, das am 6. April 2011 formell angenommen wurde.

Dieses Verfahren nennt sich im Originaltext „Privacy and Data Protection Impact Assessment Framework for RFID Applications“, übersetzt Rahmenwerk zur

Datenschutz-Folgen-Abschätzung (DSFA) für RFID-Anwendungen. Es ist entwickelt worden, um den Betreiber einer RFID-Anwendung bei der Aufdeckung von Datenschutz-Risiken in seiner Anwendung zu helfen, deren Eintrittswahrscheinlichkeit zu ermitteln und zu dokumentieren, wie diesen Risiken begegnet wird. Art und Umfang der zu treffenden Vorkehrungen können dabei von Anwendung zu Anwendung stark variieren.

Datenschutz-Folgeabschätzung für RFID

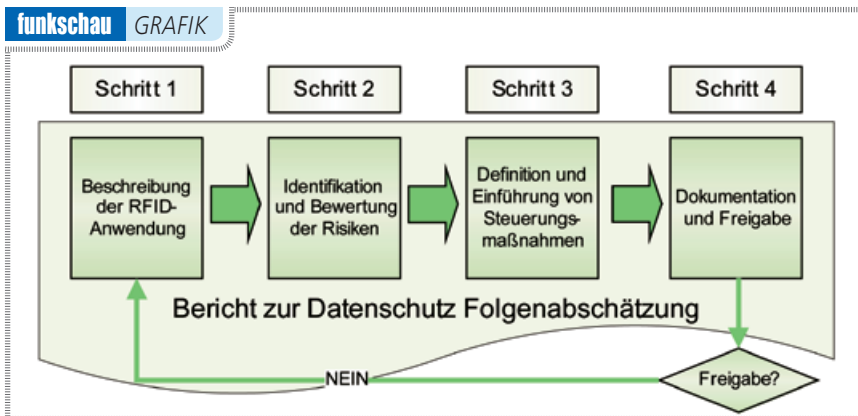
Achtung Terminalsache: Bei RFID geht der Schutz der Privatsphäre künftig als ein Freigabe-Kriterium in jedes Anwendungsprojekt ein. In einer Selbstverpflichtung hat die Wirtschaft gegenüber der EU-Kommission erklärt, künftig für jedes Betriebsprojekt einer RFID-Anwendung eine so genannte Datenschutz-Folgeabschätzung (DSFA) durchzuführen – spätestens ab September dieses Jahres

Im Grunde ist die Datenschutz-Folgeabschätzung mit der in Deutschland heute schon für bestimmte, sensible Anwendungen vorgeschriebenen Vorabkontrolle vergleichbar. Da es hierfür nur sehr wenige, teils sehr abstrakte Anleitungen gab, wurde sich bei der Festlegung des Verfahrens der DSFA vor allem am Beispiel des vom britischen Datenschutzbeauftragten herausgegebenen PIA-Handbuchs (Private-Impact-Assessments) orientiert.

Spätestens seit September 2011 muss jedes Anwendungsprojekt für RFID vor seiner Inbetriebnahme eine DSFA durchgeführt und deren Ergebnis schriftlich dokumentiert haben. Inzwischen sind



Bild: funkschau Quelle: forolia



Eine Datenschutz-Folgeabschätzung lässt sich in vier Schritte gliedern, die nacheinander abgearbeitet werden können.

neue Stimmen vernehmbar, die sich eine DSFA auch für andere, sensible M2M-Technologien als verpflichtend vorstellen können.

Wen betrifft die Datenschutz-Folgeabschätzung?

Grundsätzlich sollen alle Unternehmen und Behörden, die in Europa eine RFID-Anwendung einzusetzen planen, eine DSFA durchführen, sofern von dieser Anwendung eine relevante Risikoeinstufung für den Datenschutz erreicht wird. Bei nur unerheblichen Risiken kann auf die DSFA verzichtet werden.

Bevor Sie also in die Detailarbeit einsteigen, sollten Sie in einer Ausgangsanalyse feststellen lassen, ob für die von Ihnen geplante Anwendung eine DSFA erforderlich ist, und in welchem Umfang. Hierbei hilft Ihnen ein Entscheidungsbaum. Ergibt die Ausgangsanalyse, dass Sie eine DSFA benötigen, sollten Sie sich als nächstes um die Rahmenbedingungen kümmern.

Die DSFA – idealerweise ein Unterprojekt im Projekt

Das verabschiedete Rahmenwerk stellt einige Anforderungen an die Datenschutz Folgeabschätzung, denen man am besten in einem eigenen Unterprojekt zum Entwicklungs- und Einführungsprojekt der RFID-Anwendung, oder alternativ in einem daneben aufgestellten Projekt gerecht werden kann.

Zunächst ist die DSFA terminlich so anzuordnen, dass ausreichend Zeit bleibt, um notwendige Anpassungen vorzunehmen, und damit der Report spätestens sechs Wochen vor der Betriebsfertigstellung fertig gestellt und abgenommen ist. Wie auch in anderen Projektverfahren

üblich, sollen die Verantwortlichkeiten und Rollen bei der Durchführung und Abnahme der DSFA benannt sein. Auch müssen die Bewertungskriterien, wann die Anwendung als betriebsbereit im Sinne der DSFA anzusehen ist, vorab schriftlich festgelegt werden.

Dabei wird erwartet, dass Stakeholder in die Analyse angemessen einbezogen sind. Innerbetrieblich sollte neben dem

betrieblichen Datenschutzbeauftragten, der schon auf Grund seiner gesetzlichen Aufgaben zu beteiligen ist, auch Projektteilnehmer aus Technologie, Marketing und anderen Disziplinen teilnehmen. Außerbetrieblich kann im Einzelfall die Einbeziehung von Vertretern betroffener Personengruppen wie Betriebsrat oder Kundenbeirat und Verbraucherschutz als erforderlich angesehen werden.

Ablauf und Inhalt einer DSFA

Die DSFA ist ein Verfahren in vier Schritten.

■ **Schritt 1:** Beschreibung der RFID-Anwendung.

In diesem ersten Schritt wird Zweck und Aufbau der RFID-Anwendung dargelegt. Hier soll ein umfassendes Bild der Lösung, ihrer Umgebung und ihrer Systemgrenzen gezeichnet werden. Insbesondere die Datenflüsse sind detailliert zu beschreiben, hierfür werden Flussdiagramme empfohlen. Auch die Datenstrukturen sind zu dokumentieren, damit mögliche Verknüpfungen erkannt werden können. Weiterhin soll die aktuelle Aufgabenstellung, aber

funkschau Expertenkommentar



Frithjof Walk

Vertriebsleiter OBID bei Feig Electronic.

Die Rolle der Partner für RFID und Prozessoptimierung

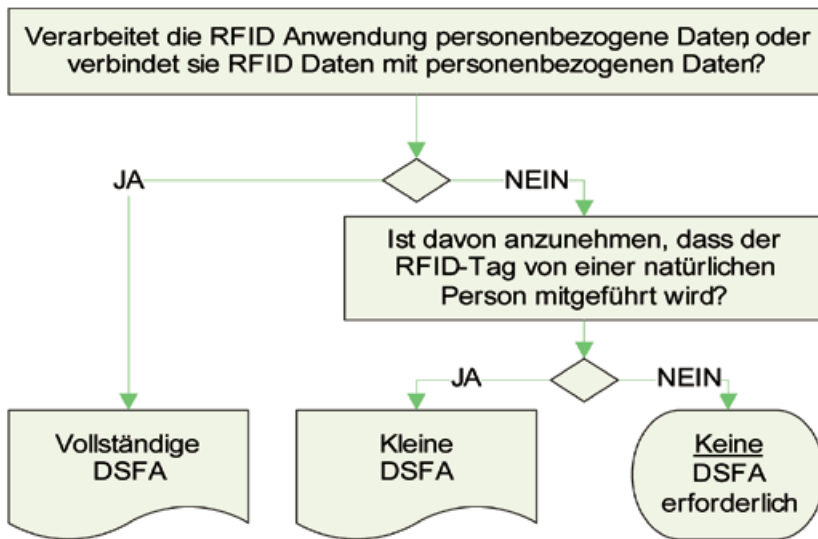
Es grenzt an eine logistische Meisterleistung, was der Wettbewerb heute von Unternehmen in der industriellen Fertigung verlangt: Sie müssen hochflexibel auf äußerst dynamische Marktanforderungen reagieren, gleichzeitig Prozesskosten senken und dabei immer höhere Qualitätsstandards erfüllen. Zudem gewinnt die lückenlose Rückverfolgbarkeit jeder einzelnen Produktcharge in vielen Branchen an Bedeutung. Und das heißt: durchgängige Transparenz in einem Netz komplex verflochtener Lieferketten.

Wie sich diese Transparenz mit RFID erreichen lässt und wie damit zugleich der Material- und Teilefluss nachhaltig optimiert wird, zeigt sich schon heute in der Automobil- und Luftfahrtindustrie. Technologien zur berührungslosen Identifikation per Funkwelle sorgen dort beispielsweise dafür, dass Baugruppen und Komponenten in der richtigen Reihenfolge und Stückzahl an der jeweiligen Anlage bereitstehen.

Doch nicht nur für große Unternehmen können RFID-Investitionen ausgesprochen lohnenswert sein. Denn auch im Mittelstand erzeugt der Wettbewerb einen zunehmenden Druck, aufwändige und kleingliedrige Montageprozesse zu beschleunigen und Fehlerquellen zu eliminieren. Aber auch Themen wie Artikelsicherung und Plagiatsschutz sprechen für den Einsatz von RFID.

Welche Technologie sich im Einzelfall empfiehlt, hängt dabei von den konkreten Produktionsabläufen ebenso ab wie von den jeweiligen Datenschutzerfordernissen und dem bestehenden IT-Umfeld. Unternehmen sind also gut beraten, sich auf einen erfahrenden Systemintegrator als Partner für ihr RFID-Projekt zu verlassen. (MK)

funkschau GRAFIK



Der Entscheidungsbaum hilft bei der Ausgangsanalyse, ob beziehungsweise welche Datenschutz-Folgeabschätzung durchzuführen ist.

Bild: Concept Factory

auch die langfristige Fort-Entwicklung der Anwendung beschrieben werden. Schließlich sollen die Beteiligten an der Informationserfassung und Verarbeitung, sowie die Anwender- und Nutzerkreise benannt werden. Auch Übergänge zu externen Systemen sind konkret darzustellen.

Schritt 2: Identifikation und Bewertung der Datenschutz-Risiken.

In diesem Schritt sollen zunächst die Szenarien festgestellt werden, unter denen personenbezogene Daten im Rahmen der vorgesehenen RFID-Anwendung gefährdet oder kompromittiert werden. Hierzu dient die EU-Datenschutz-Richtlinie beziehungsweise das Bundesdatenschutzgesetz als Maßstab.

Dabei ist zu beachten, dass Risiken aus der bestimmungsgemäß wie auch einer missbräuchlich erfolgenden Verwendung entstehen können. Ein besonderes Augenmerk legte die EU-Kommission zum Beispiel auf RFID-Tags innerhalb der RFID-Anwendung, die noch betriebsbereit sind, während sie schon in den Besitz von Verbrauchern übergegangen sind.

Eine Liste möglicher Risiken für den Datenschutz findet sich im Anhang des DSFA-Rahmenwerks. Sie kann als Leitfaden für die systematische Identifizierung von potenziellen Risiken dienen, sollte jedoch auf Vollständigkeit überprüft werden.

Nachdem die Risiken identifiziert sind, soll eine Bewertung der Risiken aus Sicht des Datenschutzes erfolgen. Hierfür soll

1. die Bedeutung der Gefahr und der Wahrscheinlichkeit des Auftretens, sowie
2. das Ausmaß der Auswirkungen bei Auftreten

ermittelt werden. Dies soll mit angemessenem Aufwand und unter Anlegen vernünftiger Bedingungen erfolgen.

Die sich daraus ergebenden Risiken können dann als gering, mittel oder hoch eingestuft werden. Aus den Risiko-Szenarien sind geeignete Schutzziele abzuleiten.

Schritt 3: Definition und Einführung von Steuerungsmaßnahmen.

In diesem Schritt soll herausgearbeitet werden, welche bestehenden oder zusätzlichen Steuerungsmaßnahmen umgesetzt werden müssen, damit Eintrittsmöglichkeit und Auswirkung der identifizierten Risiken für den Datenschutz minimiert, abgeschwächt oder verhindert werden.

Diese Steuerungsmaßnahmen können in technischen wie auch organisatori-

funkschau Expertenkommentar

Bild: Winckel



Dr. Erhard Schubert
Technischer Leiter beim RFID-Integrator Winckel.

M2M-Kommunikation und der Datenschutz

Die Verwendung neuer Datenübertragungstechniken für die Machine-to-Machine-Kommunikation ruft oft Skepsis in Bezug auf den Datenschutz hervor. Wenn persönliche Mobilgeräte wie Smartphone oder Tablet beispielsweise per Near-Field-Communication (NFC) miteinander kommunizieren, fürchten Endanwender oft, sich dadurch zum „gläsernen Bürger“ zu machen.

Dabei wird mit NFC letztendlich nur eine andere Art der Datenübermittlung eingesetzt. Im Vergleich zu anderen Datenübermittlungsmethoden wie beispielsweise dem Mobilfunknetz hat die Nahfeldkommunikation sogar den Vorteil, dass es sich um eine aktive, also vom Anwender initiierte Datenübermittlung handelt.

Unangenehme Nebeneffekte treten bei der M2M-Kommunikation fast grundsätzlich nicht durch die Übermittlung selbst, sondern durch die darauf folgende Verwendung der Daten auf. Smartphones und Mobilgeräte können schon heute durch Sensoren, Prozessoren und GPS-Empfänger eine Vielzahl von Daten erheben, die sehr sensibel sind. Das wird sich durch die weitere Verbreitung modernen M2M-Medien nicht ändern.

Bei der drahtlosen Übertragung von Daten zwischen zwei Maschinen durch NFC oder RFID können beispielsweise die gespeicherten Daten durch Locking-Funktionen vor Veränderungen und Manipulationen geschützt werden. Bei passiven Karten, wie sie aktuell beispielsweise von der Sparkasse geplant sind, werden nur die heute schon auf Magnetstreifen gespeicherten Daten übermittelt. Der Datenaustausch erfolgt dabei nur über ein anderes, technisch hochwertigeres Medium.

Jede neue Technik verlangt Verantwortung, Vertrauen und Aufklärung. Grundsätzlich gibt es keinen neuen Service oder kein neues Angebot völlig „kostenlos“. Viel wichtiger als die Beobachtung neuer Übermittlungstechnologien ist es, das Bewusstsein für die Wertigkeit der Daten bei den Anwendern weiter zu schärfen. (MK)



Markus Stamm

Senior-Counsel bei Alcatel-Lucent Deutschland in Stuttgart.

Zum Rechtsrahmen im Bereich Smart-Metering sowie Smart-Grids

Smart-Metering und Smart-Grids sind Bestandteile eines zukünftigen Energienetzes, die in der deutschen Öffentlichkeit aktuell intensiv diskutiert werden. Insbesondere, was den Datenschutz angeht, werden dabei Bedenken geäußert, ob die Privatsphäre der Endkunden gewahrt bleibt, und ob Smart-Grids nicht dazu führen, dass Endkunden „ausgespäht“ werden. Dass eine solche Diskussion erfolgreich und dabei sachlich geführt werden kann, zeigen die skandinavischen

Länder: Die Smart-Grid-Technologie ist dort weit verbreitet und der Datenschutz wird nicht weniger ernst genommen als hierzulande. Für Alcatel-Lucent ist der Schutz personenbezogener Daten von Kunden Bestandteil jeder technischen Lösung. Unsere gehostete Smart-Metering-Lösung ist darauf ausgelegt, dass Telekommunikationsanbieter und Energie- und Wohnungswirtschaft sie datenschutzkonform einsetzen können.

Wichtiger als Hinweise auf allgemeine datenschutzrechtliche Maßnahmen ist jedoch der Hinweis auf die derzeit unbefriedigenden gesetzlichen Regelungen. An deren Verbesserung wirkt Alcatel-Lucent zum Beispiel im Rahmen des Bitkom mit. Heute fehlen Regelungen, die Netzbetreibern und Energieversorgern einen zukunftsicheren Ausbau von Smart-Grids ermöglichen. Statt einer klaren, bundesweit einheitlichen Regelung für den Energiesektor gleicht das datenschutzrechtliche Regelwerk mit seinen 16 Ländergesetzen und einem Bundesgesetz einem Flickenteppich. Die zuständigen Landesparlamente setzen beispielsweise darauf, dass jeder Endkunde in die Nutzung von Smart-Metering-Technologie einwilligt. Dies ist nach Meinung von Experten keine tragfähige Grundlage für den flächendeckenden Einsatz einer neuen Technologie.

Der Gesetzgeber muss seine Verantwortung wahrnehmen; er darf nicht die Richtungsentscheidung, Smart-Grids als Zukunftstechnologie einzusetzen, dadurch konterkarieren, dass er dem Endkunden die Entscheidung aufbürdet. Vielmehr muss er selbst den datenschutzrechtlichen Rahmen für Smart-Grids setzen. Alcatel-Lucent vertritt hier die Auffassung, dass der Ausbau der Infrastruktur nicht von einer Einwilligung des Endkunden abhängig sein darf. Stattdessen ist ein verbindlicher Rechtsrahmen notwendig, der die Einwilligung überflüssig macht, aber den Schutz personenbezogener Daten garantiert und die Interessen des Endkunden wahrt. Die Nutzung personenbezogener Daten sollte zudem an die Erfordernisse der jeweiligen Tarifmodelle gebunden werden. Das heißt: Daten würden nur so häufig erhoben, wie es für den entsprechenden Tarif erforderlich ist und würden aggregiert, wo ein Personenbezug nicht mehr nötig ist. Für diese Zweckbindung muss der vorhandene Rechtsrahmen nur in geringem Umfang konkretisiert werden, da das Datenschutzrecht bereits jetzt umfangreiche Zulässigkeitsprüfungen erfordert.

Weiterhin sollte gesetzlich geregelt werden, in welchem Umfang Daten, die bei den Endkunden erhoben werden, als personenbeziehbar gelten sollen. Es ist nämlich keineswegs eindeutig, dass Daten, die beispielsweise für eine Verbrauchsstelle mit mehreren Personen erhoben werden, sich auch auf eine bestimmte oder bestimmbare natürliche Person beziehen. Ist dieser Rechtsrahmen erst einmal geschaffen, steht aus datenschutzrechtlicher Sicht einem Ausbau von Smart-Grids bei Berücksichtigung der berechtigten Interessen der Endkunden und aller übrigen Beteiligten nichts mehr im Wege. (MK)

Endlich frei!



Gehen Sie "wireless" in die weltweite Kommunikation

Vom Mobilfunk bis zur lizenzfreien Funkverbindung.

- ▶ Von GSM bis LTE
- ▶ Embedded Module
- ▶ Gateways und Router
- ▶ GLYN Board Support
- ▶ Kundenspezifische Lösungen

Seit über 10 Jahren kabellos gut – unser Wireless Support!

www.glyn.de

wireless@glyn.de



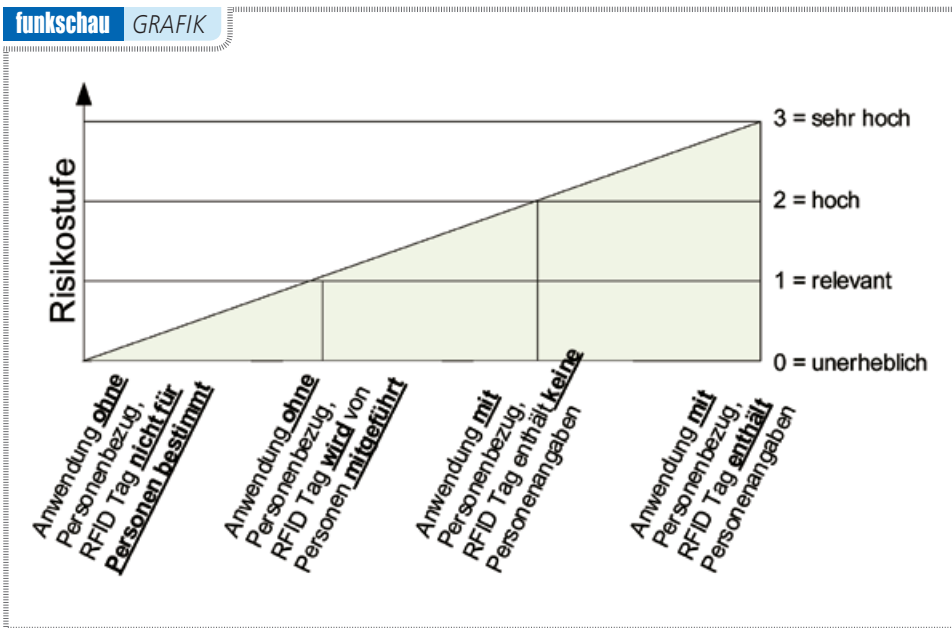


Bild: Concept Factory

schon Regelungen bestehen. Sie werden ihrem Charakter nach in vorbeugende oder aufdeckende Maßnahmen unterschieden. Vorbeugende Maßnahmen verhindern den Schadenseintritt, aufdeckende Maßnahmen informieren über gerade stattfindende oder bereits eingetretene schädigende Umstände.

Auch der bewusste Verzicht auf Risikermöglichende Umstände kann eine Steuerungsmaßnahme darstellen. So kann eine als realistisch eingestufte Gefährdung zum Beispiel vermieden werden, wenn im gefährdeten Bereich keine RFID-Lesegeräte installiert werden.

Im Ergebnis dieses Schrittes ist zu jedem der ermittelten Risiken und den damit verbundenen Risiko-Bewertungen eine Entscheidung zu treffen, welche der ermittelten Steuerungsmaßnahmen diesen wirksam begegnen soll und damit umgesetzt werden müssen. In der Dokumentation zur DSFA soll auch erläutert sein, wie die Steuerungsmaßnahmen sich auf die spezifischen Risiken beziehen, und wie deren Anwendung zu einem akzeptablen Risikolevel führen soll.

Auch für die Beschreibung von Steuerungsmaßnahmen finden sich Beispiele im Anhang zum DSFA-Rahmenwerk.

■ Schritt 4: Dokumentation und Freigabe.

Sobald die Risikobewertung mit den beschlossenen Steuerungsmaßnahmen abgeschlossen wurde, ist die DSFA in einem Bericht zu dokumentieren. Der Bericht umfasst die Beschreibung der Anwendung aus Schritt 1, sowie die Dokumentation von Ablauf und Ergebnissen der Schritte 2 und 3. Er wird dabei auch sensible, gegebenenfalls vertrauliche Unternehmens- und Produkt-Informationen enthalten.

Dieser Bericht ist dem vor Beginn der DSFA namentlich benannten Verantwortlichen zur Freigabe vorzulegen. Die Freigabe hat schriftlich zu erfolgen. Erst nach erfolgter Freigabe soll die Anwendung in Betrieb gehen.

Wird die Freigabe nicht erteilt, sind im Rahmen eines erneuten Durchlaufs der Schritte 1 bis 4 weitere Überlegungen anzustellen, bis das dokumentierte Ergebnis eine Freigabe für den Betrieb der Anwendung rechtfertigen kann.

Der unterzeichnete DSFA-Bericht, mit dem unterschriebenen Freigabebeschluss ist dann bei der im Unternehmen für den Datenschutz zuständigen Stelle aufzube-

funkschau Expertenkommentar

Bild: Carl W. Major



Carl W. Major

Partner bei Trusted Technologies and Solutions.

RFID erfordert umfassende Sicherheitsarchitektur

Überall wo Menschen, Waren oder Geld unterwegs sind, kommen auch RFID-Anwendungen zum Einsatz. So vielfältig wie die Verwendungsmöglichkeiten der automatischen Identifizierung sind leider auch die Gelegenheiten zum Missbrauch. Je nach technischer Beschaffenheit können Daten auf RFID-Tags etwa ausgelesen, beschrieben oder verändert werden, ohne dass der Träger dies bemerkt. Verhaltensdaten können unbemerkt gesammelt, gespeichert und zu Einkaufs- oder Bewegungsprofilen ausgewertet werden. Die gesammelten Daten können zweckentfremdet weiterverbreitet werden.

Zwar werden sowohl die Tags als auch die Lese- und Schreibgeräte standardkonform vor unbefugtem Zugriff und Manipulation geschützt. Aber für die drahtlose Kommunikation dazwischen fehlen bisher einheitliche Standards. Heutige Maßnahmen mit bekannten Internet-Technologien schützen zwar den Weg vom Leser zur zentralen Anwendung oder Datenbank, wie ist es aber mit der Weiterverarbeitung?

Um Datenmissbrauch zu verhindern, ist im Umgang mit RFID eine stabile Sicherheitsarchitektur dringend nötig. Die EU Kommission hat am 12. Mai 2009 deshalb 27 Prinzipien zum Datenschutz in RFID-Anwendungen veröffentlicht. Passend dazu wurde im Januar 2011 eine Rahmenempfehlung ausgegeben – eine Art Vorgehensmodell für die Industrie. Kern hiervon ist das so genannte PIA-Verfahren (Personal Impact Assessment), um die Schutzbedarfsermittlung personenbezogener Daten bei der Anwendungsentwicklung zu systematisieren.

Eine Empfehlung zu einer PIA-Metrik, analog zur Business-Impact-Analyse, welche die Grundlage jeglicher Sicherheitsanalyse bildet, enthält das EU-Rahmenpapier allerdings nicht. Hier sind Spezialisten wie die TTS, Trusted Technologies and Solutions, gefragt. Sie beraten Unternehmen dabei, RFID-Lösungen in Punkto Datenschutz sicher zu machen und in die unternehmensspezifische Sicherheitsarchitektur einzubauen. (MK)

funkschau GRAFIK

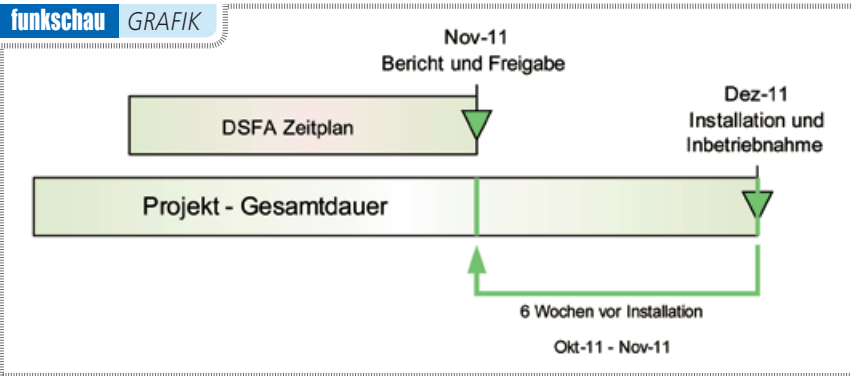


Bild: Concept Factory

- der Datensparsamkeit und
 - der Transparenz
- außer acht. Sie sollten daher nicht kritiklos und insbesondere nicht ohne eine Ergänzung dieser Aspekte angewendet werden.

Fazit und Ausblick

Mit der Datenschutz-Folgeabschätzung kommt ein komplexes Analyseverfahren auf Anwendungsbetreiber zu, das auch ohne gesetzliche Vorgabe die anzuwendenden Compliance-Regeln verbindlich erweitert. Mit einer Ausweitung auf andere Anwendungen außer RFID darf wohl mittelfristig gerechnet werden. Leider hat es die Industrie versäumt, Anhaltspunkte dafür zu geben wie sich der Beschreibungsumfang einer „Vollständigen DSFA“ von dem einer „Kleinen DSFA“ unterscheidet. Dies wird sich daher erst in der Praxis zeigen müssen. (MK)

Es empfiehlt sich, die Datenschutz-Folgeabschätzung im Rahmen des RFID-Gesamtprojektes mit mindestens sechs Wochen Vorlauf einzuplanen.

wahren, und den Aufsichtsbehörden bei Verlangen vorzulegen.

Einsatz von Vorlagen – Vorteile und Grenzen

Das Rahmenwerk nimmt in einigen Passagen Bezug auf Vorlagen, die bei der Durchführung einer DSFA hilfreich sein können. Für Anwendungen des E-Ticketing im Personenverkehr und auf Veranstaltungen, Handelslogistik und den elek-

tronischen Mitarbeiterausweis hat das Bundesamt für Sicherheit in der Informationstechnik BSI gemeinsam mit der Industrie technische Richtlinien zu RFID erstellt, die in Teilen der DSFA als Vorlagen dienen dürfen. Da diese technischen Richtlinien vorrangig auf die Datensicherheit abstellen, lassen sie eine Reihe der Grundfragestellungen zum Datenschutz wie

- der Berechtigungsgrundlage für die Verarbeitung,



Mathias Reinis

Datenschutz-Sachverständiger bei Concept Factory in Bonn und Markus Kien

M2M Datenterminals

GSM - GPRS - EDGE - JAVA - UMTS - HSPA - HSDPA - GPS

PC104-Steckkarte

MC66 Terminal
GSM/GPRS-Terminal
für alle grundlegenden M2M-Lösungen

PCI-Card

MC80 Terminal (o. Abb.)
mit JAVA programmierbaren
Signalisierungs LEDs

MC88/MC88i Terminal
JAVA, GPRS und TCP/IP
- mit Mini-USB-Port (MC88i)

**Antennen
Netzteile
HF-Adapter
Zubehör**

TM-Terminal
für industrielle Applikationen

SMC2
Smart Modem Controller (geöffnet)

MC Technologies GmbH - Kabelkamp 2 - D-30179 Hannover - www.mc-technologies.net
Telefon +49 511 67 69 99 - 0 - Telefax +49 511 67 69 99 185 - info@mc-technologies.net