Die Technische Richtlinie für den sicheren RFID-Einsatz

Motivation zur Erstellung und Ziele des Richtlinienwerks
Innerhalb der letzten Jahre hat sich der Einsatz der so genannten Radio Frequency Identification Technologie (RFID) stark verbreitet. Die Aktivitäten des Bundesamtes für Sicherheit in der Informationstechnik (BSI) zielten bisher darauf ab, generische Sicherheitsbetrachtungen zu dieser Technologie zu erstellen und somit zu einer objektiven Diskussion evtl. vorhandener Gefährdungen des Technikeinsatzes und möglicher Anwendungsfelder beizutragen. Ein Ergebnis dieser Arbeiten ist die Studie „Risiken und Chancen des Einsatzes von RFID-Systemen" [BSI_2004].

Als weiteren Schritt zur Erhöhung des IT-Sicherheitsniveaus in Deutschland wurden, basierend auf den vorhergehenden Aktivitäten, für typische RFID-Einsatzfelder Technische Richtlinien formuliert, die Maßnahmenempfehlungen für den jeweiligen Technikeinsatz enthalten.

Betrachtete Einsatzfelder sind:
- der Zutritt zu Veranstaltungen (Event-Ticketing)
- die Nutzung öffentlicher Verkehrsmittel (ÖPV-Ticketing und NFC-Ticketing)
- das Verwenden von EPC-konformen Transpondern in der Handelskette.

Die Technische Richtlinie RFID (TR RFID) soll dabei den folgenden Zielen dienen:

1. Verwendbarkeit als Leitfaden für Systemlieferanten und Systemanwender zur sachgerechten Implementierung von spezifischen RFID-Systemlösungen bzgl. Funktions- und Informationssicherheit und Datenschutz

2. Schaffung von Aufmerksamkeit und Transparenz in Bezug auf Sicherheitsaspekte

3. Basis für eine Konformitätserklärung der Systemlieferanten oder Betreiber und die Vergabe eines Gütesiegels durch eine Zertifizierungsstelle.

Die Methodik der TR RFID
RFID-basierte Systeme können sehr komplex sein. In den meisten Fällen gehören zur Systemlösung viele Komponenten, die nicht mit RFID ausgestattet sind. Auf der anderen Seite dürfen bei der Betrachtung der Systemsicherheit nicht nur das Medium und die Lesegeräte berücksichtigt werden.

Die Technische Richtlinie muss alle für die RFID-Technik relevanten Sicherheitsaspekte im Detail einbeziehen. Diese Aspekte hängen stark vom Einsatzgebiet und der jeweiligen Implementierung der Systemlösung ab.

Das formulierte Richtlinienwerk enthält daher detaillierte Angaben über das Einsatzgebiet und die zugehörigen Betriebsprozesse. Basierend auf diesen Prozessen werden Use Cases bestimmt, die für die Sicherheitsbetrachtung des RFID-Systems relevant sind. Diese Use Cases werden anschließend als Grundlage für die Ermittlung von Gefährdungen und eine detaillierte, systemspezifische Sicherheitsbewertung für die mit RFID im Zusammenhang stehenden Bereiche des Systems genutzt. Abbildung 1 zeigt diese Vorgehensweise am Beispiel des eTicketing im ÖPV.

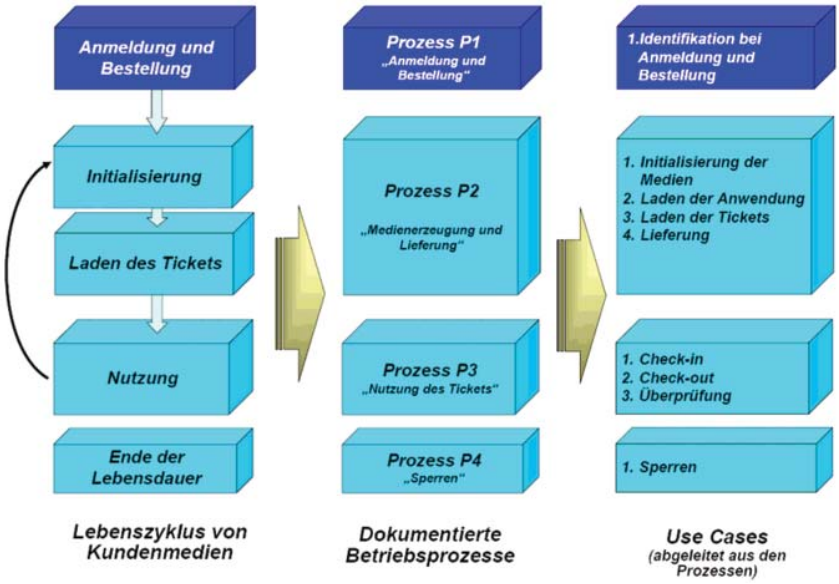

Abb. 1: Bestimmung RFID-relevanter Use Cases für das eTicketing nach [ISSE2007]

Alle anderen Systemkomponenten werden nur allgemein behandelt. Die vorgeschlagenen Sicherheitsmaßnahmen basieren auf offenen IT-Sicherheitsstandards.

Dieses Konzept legt den Schwerpunkt der Betrachtung auf die für RFID relevanten Systemteile und gewährleistet dennoch die Berücksichtigung aller Sicherheitsaspekte.

Skalierbarkeit und Flexibilität
Die TR RFID soll in erster Linie Sicherheitsfragen behandeln. Parallel muss für alle Implementierungen, die auf dieser Richtlinie aufsetzen, ein wirtschaftlicher Betrieb möglich sein. Daher sollen die folgenden Anforderungen an die Methodik der Richtlinie berücksichtigt werden:

1. Es muss möglich sein, Systeme so zu implementieren, dass eine Ausgewogenheit von Kosten und Nutzen erreicht wird.

2. Die für die Technische Richtlinie ausgewählten Einsatzszenarien umfassen eine große Bandbreite, von kleinen bis zu landesweiten oder sogar grenzüberschreitenden Anwendungen. Wichtig ist, dass das in der Richtlinie verwendete Konzept für Systemlösungen aller Größen und verschiedener Komplexität genutzt werden kann.

3. In vielen Fällen lässt sich die Wirtschaftlichkeit einer Systemlösung wesentlich leichter durch die Kooperation mit Geschäftspartnern erreichen. Dies gilt insbesondere für eTicketing-Anwendungen, bei denen es vorteilhaft sein kann, wenn bereits beim Kunden verfügbare Medien (z.B. NFC-fähige Telefone) für zusätzliche Anwendungen verwendet werden können.

Um die genannten Anforderungen zu erfüllen, wird für diese Technische Richtlinie folgendes Konzept verwendet:

1. Ein passendes Rollenmodell und die Struktur einiger Hauptelemente (Produkte, Applikationen und Medien) werden beschrieben. Dieses Modell unterstützt einen skalierbaren und erweiterbaren Ansatz.

2. Die Technische Richtlinie muss Sicherheitskonzepte anbieten, die alle in einer Infrastruktur verwendeten Kombinationen von Einsatzszenarien und Medien umfassen.

3. Gleiche Einsatzgebiete (insbesondere im eTicketing), die die Möglichkeit für anwendungsübergreifende Partnerschaften bieten, werden in den entsprechenden Technischen Richtlinien mit so viel Kommunalität wie möglich behandelt. Die Sicherheitsbewertung basiert auf ähnlichen Sicherheitszielen, die Schutzmaßnahmen verwenden, wenn möglich, die gleichen Mechanismen.

4. Eine besondere Herausforderung besteht bei system- und anwendungsübergreifenden Partnerschaften im Hinblick auf die Systemsicherheit. Es muss gewährleistet sein, dass die Sicherheit eines Systems nicht von Schwächen eines anderen Systems untergraben wird.

Die Sicherheitsmethodik

Jede Technische Richtlinie enthält Beispiele zur Durchführung der Sicherheitsbewertung in bestimmten Einsatzszenarien. Diese können an die Anforderungen und Randbedingungen der speziellen Systemimplementierung angepasst werden.

Abbildung 2 zeigt das in allen Technischen Richtlinien verwendete Konzept der Sicherheitsbewertung.

Grundsätzlich orientiert sich dieses Vorgehen an den Standards

- BSI 100-1 „Managementsysteme für Informationssicherheit (ISMS)“,
- BSI 100-3 „Risikoanalyse auf der Basis von IT-Grundschutz“,
- ISO/IEC 27001:2005 „Information technology – Security techniques – Information security management systems – Requirements“ und
- ISO FCD 27005 „IS Risk Management“, (Stand 12-06).

Eine Besonderheit der Vorgehensweise ist einerseits jedoch das Formulieren von Maßnahmen unterschiedlicher Mechanismenstärke für unterschiedlich schutzbedürftige Anwendungen und zu verarbeitende Informationen sowie andererseits das Empfehlen von sehr detailliert auf bestimmte Einsatzgebiete zugeschnittenen Maßnahmen. Hiermit ist es dem Anwender des Richtlinienwerks möglich, ohne das vollständige Durchlaufen der Methodik alleine durch die Wahl eines bestimmten, durch die TR vorgegebenen Einsatzszenarios sowie der Wahl einer zugehörigen Schutzbedarfskategorie sofort zu Maßnahmenempfehlungen zu gelangen.

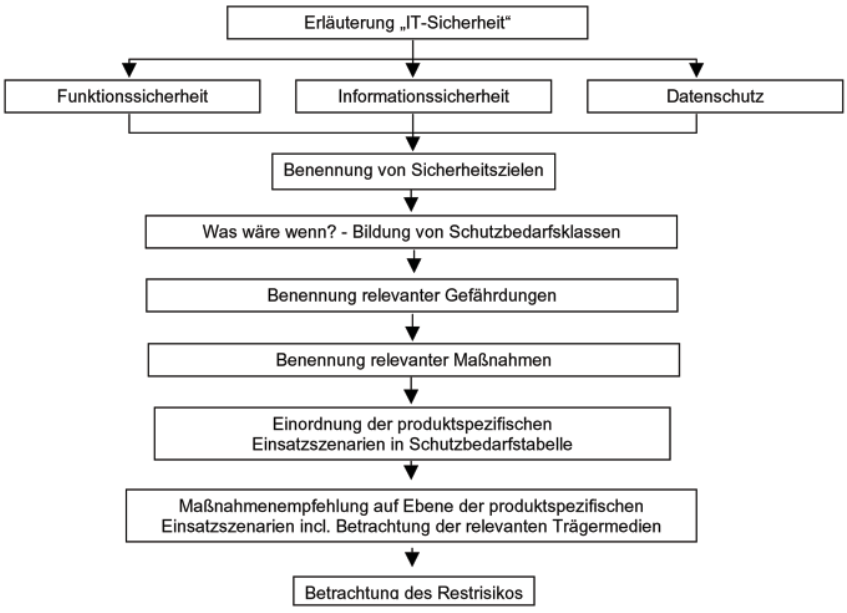

Abb. 2: Vorgehensweise der Sicherheitsbetrachtung nach [ISSE2007]

Abstimmungsprozesse mit Anbietern, Betreibern und potenziellen Nutzern von RFID-Systemen

Die gewählte Vorgehensweise bei der Erstellung der TR RFID setzte voraus, dass ein umfangreiches Wissen über Prozesse sowie an den Prozessen beteiligten Akteuren im Bereich der zu betrachtenden Einsatzgebiete der RFID-Technik vorhanden ist. Dies war nur durch das Einbinden von Systemanbietern und Betreibern der Technologie in den Erstellungsprozess der Dokumente möglich.

Weiterhin sollten bereits frühzeitig die Interessen des Verbraucherschutzes sowie des Datenschutzes berücksichtigt werden. Aus diesem Grund fanden zu jedem innerhalb der TR RFID behandelten Einsatzgebiet Workshops statt, an denen Vertreter der genannten Gruppen teilgenommen haben. Den Abschluss der Abstimmungsphase bildete ein öffentlicher Workshop, an den sich eine Kommentierungsphase anschloss, während derer allen Interessierten die Möglichkeit zur Kommentierung der vorliegenden Dokumente gegeben wurde.

Literatur

[ISSE2007]
Bartels, C., Kelter, H., Technical Guidelines for Implementation and Utilisation of RFID-based Systems, aus ISSE/SECURE2007, Securing Electronic Business Processes, Vieweg-Verlag 2007, ISBN 978-3-8348-0346-7

[BSI_2004]
Hilty, L., Kelter, H., Köhler, A., Oertel, B., Ullmann, M., Wittmann, S., Wölk, M., „Risiken und Chancen des Einsatzes von RFID-Systemen“, herausgegeben vom Bundesamt für Sicherheit in der Informationstechnik, SecuMedia-Verlag 2004, ISBN 3-922746-56-X

Harald Kelter
Bundesamt für Sicherheit in der Informationstechnik (BSI)
E-Mail: harald.kelter@bsi.bund.de