Technische Richtlinie für den sicheren RFID-Einsatz

Mit Einführung neuer Technologie stellt sich häufig die Frage nach dem Sicherheitsniveau einer darauf basierenden Anwendung. Zur Bewertung des Sicherheitsniveaus solcher Anwendungen gibt es verschiedene Ansätze mit unterschiedlichem Komplexitätsgrad. Der vorliegende Artikel beschreibt die Verwendung technischer Richtlinien für Radio Frequency Identification (RFID) und die Anwendung des elektronischen Ticktings als eine mögliche Methode zur Festlegung des erforderlichen Sicherheitsniveaus.

Von Harald Kelter, BSI

Innerhalb der letzten Jahre hat sich der Einsatz der so genannten Radio-Frequency-Identification-Verfahren (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 eventuell vorhandener Gefährdungen des Technikeinsatzes und möglicher Anwendungsfelder beizutragen. Ein Ergebnis dieser Arbeiten ist die Studie „Risiken und Chancen des Einsatzes von RFID-Systemen“ [1].

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:

- Verwendbarkeit als Leitfaden für Systemlieferanten und Systemanwender zur sachgerechten Implementierung von spezifischen RFID-Systemlösungen bezüglich Funktions- und Informationssicherheit und Datenschutz,
- Schaffung von Aufmerksamkeit und Transparenz in Bezug auf Sicherheitsaspekte sowie
- Basis für eine Konformitätserklärung der Systemlieferanten oder Betreiber und die Vergabe eines Gütesiegels durch eine Zertifizierungsstelle.

Zur Umsetzung dieser Ziele sind folgende Informationen erforderlich:

- Ermittlung der Sicherheitsanforderungen an ein RFID-System eines Einsatzgebietes,
- Benennung der spezifischen Gefährdungen, geeigneter Gegenmaßnahmen und des möglicherweise verbleibenden Restrisikos sowie
- Definition der Kriterien für eine Konformitätserklärung beziehungsweise Zertifizierung.

Methodik

RFID-basierte Systeme können sehr komplex sein. In den meisten Fällen gehören zur Systemlösung auch viele Komponenten, die nicht mit RFID ausgestattet sind. Auf der anderen Seite dürfen bei der Be-

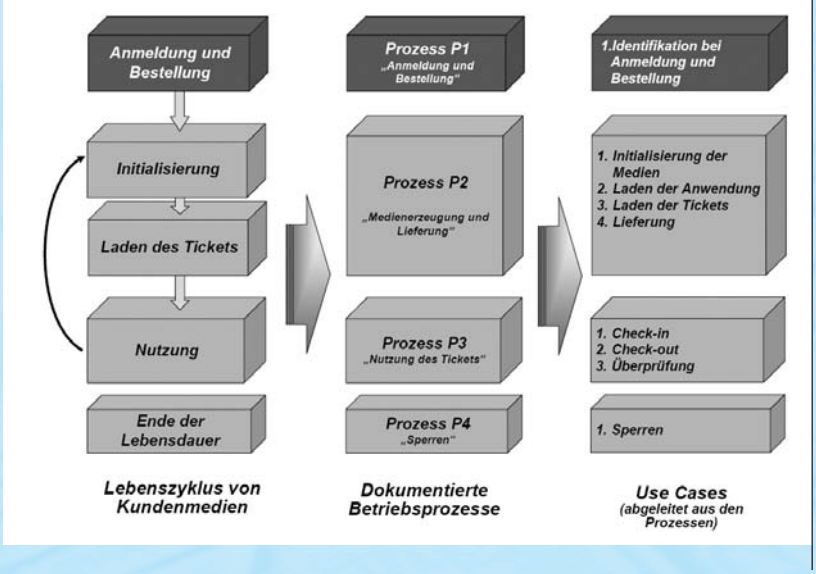

Abbildung 1: Bestimmung RFID-relevanter Use-Cases für das E-Ticketing nach [2]

trachtung der Systemsicherheit nicht nur das Medium und die Lesegeräte berücksichtigt werden.

Die Technische Richtlinie RFID muss alle für RFID 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 (einschließlich der Vertriebskanäle und -prozesse). Die Prozesse decken den gesamten Lebenszyklus eines Trägermediums oder Transponders ab. Basierend auf diesen Prozessen werden Use-Cases bestimmt, die für die Sicherheitsbetrachtung des RFID-Systems relevant sind. Diese Use-Cases werden dann 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 E-Ticketing im ÖPV.

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.

Auf der anderen Seite lässt die technische Richtlinie auch Raum für individuelle und anwendereigene IT-Implementierungen (Back-Offices, Vertriebs- und Logistiksysteme etc.). Dies unterstützt insbesondere die Erweiterung bestehender Systeme um die RFID-Technologie.

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 Methodologie der Richtlinie berücksichtigt werden:

_____ Es muss möglich sein, Systeme so zu implementieren, dass eine Ausgewogenheit von Kosten und Nutzen erreicht wird. Dies bedeutet in der Praxis, dass die Schutzmaßnahmen den ermittelten Schutzbedarf zwar erfüllen, aber nicht übertreffen müssen. Beispiel: Werden nur preiswerte Produkte verwendet, die eine relativ niedrige Sicherheitsanforderung haben, sollten die Schutzmaßnahmen entsprechend gestaltet werden. Dies ermöglicht beispielsweise die Verwendung preiswerter Medien, wodurch sich die Kosten für die Systemimplementierung und den Betrieb verringern.

_____ 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.

_____ In vielen Fällen lässt sich die Wirtschaftlichkeit einer Systemlösung wesentlich leichter durch die Kooperation mit Geschäftspartnern erreichen. Dies gilt insbesondere für E-Ticketing-Anwendungen, bei denen es sehr vorteilhaft sein kann, wenn bereits beim Kunden verfügbare Medien (z. B. Karten mit Mehrfachanwendung oder NFC-fähige Telefone) für zusätzliche Anwendungen, Produkte und damit verbundene Dienstleistungen wieder verwendet werden können.

Abbildung 2 zeigt, dass unter Umständen verschiedene Produkte beziehungsweise Einsatzszenarien in einem System unterstützt werden müssen. Dabei werden diese Produkte möglicherweise auf verschiedene Trägermedien aufgebracht.

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

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

_____ Die technische Richtlinie muss Sicherheitskonzepte anbieten, die alle in einer Infrastruktur verwendeten Kombinationen von Einsatzszenarien und Medien umfassen. Dies wird durch individuelle Sicherheitsbewertungen, die auf den relevanten Use-Cases basieren, erreicht.

_____ Gleiche Einsatzgebiete (insbesondere im E-Ticketing), welche die Möglichkeit für anwendungs-

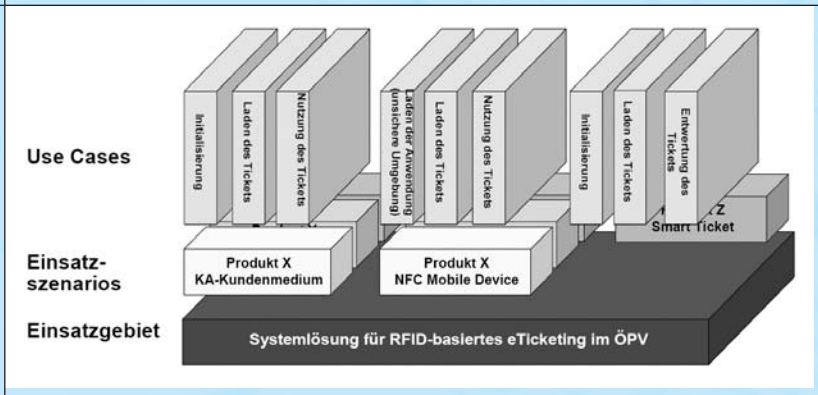

Abbildung 2: Beispiel für Einsatzszenarien und relevante Use-Cases für E-Ticketing im ÖPV nach [2]

übergreifende 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.

_____ 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. Dies erfordert normalerweise eine umfassende Sicherheitsbewertung beider Systeme. Die technischen Richtlinien widmen sich diesem Problem durch Einführung eines skalierbaren und transparenten Konzepts für die Anwendung von Schutzmaßnahmen gegenüber den festgestellten Gefährdungen, den „Schutzbedarfsklassen“: Insgesamt werden drei Klassen von 1 (normale Anforderung) bis zu 3 (hohe Anforderung) verwendet. Alle Schutzmaßnahmen werden entsprechend in drei Stufen definiert, von normalem Schutz bis zu erweitertem Schutz. Bei jeder individuellen Systemimplementierung wird zuerst die Schutzbedarfskategorie für jedes Sicherheitsziel definiert. Daraus ergibt sich der Umfang der zu ergreifenden Schutzmaßnahmen. Dieses Konzept bietet eine einfache Möglichkeit zur Installation einer sicheren Systemkooperation. Es muss lediglich sichergestellt werden, dass die Schutzbedarfsklassen beider Systeme zusammenpassen.

Tabelle 1 zeigt den Aufbau aller bisher erstellten technischen Richtlinien.

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 3 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 2006-12).

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.

Abstimmungsprozesse

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 RFID-Technik in den Erstellungsprozess der Dokumente möglich. Weiterhin sollten bereits frühzeitig die Interessen des Verbraucherschutzes sowie des Datenschutzes berücksichtigt werden. Aus diesem Grund fanden im Verlauf des Jahres 2007 zu jedem innerhalb der TR RFID behandelten Einsatzgebiet Workshops statt, an denen Vertreter der genannten Gruppen teilgenommen haben. Den

Kapitel	Inhalt
Beschreibung des Einsatzgebiets	Beschreibung des Einsatzgebiets: Aufbau, Leistungen, spezielle Randbedingungen etc.
Produkte und Leistungen	Beschreibung von Beispielprodukten und -leistungen sowie Vertriebskanälen
Definitionen	Modelle, Begriffsdefinitionen
Einführung in die Methodologie	Vorstellung des für die Sicherheitsbewertung verwendeten Konzepts sowie der Methoden
Allgemeine Anforderungen	Allgemeine Anforderungen der beteiligten Parteien, beachtenswerte Aspekte etc.
Betriebsprozesse	Beschreibung von Betriebsprozessen, die für den Lebenszyklus von Trägermedien von Bedeutung sind
Use-Cases	Definition von RFID-relevanten Use-Cases
Sicherheitsbewertung	1. Einführung in die IT-Sicherheit 2. Definition spezieller Sicherheitsziele, Schutzbedarfsklassen und Gefährdungen 3. Vorgeschlagene Schutzmaßnahmen

Tabelle 1: Aufbau der TR RFID

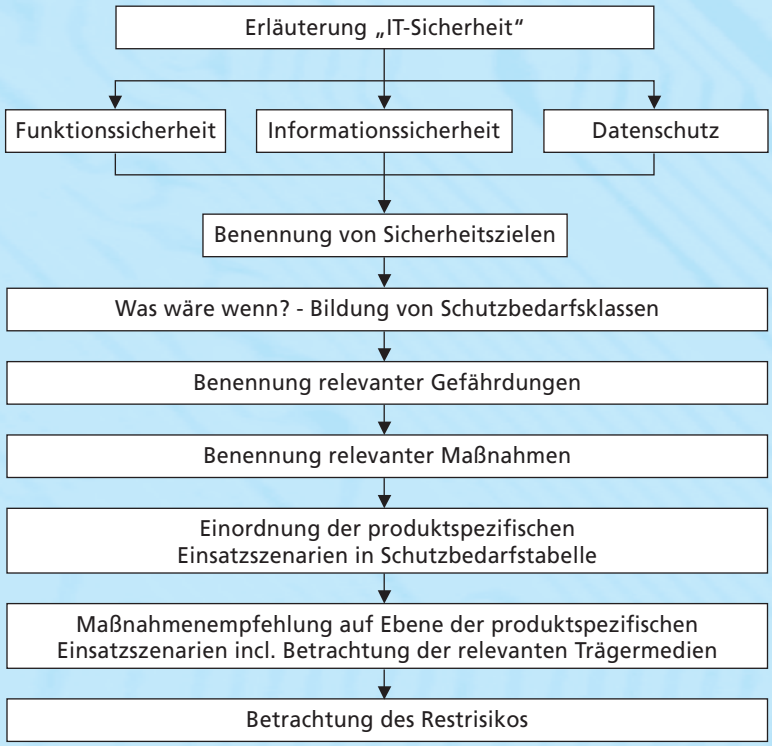

Abbildung 3: Vorgehensweise der Sicherheitsbetrachtung nach [2]

Abschluss der Abstimmungsphase bildete ein öffentlicher Workshop im Dezember 2007, an den sich eine Kommentierungsphase anschloss, während derer allen Interessierten die Möglichkeit zur Kommentierung der vorliegenden Dokumente gegeben wurde.

Weitere Vorgehensweise

Zum Zeitpunkt der Veröffentlichung dieses Artikels sind eingegangene Kommentare eingefügt beziehungsweise mit den kommentierenden Stellen diskutiert worden. Eine Veröffentlichung der Final-Versionen der technischen Richtlinien für die Einsatzgebiete Event-Ticketing, ÖPV-Ticketing und NFC-Ticketing steht dementsprechend kurz bevor. Weiterhin ist zur CeBit 2008 mit der Veröffentlichung einer Entwurfsfassung der technischen Richtlinie für das Einsatzgebiet der Handelslogistik zu rechnen. An diese Veröffentlichung wird sich ebenfalls eine öffentliche Kommentierungsphase anschließen. Das vollständige Richtlinienwerk wird dementsprechend im Sommer 2008 in einer finalen deutschen und englischsprachigen Version vorliegen. ■

Literatur

[1] BSI (Hrsg.), L. Hilty, H. Kelter, A. Köhler, B. Oertel, M. Ullmann, S. Wittmann, M. Wölk, Risiken und Chancen des Einsatzes von RFID-Systemen, SecuMedia-Verlag, 2004, ISBN 3-922746-56-X

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

kurz notiert

BSI veröffentlicht zwei neue Studien

Log-Daten-Studie

Log- und Monitoringdaten werden in jedem IT-Verbund von den verschiedensten IT-Systemen und Anwendungen in großer Menge und Vielfalt generiert. Vielfach enthalten die erzeugten Meldungen Informationen, die auf mögliche Sicherheitsprobleme oder bereits eingetretene Sicherheitsvorfälle schließen lassen. Die Idee, diese Informationsquellen zur Verbesserung der IT-Sicherheit zu erschließen, liegt daher nahe.

Die „Studie über die Nutzung von Log- und Monitoringdaten im Rahmen der IT-Frühwarnung und für einen sicheren IT-Betrieb“ dokumentiert den Stand der Technik im Hinblick auf die Verarbeitung und Speicherung von Log- und Monitoringinformationen und soll die Grundlage dafür legen, dass diese Informationen in IT-Frühwarnsystemen effizient genutzt werden können.

Web-2.0-Studie

Der Begriff Web 2.0 ist ein derzeit häufig gebrauchtes Schlagwort, dessen Bedeutung allerdings nicht immer ganz klar ist und je nach Kontext schwanken kann. Die meisten Anwendungen, die mit dem Stichwort Web 2.0 in Verbindung gebracht werden, haben aber eines gemeinsam: Sie nutzen intensiv aktive Inhalte.

Die vorliegende Studie „Web 2.0“ beschäftigt sich mit den Sicherheitsaspekten einiger dieser Anwendungen, insbesondere mit einer Technik, die in vielen Fällen die technische Grundlage für Web-2.0-Anwendungen ist: Asynchronous JavaScript and XML – kurz: Ajax.

Das Ergebnis der Studie bestätigt erneut die Position des BSI, von der Verwendung aktiver Inhalte in Web-Anwendungen abzuraten. Den neuen Möglichkeiten, die Verfahren wie Ajax bieten, steht eine Anzahl neuer Gefährdungen gegenüber, die bei einer Abwägung von Nutzen gegen Risiko klar *gegen* die Nutzung aktiver Inhalte sprechen.

Beide Untersuchungen stehen unter www.bsi.bund.de/literat/ zum kostenfreien Download zur Verfügung.