IT-SECURITY

Die Sicherheit von RFID-Systemen

Jede Woche beantworten Sicherheitsexperten Leserfragen und geben Ratschläge, wie sich die Sicherheit in einem Unternehmen erhöhen lässt.

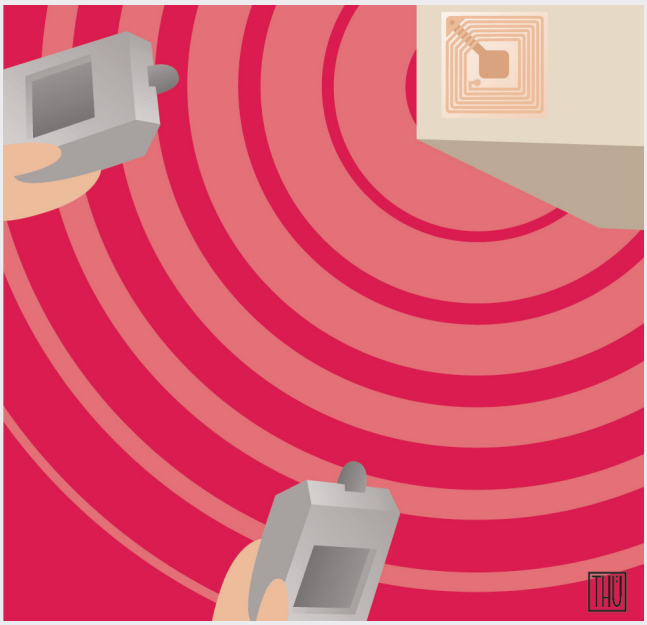

ILLUSTRATION: CW/THÜ

Frage: Die Verwendung von RFID-Systemen nimmt stetig zu. Stellen diese Systeme nicht ein gefundenes Fressen für eine neue Generation von Hackern dar?

In der Tat führen die sinkenden Preise in der RFID-Branche (Radio Frequency Identification) zu einem akuten Verwendungsanstieg – sei es zur Identifikation von Banknoten, Tieren oder Einkaufswaren. Ein RFID-System besteht aus einem Lesegerät, welches über eine Luftschicht mit dem Transponser (RFID-Tag) kommunizieren kann. Jeder Transponder muss eine eindeutige Identifikation (ID) besitzen und einem bestimmten Trägerobjekt zugeordnet sein. Das Zusammenspiel der drei unterschiedlichen Komponenten und jeweils zugehörigen Schnittstellen zeigt bereits das Angriffspotenzial von RFID-Systemen.

Ausspähen: Ein Unbefugter verschafft sich Zugang zu vertraulichen Daten. Die Bedrohung durch Ausspähen kann zweierlei Ursachen haben.

Die Luft als Transportmedium zwischen RFID-Tag und Lesegerät stellt das erste grosse Sicherheitsproblem dar. Wie bereits aus der Wireless-Technologie bekannt, können über die Luft transportierte Daten ziemlich leicht mit einem Empfänger abgehört werden.

Mit einem eigenen Lesegerät hingegen zielt ein Späher direkt auf die gespeicherten Daten eines Tags. Er muss in der Regel allerdings in der Lage sein, die Identität des Lesegeräts zu fälschen.

> «Durch den Einsatz von RFID-Tags können Bewegungs- und Konsumprofile erstellt werden.»

Täuschen: Unter einer Täuschung versteht man das Einspeisen von falschen Daten ins System. Dies kann wiederum auf verschiedene Arten praktiziert werden: Zum einen können die Daten, welche auf dem Tag gespeichert sind, verändert werden. Zum anderen kann ein Hacker, der die ID und allfällige Passwörter eines Tags in Erfahrung bringt, diesen Tag nachbilden oder klonen und dessen Identität gegenüber einem Lesergerät vortäuschen. Eine weitere Täuschung besteht darin, den Transponder vom Trägerobjekt abzulösen. Somit kann entweder die Identität des Trägerobjekts verschleiert oder ein anderes Objekt als das ursprüngliche ausgegeben werden.

Denial of Service (DoS): Auch auf RFID-Systeme können DoS-Attacken verübt werden. Diese haben zur Folge, dass das System in seiner korrekten Funktionsweise beeinträchtigt wird. Dazu gehören unter anderem die Zerstörung der Tags (durch Knicken oder durch chemische Stoffe), das Senden von Störsignalen oder auch Blocker-Tags, die eine grosse Zahl von Tags simulieren und somit das Lesegerät ausser Betrieb setzen.

Doch RFID-Tags beeinträchtigen auch die Privatsphäre: Der Einsatz von RFID-Tags ermöglicht die Erstellung von exakten Bewegungs-, Konsum- und Kontaktprofilen. Dies bedeutet einen massiven Einschnitt in unsere Privatsphäre.

Wie lassen sich nun die Daten von RFID-Systemen schützen? Durch starke Authentifizierung von Tags gegenüber einem Lesegerät und umgekehrt lassen sich die Daten über Zugriffsrechte schützen. Das Abhören einer Kommunikation über die Luftschicht kann kaum verhindert werden. Doch werden die Daten verschlüsselt übertragen, ist das Horchen mit erheblich höherem Aufwand verbunden.

Eine Reihe weiterer Massnahmen werden an dieser Stelle zur Vervollständigung erwähnt:

Einsatz von Read-Only-Tags, abhörsichere Antikollisionsprotokolle, Pseudomisierung (Verschleierung der Tag-Identität), starke Verbindung des Tags mit dem Trägerobjekt (kein Entfernen) sowie Speicherung der eigentlichen Daten nicht auf dem Tag, sondern in einer Datenbank im Backend.

Die Gefahr, dass Daten ungerechtfertigt ausgewertet werden, geht allerdings nicht nur von Angreifern aus. Auch die Betreiber einer solchen RFID-gestützten Datenbank lassen sich gerne entgegen der gängigen Datenschutzbestimmung des Bundes zur Erstellung von personenbezogenen Statistiken hinreissen. ■

Der Autor
Ivan Roman ist Consultant und Trainer bei Roman-Consulting & Engineering in Zürich, www.roman.ch

Unsere Experten beantworten Ihre Fragen. Schreiben Sie uns: it-security@computerworld.ch

Ein Archiv der Helpdeskartikel finden Sie im Internet: www.computerworld.ch