

RFID-EINSATZ IM KRANKENHAUS

Störungen bei medizinischen Geräten möglich



Beim Einsatz von drahtloser Funktechnologie im medizinischen Bereich ist Vorsicht angebracht. In einer im US-amerikanischen Ärzteblatt (JAMA2008; 299: 2884–90; <http://jama.ama-assn.org/cgi/content/short/299/24/2884>) veröffentlichten Studie haben niederländische Wissenschaftler nachgewiesen, dass RFID-Etiketten auf einer Intensivstation die Funktion von lebenswichtigen medizinischen Geräten stören können. RFID-Chips werden beispielsweise zur Patienteniden-

tifikation oder zur Geräteortung eingesetzt. Dabei handelt es sich um elektronische Transponder, die entweder aktiv elektromagnetische Signale aussenden oder passiv durch ein Lesegerät zur Emittierung von elektromagnetischen Wellen angeregt werden. Die zur Ablesung erforderlichen elektromagnetischen Wellen sind jedoch ein potenzielles Sicherheitsrisiko.

Die Forscher untersuchten, was passiert, wenn aktive und passive RFID-Chips sich in der Nähe von medizintechnischen Geräten, wie Be-

atmungsgeräten, Ventilatoren, Infusionspumpen, Narkosegeräten oder Herzschrittmachern, befinden. Das aktive RFID übermittelte die Informationen auf einer Frequenz von 125 kHz. Das passive RFID wurde auf der Frequenz von 868 MHz zur Datenübermittlung angeregt. Zunächst betrug die Entfernung zu den medizinischen Geräten zwei Meter, sie wurde dann um jeweils 50 cm verringert, wenn keine Störung auftrat, oder um 50 cm erweitert, wenn es zu einer Störung kam. Letzteres war häufiger der Fall: So traten in einer Entfernung von einem Zentimeter bis sechs Metern bei 34 von 123 Tests Fehlfunktionen der medizinischen Geräte auf. In 22 Fällen waren diese Störungen gefährlich, weil Beatmungsgeräte ausfielen oder selbsttätig die Atemfrequenz veränderten, weil Infusionspumpen stoppten oder externe Schrittmacher den Dienst versagten, weil ein Dialysegerät ausfiel oder der EKG-Monitor eine nicht vorhandene Rhythmusstörung anzeigte.

Diese Fehlfunktionen können zu schwerwiegenden medizinischen Komplikationen führen. Die Wissenschaftler fordern daher ausgiebigere Tests im Intensivbereich. **KBr**

STUDIE

Hackerattacken auf Herzschrittmacher

Computerhacker sind theoretisch in der Lage, Herzschrittmacher und automatische Defibrillatoren (ICD) gezielt zu manipulieren und so beispielsweise Attentate auf prominente Implantatträger zu verüben. Darauf haben US-Computerexperten aus Boston in einer experimentellen Studie hingewiesen.

ICDs sind mit einem eingebauten Radiosender für einen drahtlosen Datenaustausch ausgestattet. Die Daten werden dabei in der Regel über eine direkt auf die Brust aufgelegte Antenne übertragen. Diese enthält einen Magnetschalter, um eine versehentliche Störung, etwa durch elektromagnetische Felder, zu verhindern. Diese Sicherung ist aber für Computerspezialisten zu überwinden, denn die Software, die die-

sen Schalter steuert, lässt sich von außen abstellen. Außerdem können die auf dem ICD gespeicherten Daten ausgelesen werden. Die an den Experimenten beteiligten Experten halten verschiedene Angriffsszenarien für möglich - vom einfachen Abschalten des Geräts bis hin zur Induktion einer tödlichen Entladung der Batterie.

Bislang war die Reichweite der Sender gering, sodass ein Attentäter dem ICD-Träger schon sehr nahe kommen müsste, um Kontakt mit dem Steuergerät des ICD aufnehmen zu können. Inzwischen stellen viele Hersteller ihre Geräte jedoch mit stärkeren Sendern aus. Technisch wäre es möglich, die Geräte über ein WLAN-Netz mit dem Internet zu verbinden. Die Daten des



ICD könnten dann auf einem Server gespeichert werden. Solche Systeme ermöglichen Kardiologen eine telemetrische Betreuung ihrer Patienten, bieten aber auch Möglichkeiten zu Manipulationen.

Die Forscher sehen zwar keine unmittelbar drohende Gefahr für die Patienten, fordern jedoch eine Verbesserung der Sicherheitsstandards bei den Implantaten. **KBr**

**Dreikammer-
Herzschritt-
macher**