news 15.03.2006 15:07

Katze mit Computervirus

Mit Hilfe einer Datenbank für ausgelesene Informationen lassen sich RFID-Transponder, wie sie auch zur Markierung von Haustieren benutzt werden, als Gastgeber für Virensoftware missbrauchen. Andrew Tanenbaum, der Erfinder des Betriebssystems Minix, hat auf der **IEEE Conference of Pervasive Computing[1]** in Pisa gleich mehrere Angriffsszenarien zur drahtlosen Datenerfassung per RFID beschrieben. Wie der gebürtige US-Amerikaner auch auf einer **Website[2]** der freien Universität Amsterdam darlegt, könnte zum Beispiel ein böswilliger Hacker einen RFID-markierten Artikel regulär im Supermarkt erstehen und den darauf angebrachten Transponder anschließend durch einen von ihm selbst programmierten ersetzen. Schmuggelt er die Ware mit der manipulierten Auszeichnung zurück in den Laden und legt sie erneut zur Bezahlung vor, kann er Supermarkt-Software, die sonst nur digitale Preisschildchen übers RFID-Lesegerät auswerten muss, mit schädlichem Code füttern.

Um die Machbarkeit solcher Attacken zu beweisen, hat Tanenbaum einen Virus für RFID-Middleware des Anbieters Oracle geschrieben, der mit gemeinhin verfügbaren 128 Byte an Transponder-Memory auskommt. Einmal in die Datenbank eingebracht, entpuppt sich der Transponder-Inhalt als so genannter Quine – ein Programm, das seinen eigenen Quelltext ausgibt – und vermag sich in der Datenbank zu replizieren. Auf diesem Weg ist auch die Infektion weiterer Transponder vorstellbar. Ähnliche Szenarien bauen auf die reiskorngroßen RFID-Tags, die hierzulande das Identifizieren entlaufener Haustiere erleichtern sollen und die typischerweise von Tierärzten oder Tierheimen kodiert und injiziert werden, daher der Titel von Tanenbaums Vortrag (**PDF-Datei[3]**).

Der Professor beschreibt auch andere Techniken, mit denen man ein RFID-System in der Theorie sabotieren kann, etwa einen Wurm, der sich per Internet auf die RFID-Middleware ausbreitet. Seine Anleitung zur Gegenwehr beschränkt sich indes auf eher allgemeine Faustregeln, etwa, dass man unbenötigte Nutzerkonten für RFID-Middleware blockieren und die Software insgesamt mit möglichst begrenzten Nutzerprivilegien betreiben solle.

Siehe dazu auf Telepolis:

- **Der erste RFID-Virus wurde präsentiert[4]**

(**hps[5]**/c't) (hps/c't)

URL dieses Artikels:
http://www.heise.de/newsticker/meldung/70871

Links in diesem Artikel:
[1] http://cnd.iit.cnr.it/percom2006/
[2] http://www.rfidvirus.org/index.html
[3] http://www.rfidvirus.org/papers/percom.06.pdf
[4] http://www.heise.de/tp/r4/artikel/22/22252/1.html
[5] mailto:hps@ct.heise.de

Copyright © 2006 Heise Zeitschriften Verlag