Onderzoekers vinden manier om rfid-chips te infecteren

Woensdag 15 maart 2006, 11:33 - Onderzoekers van de Vrije Universiteit Amsterdam hebben een manier gevonden om kwaadaardige code aan een rfid-chip toe te voegen.

Door Wilbert de Vries

Rfid (radio frequency identification) is een steeds vaker gebruikte technologie die het mogelijk maakt om goederen te voorzien van een 'elektronische chip'. Bedrijven kunnen met speciale scanapparatuur eenvoudig zien waar bepaalde goederen zich in het productie- of verzendproces bevinden.

Speciaal geprepareerde rfid-chips zouden echter misbruikt kunnen worden om een virus te verspreiden of om een achterdeur in een systeem te openen. Het onderzoek is uitgevoerd door promovenda Melanie Rieback en Student Patrick Simpson van de VU onder toezicht van hoogleraar Andy Tanenbaum.

In hun rapport 'Is Your Cat Infected With a Computer Virus?' (pdf) leggen de onderzoekers uit op welke manieren een rfid-chip misbruikt zou kunnen worden.

Zo zou een chip kunnen worden geïnfecteerd met kwaadaardige code. Zodra deze chip vervolgens in bijvoorbeeld een distributiecentrum wordt uitgelezen, wordt in de rfid-chip verstopte sql-code uitgevoerd, waarna de achterliggende database gecompromitteerd is.

"Rfid-malware bedreigt een reeks applicaties", zo schrijven de onderzoekers in hun rapport. "Ontwikkelaars van rfid-systemen moeten hun systemen beschermen om de schade te beperken als hackers op grotere schaal met rfid-exploits, rfid-wormen en rfid-virussen gaan experimenteren."

"Als je de code op een website publiceert, schieten fabrikanten ineens in de stress", zegt Tanenbaum. "Dit zorgt er hopelijk voor dat ze het serieus nemen. Dit moet hen wakkerschudden voordat het op grote schaal wordt toegepast."

Meer informatie over rfid vindt u in de eerder deze week gepubliceerde bijlage 'Draadloos privacygevaar' of het 'Dossier rfid'.

14:37 : Reactie Tanenbaum toegevoegd