

Technologie toont haar kwetsbare zijde

door Dylan de Gruijl. donderdag 13 maart 2008 | 08:42 | Laatst bijgewerkt op: donderdag 13 maart 2008 | 08:43

Niet alleen de ov-chipkaart is gekraakt, ook de chip in toegangspasjes van gebouwen blijkt lek. „Verhoogde waakzaamheid is geboden. Je kunt altijd nog een portier bij gebouwen zetten.” De Duitse computerexpert Karsten Nohl maakt zich weinig illusies meer over de beveiliging van de ov-chipkaart en toegangspasjes voor tal van overheids- en bedrijfsgebouwen.

Nu de chip – de Mifare Classic – volledig is gekraakt, zijn beide 'extreem kwetsbaar' voor criminelen.

Het begon met zijn geruchtmakende ontdekking dat de 'sleutel' op de ov-chipkaart, die de strippenkaart en het treinkaartje moet vervangen, makkelijk is te achterhalen. Dat maakt de kans op zwartrijden een stuk groter.

Dat valt in het niet bij de ontdekking die de Radboud Universiteit gisteren presenteerde. De 'contactloze' toegangspasjes met diezelfde Mifare Classic-chip blijken lek. Bloedlink, oordeelt Nohl, werkzaam aan de Universiteit van Virginia (VS). " Wereldwijd is ruim een miljard kaarten met die chip in omloop, voor het openbaar vervoer en voor de toegang tot gebouwen waar bijvoorbeeld chemische spullen liggen en communicatie-installaties. Ik weet dat ook het Duitse leger pasjes met die chip heeft aangeschaft."

Voor een leek is het nauwelijks te bevatten. In een tijd waarin iedereen wel een chippas in zijn portemonnee heeft, staat de technologie ineens volop ter discussie. De Tweede Kamer, die gisteren een hoorzitting hield over de ov-chipkaart, vroeg zich gisteren af of elektronisch zakkenrollen nu een reëel gevaar is. Volgens TNO-onderzoeker Richard Kerkdijk, die de beveiliging van de ov-chipkaart onlangs tegen het licht hield, is dat zo simpel nog niet. Geld stelen voor eigen gebruik is onmogelijk, maar met de juiste apparatuur kan de elektronische portemonnee op de ov-chipkaart wel worden beïnvloed. " Het is mogelijk geld te verwijderen of het saldo te verlagen", aldus Kerkdijk. "Dat noemen we vandalisme."

TranksLink Systems (TLS) heeft al besloten over twee jaar een betere – en duurdere – chip in de kaart te zetten. In de tussentijd zou de kans op grootschalige fraude – lees: zwartrijden – klein zijn. Zo beschikt de ov-chipkaart over een extra code, die niet is gekraakt. Ook spoort het systeem een gekopieerde kaart altijd binnen twee dagen op. De reiziger, zo benadrukt TLS, wordt schadeloos gesteld.

Of dat genoeg is, betwijfelt Marc Witteman, die met zijn bedrijf Riscure chipkaarten test. Hij heeft een advies: stap zo snel mogelijk over op een veiliger chip. "De beveiliging is nu zo ver afgebroken dat die niet veel meer voorstelt. Misschien had TLS al veel eerder voor een andere chip moeten kiezen. Dat had eenvoudig gekund." Ook Witteman ziet het gedoe rond de ov-chipkaart als een kleinigheid. Het echte gevaar zit bij de toegangspasjes. Die hebben niet de extra beveiligingslagen van de ov-chipkaart en zijn dus veel kwetsbaarder. " Verhoogde waakzaamheid is geboden. Je kunt altijd nog een portier bij gebouwen zetten."

Chipfabrikant NXP wijst erop dat nieuwe, veilige generatie verkrijgbaar is. Die kost wel een paar cent extra. Voor miljoenen toegangspassen en ov-chipkaarten loopt dat al snel in de miljoenen euro's.