Toegangspasjes gekraakt

door Michiel Willems. donderdag 13 maart 2008 | 08:42 | Laatst bijgewerkt op: donderdag 13 maart 2008 | 10:57

NIJMEGEN - Vele miljoenen toegangspasjes voor de beveiliging van overheids- en bedrijfsgebouwen, militaire terreinen en panden van particuliere organisaties zijn eenvoudig na te maken.

Daardoor is het mogelijk onder een gestolen identiteit ergens binnen te komen. Een onderzoeksgroep van de Radboud Universiteit Nijmegen heeft gisteren bekendgemaakt de chip te hebben gekraakt die toegang geeft tot veel beveiligde gebouwen van de overheid.

Omdat de staatsveiligheid in het geding is, hebben de onderzoekers vrijdag minister Ter Horst van Binnenlandse Zaken geïnformeerd. Zij heeft zaterdag direct medewerkers van de veiligheidsdienst AIVD naar Nijmegen gestuurd, die hebben vastgesteld dat de methode werkt. Op zondag is producent NXP (voorheen Philips Semiconductors) gewaarschuwd. De Tweede Kamer is gistermiddag op de hoogte gebracht. Alle ministers is verzocht maatregelen te nemen om de beveiliging van overheidsgebouwen, waaronder gevangenissen en militaire terreinen, te garanderen. Hoogleraar computerbeveiliging Bart Jacobs van de Radboud Universiteit zei gisteren dat sprake is van een acuut veiligheidsprobleem. De publicatie van het onderzoek met alle details over de werkwijze van de studenten is om die reden voorlopig opgeschort. Onderzoeksleiders en studenten communiceren al geruime tijd in het diepste geheim over hun onderzoek.

Jacobs: "Ze beschikken over explosieve informatie.
Nadat duidelijk was dat grote belangen in het geding waren, heeft de onderzoeksgroep in volledige afzondering gewerkt. Als informatie zou uitlekken, zou misbruik eenvoudig zijn, met wellicht grote gevolgen. Als wij de chip relatief eenvoudig kunnen kraken, kunnen anderen dat ook."

In Nederland zijn twee miljoen toegangspasjes van overheidsgebouwen met de onveilige chip in omloop. Een veelvoud is verwerkt in pasjes van allerlei particuliere bedrijven en organisaties. Wereldwijd heeft de fabrikant van de chip, het Nijmeegse NXP, meer dan één miljard exemplaren verkocht.

Studenten van de onderzoeksgroep Digital Security van de Radboud Universiteit demonstreerden gisteren dat met een apparaatje ter grootte van een pakje sigaretten de informatie op elk toegangspasje kan worden gelezen en opgeslagen zonder dat de pashouder het in de gaten heeft. Het lezen van het pasje gebeurt in het voorbijgaan, zonder dat er contact is met de pashouder. Vervolgens kan met de afgetapte informatie vrij eenvoudig een pasje worden nagemaakt. De onderzoekers, die eerder aantoonden dat de ov-chipkaart slecht beveiligd is, zijn er ook in geslaagd de informatie af te tappen die is opgeslagen in pasjeslezers bij toegangsdeuren.

Het beveiligingslek treft ook de nieuwe ov-chipkaart, maar de Nijmeegse studenten hebben die niet gekraakt. Hoogleraar Jacobs vindt dat de ontcijfering van miljoenen toegangspassen het probleem van de gekraakte ov-chipkaart tot een bijzaak maakt.

Vanwege de grote veiligheidsbelangen is de Radboud Universiteit gisteren bewust afgeweken van de gebruikelijke procedure dat resultaten van wetenschappelijk onderzoek pas naar buiten komen na publicatie in vakliteratuur.

De voorzitter van het college van bestuur, ir. R. de Wijkerslooth de Weerdesteyn: "Het was al snel duidelijk dat de ontdekking verstrekkende gevolgen had en dat de overheid tijdig moest worden ingelicht. Dat hebben we gedaan om te voorkomen dat kwaadwillenden misbruik van de siutatie zouden maken."

In een reactie liet producent NXP gisteravond weten het kraken van de chip, de 'Mifare Classic' heel vervelend te vinden. "Onze producten zullen altijd het doelwit van hackers zijn. Maar het hangt van de aanvullende beveiliging van de pasjes af of misbruik ook echt mogelijk is."