Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2007–2008

31 200 VII Vaststelling van de begrotingsstaten van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (VII) voor het jaar 2008

Nr. 74

BRIEF VAN DE MINISTER VAN BINNENLANDSE ZAKEN EN KONINKRIJKSRELATIES

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 11 juli 2008

Op 19 maart 2008 heeft een Algemeen Overleg (AO) (31 200 VII, nr. 57) met de vaste kamercommissie van BZK plaatsgevonden over chiptechnologie van toegangspassen. Naar aanleiding van dit AO heeft uw Kamer gevraagd om een nadere toelichting op een aantal punten:
– eerdere signalen over risico's van chiptechnologie van toegangspassen;
– de invoering van de rijkspas;
– verder onderzoek van de AIVD naar chiptechnologie van toegangspassen;
– aansprakelijkheid.
Met deze brief informeer ik u achtereenvolgens over bovenstaande punten.

Signalen over risico's toegangspassen

In het algemeen geldt dat producten die gebruikt worden ter bescherming van waardevolle belangen in de belangstelling staan. Vanuit maatschappelijke betrokkenheid, criminele drijfveren of wetenschappelijke interesse wordt de «sterkte» van dit soort producten getoetst. In het geval van de Mifare Classic chip geldt dit ook.

De eerste signalen over het kraken van de Mifare Classic chip zijn er in *december 2007*. De Duitse hackers Nohl en Plötz maken bekend dat ze de werking van de Mifare Classic chip deels hebben blootgelegd, maar de «sleutels» van de kaart nog niet te hebben gevonden. Naar aanleiding van deze bevindingen besluiten de beveiligingsambtenaren van de verschillend ministeries om de ontwikkelingen nauwgezet te monitoren. De aandacht in de media gaat op dat moment vooral uit naar het gebruik van de chip in de OV-kaart.

In *januari 2008* verschijnt een rapport van TNO naar de risico's als gevolg van het bericht van de Duitse hackers Nohl en Plötz. De claims van Nohl

KST121257
0708tkkst31200VII-74
ISSN 0921 - 7371
Sdu Uitgevers
's-Gravenhage 2008

en Plötz worden grotendeels onderschreven. TNO schat in dat de feitelijke kraak van de chip(kaart) op een termijn van zes maanden moet worden verwacht (echter alleen met relatief veel moeite en dure apparatuur). Naar aanleiding van o.a. het rapport van TNO heb ik GOVCERT.nl (de Nederlandse ICT emergency-response organisatie) opdracht gegeven om een eigen analyse en rapportage op te stellen. Deze is eind januari opgeleverd en onder de beveiligingsambtenaren (BVA's) van de ministeries verspreid.

Vrijdag *7 maart 2008* is binnen de rijksoverheid voor het eerst bekend geworden dat een studiegroep van de Radboud Universiteit te Nijmegen er in is geslaagd een methode te ontwikkelen waarmee de Mifare Classic chip, met gebruikmaking van breed verkrijgbare commerciële producten en tegen geringe kosten, relatief eenvoudig te kraken is.
Vervolgens heb ik verschillende acties ondernomen:

- Zaterdag 8 maart 2008 is een delegatie van de AIVD (Nationaal Bureau voor Verbindingsbeveiliging (NBV)) afgereisd naar Nijmegen. De onderzoeksresultaten worden gestaafd, een kraak is klaarblijkelijk met eenvoudige middelen mogelijk.
- Maandag 10 maart 2008 wordt een (interne) «taskforce» ingericht om alle aspecten in kaart te brengen en (vervolg)acties te bespreken.
- Woensdag 12 maart 2008 is een (informerende) brief gestuurd aan de Tweede Kamer.
- Donderdag 13 maart 2008 worden alle Secretarissen-generaal middels een brief geïnformeerd over mogelijk te nemen maatregelen.
- Maandag 17 maart 2008 krijgen alle BVA's van de ministeries ter informatie een uitgebreide lijst met mogelijk te nemen maatregelen.
- Kort na het AO van 19 maart 2008 hebben alle gemeenten, provincies en vitale sectoren een brief van mij ontvangen waarin ze zijn geïnformeerd over het probleem met de Mifare Classic chip en mogelijk te nemen maatregelen.

Invoering Rijkspas

Het programma Rijkspas is er op gericht om op een veilige manier toegang tot rijksoverheidsorganisaties te realiseren. Hierbij is het van belang om verschillende componenten van de Rijkspas zoals infrastructuur, toegangskaart en chiptechnologie in samenhang te ontwikkelen. Dit vereist goede procesafspraken. Om e.e.a. goed te laten verlopen zijn strikte controles ingebouwd middels audit programma's en (monitorings)processen (vooraf en achteraf).
In gezamenlijkheid met het programma Defensiepas heeft het programma Rijkspas aan TNO en PricewaterhouseCoopers (in combinatie met Universiteit van Nijmegen) opdracht verleend om met aanbevelingen te komen ten aanzien van het gebruik van chip(s) op de Rijkspas.

Het interdepartementale programma Rijkspas kan worden verbreed. Dit betekent dat het aantal deelnemers en de mogelijke toepassingen gefaseerd ingevoerd en uitgebreid kunnen worden.
Hierbij is het van belang dat toetredende organisaties voldoen aan vooraf afgesproken normenkaders. De uiteindelijke toegangspas zal zijn voorzien van het nieuwe Rijkslogo en uitgerust zijn met «echtheidskenmerken» ten behoeve van authenticatie en identificatie.

Het programma Rijkspas heeft maximaal gebruik gemaakt van de aanwezige ervaring en kennis van het programma Defensiepas. Dit is in lijn met aanbevelingen uit onderzoek naar de mogelijkheden van introductie van één rijksbrede toegangspas voor alle rijksoverheid medewerkers (d.d. januari 2007). Daar waar mogelijk maakt het programma Rijkspas gebruik van industriestandaarden om toekomstbestendigheid te optimaliseren en/of beheerskosten te minimaliseren. Vanwege de diversiteit aan deelne-

mers is gekozen voor een model waarbij bestaande «mandaatregelingen» niet worden aangetast. Met andere woorden iedere organisatie beslist uiteindelijk zelf wie er toegang tot zijn of haar organisatie heeft/krijgt.

Omdat het programma Defensiepas en het programma Rijkspas gebaseerd zijn op vrijwel dezelfde normenkaders, is de intentie uitgesproken dat beide programma's op termijn naar één pasprogramma zullen migreren. N.a.v. de ontwikkelingen van de afgelopen maanden heeft het ministerie van Defensie aangegeven dit migratieproces mogelijk te versnellen. Het besluit ten aanzien van een mogelijke uitrol van de Defensiepas is tot juli 2008 opgeschort.

Het programma Rijkspas zal in het laatste kwartaal van 2008 worden ingevoerd. Hierbij zijn de volgende stappen te onderscheiden:
- mei 2008: uitkomst onderzoek Contactloze chip;
- juli 2008: besluitvorming contactloze chip;
- oktober 2008: opdracht productie Rijkspas;
- 4e kwartaal 2008: uitrol éérste Rijkspas.

Afgesproken is dat de Haagse kerndepartementen (met uitzondering van Defensie) participeren in de eerste fase van het programma Rijkspas. De invoering van Rijkspas bestaat (opeenvolgend) uit drie fasen:
1. fysieke departementale toegang;
2. fysieke interdepartementale toegang;
3. andere applicaties (bijvoorbeeld toegang tot netwerken).

Andere partijen binnen de rijksoverheid die recentelijk interesse hebben getoond om mogelijk te gaan participeren in het programma Rijkspas zijn: de justitie keten, de Tweede Kamer en de belastingdienst.

Onderzoek AIVD

Het NBV van de AIVD heeft nader onderzoek gedaan naar de gevolgen van de kraak van de Mifare Classic chip voor de toegangsbeveiliging van ministeries.
Om op korte termijn de dreiging van het zich ongeautoriseerd toegang verschaffen tot ministeries te verminderen is het nodig de toegangsbeveiliging in zijn geheel te beschouwen. De Mifare Classic chip is daarin slechts een onderdeel. Onderzoek door de AIVD naar deze systemen wijst uit dat het mogelijk is om de «weerstand» te vergroten door het nemen van maatregelen op organisatorisch en/of technisch vlak. De verschillende ministeries zijn op de hoogte gebracht van mogelijke maatregelen die zij kunnen nemen.
Daarnaast heeft het onderzoek uitgewezen dat het, op de langere termijn, noodzakelijk is over te gaan op een andere chip als basis voor de toegangsbeveiliging. Dit wordt gedaan met de invoering van de nieuwe Rijkspas.

De beveiliging van toegangspassen is primair de verantwoordelijkheid van afzonderlijke ministeries. Tot op heden was dit niet de taak van de AIVD. De AIVD adviseert de rijksoverheid ter bevordering van de beveiliging van bijzondere informatie (Staatsgeheim gerubriceerd of Departementaal Vertrouwelijk). Echter, omdat is gebleken dat er behoefte is aan een centrale organisatie binnen de rijksoverheid waar advies kan worden ingewonnen over de beveiliging van gevoelige informatie die niet tot het domein van de bijzondere informatie behoort, heeft de AIVD een voorstel uitgewerkt voor uitbreiding van haar takenpakket. Dit voorstel wordt ter besluitvorming voorgelegd aan het kabinet.

Aansprakelijkheid

In april hebben verschillende gesprekken plaatsgevonden tussen de chipfabrikant van de Mifare Classic Chip en mijn ministerie. Uit deze gesprekken is gebleken dat de chipfabrikant een eerste schakel is in een keten. De chipfabrikant levert chips aan derden (geen passen), die deze samen met andere halffabricaten verwerken tot een (toegangs)pas. Uiteindelijk is er dan één leverancier die de pas (aan een ministerie) levert (al dan niet via de leverancier van het totale toegangscontrolesysteem). Er is dus geen contract tussen de ministeries en de chipfabrikant op basis waarvan de ministeries de chipfabrikant contractueel zouden kunnen aanspreken (nog los van de vraag of een contract daar wel grondslag voor biedt – zie onder).

In bepaalde gevallen is het echter mogelijk een producent (zoals de chipfabrikant) van een gebrekkig product, zonder een contract op grond van de wet, rechtstreeks aan te spreken (wettelijke bepalingen m.b.t. *Productaansprakelijkheid*). In dit geval is dat juridisch niet haalbaar omdat zelfs indien de toegangspas een gebrek vertoont in de zin van artikel 6:186 van het Burgerlijk Wetboek, er niet aan de voorwaarden is voldaan van Afdeling 3, *Productenaansprakelijkheid,* van het Burgerlijk Wetboek.

Als laatste merk ik op dat ook voor contractuele aansprakelijkheid van de leverancier(s) niet of nauwelijks enige grond bestaat. Voor zover het de ministeries van Justitie en BZK aangaat, is de oorspronkelijke toegangspas midden jaren negentig geleverd in het kader van een RisicoBeheerSysteem (RBS). De toegangspas van de oorspronkelijke leverancier van RBS is later vervangen door een toegangspas met de Mifare Classic Chip. Uit de verslagen die betrekking hebben op deze vervanging blijkt niet dat het aspect «onkraakbaar» enige rol heeft gespeeld en dat ter zake (contractuele) garanties zouden zijn afgegeven door de leverancier(s).

Gelet op de geringe kans van slagen van een aansprakelijkheidsactie en gegeven het feit dat er tot op heden geen materiële schade van betekenis is geleden, is er geen aanleiding de chipfabrikant of de leverancier(s) van de toegangspassen aansprakelijk te stellen.

De minister van Binnenlandse Zaken en Koninkrijksrelaties,
G. ter Horst