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. 57

VERSLAG VAN EEN ALGEMEEN OVERLEG

Vastgesteld 18 april 2008

De vaste commissie voor Binnenlandse Zaken en Koninkrijksrelaties[1] heeft op 19 maart 2008 overleg gevoerd met minister Ter Horst van Binnenlandse Zaken en Koninkrijksrelaties over:

– **de brief van de minister over chiptechnologie (toegangs-) passen d.d. 12 maart 2008 (31 200-VII, nr. 50).**

Van dit overleg brengt de commissie bijgaand beknopt verslag uit.

Vragen en opmerkingen uit de commissie

Mevrouw **Gerkens** (SP) vindt dat bij een nieuwe chip gekozen moet worden voor een bewezen veilig concept met een open standaard en niet voor een chip die als beveiliging geheimhouding heeft.

– De beveiliging van systemen berust op een totaalplaatje. Als één schakel niet te vertrouwen is, is de hele keten kwetsbaar geworden. Welke aanvullende maatregelen zijn inmiddels getroffen?
– Heeft de minister wat de betrouwbaarheid van RFID-chips betreft aldoor vertrouwd op het oordeel van leveranciers? Kunnen zij aansprakelijk worden gesteld?
– Hebben experts nooit alarm geslagen over de gebrekkige beveiliging van de chip? Hoe is het mogelijk dat TNO de passen voldoende beveiligd achtte?

De heer **Hessels** (CDA) zegt dat nieuwe technologieën in de veiligheid altijd moeten samengaan met menselijk handelen. Hij vraagt of de beveiliging van overheidsgebouwen gegarandeerd is als de systemen uitvallen.

– Het kraken van de RFID-chip in de toegangspassen wijst erop dat de overheid op achterstand is gezet. De versleuteling van de codes moet zo snel mogelijk op een hoger peil worden gebracht. Kan dat met de bestaande passen? Zo nee, welke kosten zijn gemoeid met vervanging en op welke termijn kan dat gerealiseerd worden? Welke maatregelen worden in de tussentijd genomen? Wist de minister dat de chip gekraakt kon worden? Welke afspraken zijn bij levering gemaakt?
– Een goede controle op fysieke eigenschappen, bijvoorbeeld via een irisscan, lijkt noodzakelijk. Welke lessen worden geleerd uit andere sectoren en andere landen?
– Wat is de stand van zaken rond het onderzoek van de AIVD? Is de

[1] Samenstelling:
Leden: Van Beek (VVD), Van der Staaij (SGP), De Pater-van der Meer (CDA), Van Bochove (CDA), Duyvendak (GroenLinks), Hessels (CDA), Gerkens (SP), Haverkamp (CDA), Leerdam (PvdA), voorzitter, De Krom (VVD), ondervoorzitter, Griffith (VVD), Boelhouwer (PvdA), Irrgang (SP), Kalma (PvdA), Schinkelshoek (CDA), Van der Burg (VVD), Brinkman (PVV), Pechtold (D66), Van Raak (SP), Thieme (PvdD), Kuiken (PvdA), Leijten (SP), Heijnen (PvdA), Bilder (CDA) en Anker (ChristenUnie).
Plv. leden: Teeven (VVD), Van der Vlies (SGP), Van de Camp (CDA), Smilde (CDA), Van Gent (GroenLinks), Knops (CDA), Polderman (SP), Spies (CDA), Wolbert (PvdA), Aptroot (VVD), Zijlstra (VVD), Vermeij (PvdA), Van Gerven (SP), Heerts (PvdA), Çörüz (CDA), Remkes (VVD), De Roon (PVV), Van der Ham (D66), Van Bommel (SP), Ouwehand (PvdD), Timmer (PvdA), De Wit (SP), Kraneveldt-van der Veen (PvdA), Van Haersma Buma (CDA) en Cramer (ChristenUnie).

KST117604
0708tkkst31200VII-57
ISSN 0921 - 7371
Sdu Uitgevers
's-Gravenhage 2008

dienst voldoende toegerust om deze technische analyse te maken? Worden de hackers betrokken bij het dichten van de gaten in het systeem?
– Hoe zal de overheid reageren als de precieze handelwijze van de groep van de Radboud Universiteit direct gepubliceerd wordt?

De heer **Brinkman** (PVV) maakt zich na de kraak van de toegangspassen zorgen over de veiligheid in het Tweede Kamergebouw. Wat heeft de minister gedaan om overheidsgebouwen extra te beveiligen? Moet in de beveiliging de menselijke component niet worden versterkt? Wordt gedacht over de invoering van een irisscan?
– Is de minister van mening dat voldoende aanvullende maatregelen zijn genomen? Zijn er nog zwakke schakels? Is de minister op de hoogte van de details van de bevindingen van de Radboud Universiteit? Heeft het onderzoek van de AIVD al tot enig resultaat geleid? Worden nieuwe systemen in dit onderzoek meegenomen?
– Bij de toepassing van een nieuwe chip dient de minister de voorwaarde te stellen dat het product minimaal een bepaalde periode veiligheid biedt.

Mevrouw **Van der Burg** (VVD) vraagt naar de precieze omvang van het probleem en de extra maatregelen die inmiddels zijn genomen. Ook is zij benieuwd naar de kosten van de overbruggingsmaatregelen en het versneld invoeren van de rijkspas.
– De indruk bestaat dat de communicatie niet goed geregeld is. Mensen die verantwoordelijk zijn voor de veiligheid van gebouwen, weten niet altijd waar zij terechtkunnen.
– Wat zijn de privacyrisico's wanneer de op een pas opgeslagen gegevens gekraakt kunnen worden?
– Heeft intercollegiaal en internationaal contact plaatsgehad over de recente ontwikkelingen en worden in dat kader mogelijke maatregelen besproken?
– Afgelopen zomer werd al duidelijk dat de Mifare Classic-chip te kraken is. Heeft de minister toen al stappen ondernomen? Heeft het kraken van de ov-chipkaart, die additioneel beveiligd was, bij de minister de alarmbel doen rinkelen?

Mevrouw **Kuiken** (PvdA) wil dat de overheid de krakers uitnodigt om uit te zoeken waar de systemen tekortschieten. Een chip is slechts een onderdeel van de noodzakelijke veiligheidsmaatregelen. Om het totale systeem te controleren, is het wenselijk om af en toe een mystery guest in te zetten.
– De vraag of een nieuwe chip een open standaard moet hebben, dient door deskundigen te worden beantwoord.
– Is er al misbruik gemaakt van gekraakte toegangspassen?

De heer **Anker** (ChristenUnie) heeft het idee dat de overheid op het punt van ICT vaak achter de feiten aanloopt. Er had eerder op de veiligheidsaspecten van de chip kunnen worden ingegaan. De komende tijd moet getracht worden voorop te blijven lopen. De overheid moet met behulp van professionals actief sturen op dit proces.
– Wat zijn de risico's van het komende biometrisch paspoort?
– Wanneer is het AIVD-onderzoek gereed? Welke risico's worden in de tussentijd gelopen?
– Veiliger chips zijn duurder. Welk begrotingsconsequenties ziet de minister?

De heer **Duyvendak** (GroenLinks) denkt dat de overheid naïef is geweest over de veiligheid en vraagt de minister welke les uit het kraken van de chip is getrokken.

– Hoe serieus is het probleem met de passen, mede in relatie tot de problemen rond de ov-chipkaart?
– Wat zijn de gevolgen als de Radboud Universiteit het resultaat van het onderzoek bekendmaakt? Hoe zal grootschalig misbruik worden voorkomen?
– Een beperkt aantal ambtenaren zal in de toekomst met de rijkspas gaan werken. Welke maatregelen worden getroffen voor de andere ambtenaren?
– Er moet voor de toekomst worden gekozen voor een chip met open standaard.

Antwoord van de minister

De **minister** zegt dat er geen acute risico's zijn zolang de details van het onderzoek van de Radboud Universiteit niet naar buiten zijn gebracht. Op het moment dat dat wel gebeurt, vermoedelijk over een aantal maanden, zullen de gegevens op een toegangspas vrij gemakkelijk gekopieerd kunnen worden. Alle instanties die gebruikmaken van dit soort passen, zijn inmiddels op de hoogte gesteld van de problemen.
– Het feit dat de chip is gekraakt, is binnenslands en buitenslands bekendgemaakt. Elke organisatie is verantwoordelijk voor haar eigen beveiliging, maar de minister voelde het als haar verantwoordelijkheid om de kraak te melden.
– Na de problemen met de ov-chipkaart is interdepartementaal over de risico's gesproken. Desalniettemin wekte het begin maart verbazing dat de informatie van de toegangspassen zo eenvoudig gekopieerd kon worden. Op 7 maart maakte de Radboud Universiteit bekend dat medewerkers erin geslaagd waren, passen te dupliceren. Op 8 maart ging een delegatie van de AIVD naar Nijmegen en op 10 maart is een taskforce ingesteld om informatie over de kraak te verspreiden. Als blijkt dat eerder signalen zijn afgegeven, zal de Kamer daarover worden geïnformeerd.
– Er is een lijst opgesteld van mogelijke aanvullende maatregelen. Op het ministerie van BZK wordt inmiddels gecontroleerd of de foto op de pas correspondeert met de drager ervan. Daarnaast moeten de medewerkers zich bewust zijn van het belang om de pas zichtbaar te dragen. Ook moeten zij onderkennen dat er vertrouwelijke informatie op de pas is opgeslagen.
– De getroffen extra maatregelen zijn tijdelijk. In het derde of vierde kwartaal van 2008 zal met nieuwe passen kunnen worden gewerkt. De extra beveiligingskosten, waarvan de hoogte moeilijk is te schatten, zullen dan niet meer noodzakelijk zijn.
– De beveiligingssoftware van de chip bestaat uit een wiskundige formule en één of meer elektronische sleutels. De beveiliging is sterker als het algoritme ingewikkelder en de sleutel langer is. De chip die gekraakt is, kent een eenvoudig algoritme en een korte sleutel.
– Het ligt niet in het voornemen om het bedrijf dat de chip heeft geleverd, aansprakelijk te stellen voor de gevolgen van de kraak. Als de leveringsvoorwaarden daartoe wel ruimte bieden, zal de regering niet schromen er gebruik van te maken en de Kamer daarover in te lichten. Het is echter te makkelijk om met de kennis van nu te zeggen dat de chip, die tien jaar geleden ontwikkeld is, onveilig is. Daarnaast is een chip slechts een onderdeel van de totale beveiliging. Op de nieuwe rijkspas zal de chip voldoen aan de hedendaagse eisen, maar ook die chip zal op termijn gekraakt kunnen worden. Organisaties die geen gebruik gaan maken van de rijkspas, zijn zelf verantwoordelijk voor het nemen van veiligheidsmaatregelen.
– Vijf departementen maken gebruik van de gekraakte technologie. Een aantal andere departementen maakt er voor de indirecte toegang gebruik van.

– De AIVD herbergt het Nationaal bureau voor verbindingsbeveiliging, dat de expertise bevat om het onderzoek te verrichten. Bij de beoordeling van de kwestie wordt een aantal organisaties, waaronder TNO, betrokken. Als de indruk bestaat dat het kennisniveau te laag is, zal de kennis worden ingekocht. De AIVD kan benaderd worden voor informatie en suggesties voor beschermingsmaatregelen. Op de website van het ministerie zal een verwijzing worden opgenomen.
– De AIVD zal samen met NXP, de producent van de chip, nagaan of technische verbeteringen van de chip mogelijk zijn. Daarnaast zal de dienst, in samenwerking met TNO, de AIVD, PWC en de Radboud Universiteit de voorziene beveiliging van de rijkspas onderzoeken. Om de drie jaar zal een assessment plaatsvinden. De technologieontwikkelingen zullen permanent worden gemonitord. Als de onderzoeken gereed zijn, zal de Kamer daarover worden ingelicht. Voor de nieuwe chip moet een technologie worden gekozen die de risico's zo klein mogelijk maakt. Of dat een technologie met open standaard is, moet door deskundigen worden uitgemaakt.
– Om de integrale beveiliging te testen, verdient het idee van de mystery guest zeker overweging. Op sommige departementen wordt het al toegepast.
– Het aantal persoonsgegevens op de gekraakte passen is beperkt.
– In de Nederlandse reisdocumenten wordt een andere chip toegepast. Er is geen enkele indicatie dat de beveiliging van die chip in gevaar zou zijn. Door het ministerie van BZK wordt met de Radboud Universiteit samengewerkt om dreiging in dat opzicht in de gaten te houden.

Toezeggingen

– De Kamer zal worden bericht over onderzoeken van de AIVD, zodra de planning daarvan bekend is.
– De Kamer zal worden geïnformeerd over eventuele eerdere signalen over de risico's van de huidige technologie in (toegangs)passen.
– De Kamer zal op de hoogte worden gehouden van de invoering van de rijkspas, inclusief de gekozen systematiek.
– De Kamer zal bericht ontvangen over de aansprakelijkheidskwesties.

De voorzitter van de vaste commissie voor Binnenlandse Zaken en Koninkrijksrelaties,
Leerdam

De griffier van de vaste commissie voor Binnenlandse Zaken en Koninkrijksrelaties,
Van Leiden