Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2012–2013

26 643 Informatie- en communicatietechnologie (ICT)

Nr. 275

VERSLAG VAN EEN ALGEMEEN OVERLEG

Vastgesteld 15 mei 2013

De vaste commissie voor Binnenlandse Zaken heeft op 27 maart 2013 overleg gevoerd met minister Plasterk van Binnenlandse Zaken en Koninkrijksrelaties over:

- **de brief van de minister van Binnenlandse Zaken en Koninkrijksrelaties d.d. 28 juni 2012 over de uitvoering van de motie van de leden Gesthuizen en El Fassed (Kamerstuk 26 643, nr. 238) over een ICT-beveiligingsassessment voor DigiD (Kamerstuk 26 643, nr. 242);**
- **de brief van de minister van Binnenlandse Zaken en Koninkrijksrelaties d.d. 30 oktober 2012 over de stand van zaken met betrekking tot de ICT-beveiligingsassessments DigiD (Kamerstuk 26 643, nr. 256);**
- **de brief van de minister van Binnenlandse Zaken en Koninkrijksrelaties d.d. 12 november 2012 met een reactie op het onderzoeksrapport van de Onderzoeksraad Voor Veiligheid inzake «Het DigiNotar-incident, waarom digitale veiligheid de bestuurstafel te weinig bereikt» (Kamerstuk 26 643 nr. 257);**
- **de brief van de minister van Binnenlandse Zaken en Koninkrijksrelaties d.d. 27 februari 2013 inzake een toezegging verslag evaluatie calamiteit DigiD op 9 januari jl. (Kamerstuk 26 643, nr. 267);**
- **de brief van de minister van Binnenlandse Zaken en Koninkrijksrelaties d.d. 22 maart 2013 over de stand van zaken inzake ICT beveiligingsassessments en Taskforce Bestuur en informatieveiligheid Dienstverlening (Kamerstuk 26 643, nr. 269).**

Van dit overleg brengt de commissie bijgaand geredigeerd woordelijk verslag uit.

De voorzitter van de vaste commissie voor Binnenlandse Zaken,
Berndsen-Jansen

De griffier van de vaste commissie voor Binnenlandse Zaken,
Van der Leeden

kst-26643-275
ISSN 0921 - 7371
's-Gravenhage 2013

Voorzitter: Van der Linde
Griffier: Hendrickx

Aanwezig zijn vier leden der Kamer, te weten: Gesthuizen, Van der Linde, Oosenbrug en Verhoeven,

en minister Plasterk van Binnenlandse Zaken en Koninkrijksrelaties, die vergezeld is van enkele ambtenaren van zijn ministerie.

Aanvang 12.30 uur

De **voorzitter**: In dit algemeen overleg over beveiligingsaspecten en ICT zijn vijf brieven aan de orde die samenhangen met de veiligheid van DigiD. Ik heet de minister van Binnenlandse Zaken en zijn medewerkers welkom. Ik stel voor, een spreektijd te hanteren van vier à vijf minuten. Voor de goede orde merk ik op dat ik als laatste spreker namens de VVD het woord zal voeren. Het voorzitterschap zal ik dan aan een collega overdragen.

Mevrouw **Gesthuizen** (SP): Voorzitter. Vandaag staat een aantal belangrijke punten op de agenda. Ik begin met een mooi citaat van deze minister: «Don't try this at home.» Hij sprak toen over hackers die met hun kunst- en vliegwerk de overheid of bedrijven kunnen helpen om de boel beter te beveiligen tegen criminelen en tegen mensen die via cybercrime anderen het geld uit de zak willen kloppen. Dat is hartstikke goed. Hacken is natuurlijk nog wel strafbaar, maar minister Opstelten onderzoekt of ethische hackers die lekken opsporen om de beveiliging te verbeteren, meer ruimte kunnen krijgen om te hacken. In hetzelfde artikel in De Telegraaf viel mij een ander citaat op, van een tweedejaarsstudent. Hij zei geen heil te zien in een eventuele verruiming in de wet: «Ik heb liever dat een hacker mij vooraf vraagt of hij mijn server moet controleren, dan dat ik ongevraagd achteraf een lijst met lekken krijg.» Ik zou daar graag een reactie van de minister op vernemen. Dit punt wordt de komende jaren natuurlijk steeds belangrijker.
Op NU.nl van 24 maart werden de complimenten voor de overheid uitgesproken omdat zij steeds meer grip heeft op ICT-beveiligingsproblemen. Dat vind ik uiteraard een positieve ontwikkeling. Ik vraag mij wel af hoe de minister het grote aantal fouten bij instanties gaat aanpakken dat relatief eenvoudig op te lossen is. 130 fouten van het in totaal ongeveer dubbele aantal fouten werden veroorzaakt door het gebruik van verouderde software of waren relatief eenvoudig te voorkomen programmeer- en instellingsfouten. Hoe kan het dat dergelijke fouten nog in veelvoud worden gemaakt?
De norm ICT-beveiligingsassessments DigiD is een selectie voor de belangrijkste DigiD-elementen uit het document ICT-beveiligingsrichtlijnen voor webapplicaties van het NCC (National CrisisCentrum). Het is erg goed dat dit er is. Vanwege het generieke belang en de individuele verantwoordelijkheid van de organisaties om de eigen ICT-beveiliging op orde te stellen, wordt organisaties uitdrukkelijk geadviseerd om bij het DigiD-gebruik de hele set van richtlijnen van het NCC toe te passen. Ik vraag mij af waarom zij slechts uitdrukkelijk worden geadviseerd. Is het niet verstandiger om dit te verplichten? Door het uitdrukkelijke advies geven wij wel aan dat het erg belangrijk is, maar waarom zetten wij niet dat laatste stapje en stellen wij het niet gewoon verplicht? Dan kunnen we mogelijk helpen als het niet gaat. Graag hoor ik hierop een reactie van de minister.
In de motie-Gesthuizen/El Fassed (26 643, nr. 242) wordt de regering verzocht om, in het belang van deze beveiliging en de ingrijpende gevolgen die gebreken in de beveiliging van DigiD kunnen hebben, te bewerkstelligen dat alle DigiD-gebruikende organisaties (nader) werk

maken van de veiligheid ervan en hiervoor eind 2012 een ICT-beveiligingsassessment laten uitvoeren. Dat is niet gelukt. Garandeert de minister dat in 2013 100% van de DigiD-gebruikende organisaties een beveiligingsassessment heeft uitgevoerd en dat 100% van de DigiD-transacties in een veilige en geteste omgeving plaatsvindt?
Het derde agendapunt betreft de reactie van het kabinet op het rapport van de Onderzoeksraad Voor Veiligheid over het grote DigiNotar-incident. Daar hebben we allemaal veel van geleerd. Uiteraard vinden wij het positief dat de minister van alles doet. Er komt ook een taskforce, maar mede gelet op hetgeen de Onderzoeksraad Voor Veiligheid nu precies heeft gezegd, vind ik een taskforce onvoldoende. Natuurlijk mag er een taskforce komen, maar ik vind het jammer dat de minister zegt dat, alhoewel hij wet- en regelgeving niet uitsluit, hij daartoe pas wil overgaan na een evaluatie. Ik heb alle rondetafelgesprekken en hoorzittingen bijgewoond die naar aanleiding van het DigiNotar-incident hebben plaatsgevonden. Ik heb er echt met kromme tenen gezeten omdat alle organisaties die daar aan tafel zaten – ik noem ook Pricewaterhouse-Coopers, OPTA – organisaties zijn die wij vertrouwden op het gebied van het toezicht. Geen van die organisaties heeft de verantwoordelijkheid genomen om ervoor te zorgen dat zij echt zeker wisten dat een en ander veilig was. Daarom heeft dit ook kunnen gebeuren. Er gebeurt natuurlijk wel al het nodige, onder andere bij OPTA en Logius, maar ik wil zien dat de minister wel regels opstelt en niet alleen met de taskforce aan de slag gaat. Als een meerderheid van de Kamer de minister daartoe oproept – zo te zien zijn wij hier met een meerderheid, de voorzitter meegerekend – wil ik overigens ook weten of dit valt onder de verantwoordelijkheid van Binnenlandse Zaken of van Veiligheid en Justitie.
Naar aanleiding van de derde aanbeveling – handhaving door OPTA en Logius; daar heeft de minister van alles in gang gezet – denk ik dat het een goed idee zou zijn als de commissie eens op werkbezoek zou gaan bij de OPTA om te zien hoe het nu allemaal goed functioneert.

Mevrouw **Oosenbrug** (PvdA): Voorzitter. De Partij van de Arbeid is er erg blij mee dat de minister tijdens zijn bezoek aan de Haagse Hogeschool zijn waardering uitsprak over het ethisch hacken. De Partij van de Arbeid heeft zich namelijk al eerder uitgesproken voor het gebruik van de kennis van ethische hackers om kwetsbaarheden in ICT-systemen op te sporen. Het Nationaal Cyber Security Centrum (NCSC) heeft inmiddels richtlijnen gepubliceerd voor responsible disclosure. Mijn fractie wil graag weten of de rijksoverheid zich aan deze richtlijn conformeert. Dan weten ethische hackers onder welke voorwaarden de rijksoverheid geen aangifte van de hack zal doen. Ook willen we de minister vragen om andere overheidsorganisaties te verzoeken duidelijkheid te geven over het hanteren van de richtlijn. Daarnaast doet de minister pogingen om computerdeskundigen en studenten te vragen actief kwetsbaarheden op te sporen. Kan de minister ons iets meer vertellen over de groepen die hiervoor worden benaderd en over de resultaten die dit tot nu toe heeft opgeleverd?
Wij complimenteren de minister met zijn aanpak van de kwetsbaarheid in het softwareplatform waar DigiD op gebouwd is. DigiD is een dag uit de lucht geweest opdat de software kon worden bijgewerkt. Hierbij ging het om de opensource-software waar de Partij van de Arbeid een voorstander van is. De opensource-software die werd gebruikt, Ruby on Rails (RoR), heeft een goede reputatie. Het was prettig om te zien dat de minister, toen hem de vraag werd gesteld, kon uitleggen dat het niet om een lek ging, maar om een kwetsbaarheid. Op het moment zelf is adequaat gereageerd op de kwetsbaarheid in het systeem. Dat is goed aangepakt. Ik vind het een goed voorbeeld waaruit blijkt hoe moet worden omgegaan met kwetsbaarheden in software en hoe deze uiteindelijk moeten worden aangepakt.

In het onderzoeksrapport van de Onderzoeksraad Voor Veiligheid wordt een aantal lessen getrokken. De minister heeft daarop een aantal maatregelen genomen. De beschrijving daarvan en de taskforce laten zien dat het toch wel een kluwen aan organisaties aan het worden is. Mijn fractie maakt zich enigszins zorgen over het feit dat we met een aantal verschillende organisaties te maken krijgen, terwijl we eigenlijk van mening zijn het dat Nationaal Cyber Security Centrum (NCSC) heel geschikt is om als coördinatiepunt op te treden. Ik wil graag weten hoe de minister daarover denkt.
Mijn collega Gesthuizen heeft al een aantal dingen genoemd; die zal ik niet herhalen.
Wij zouden graag zien dat het eenvoudiger wordt en dat een norm wordt gesteld. Door open te zijn op het moment dat zich een kwetsbaarheid uit, wek je meer vertrouwen. Ik zou graag zien dat deze lijn wordt voortgezet.

De heer **Verhoeven** (D66): Voorzitter. Vorige week omarmde de minister het idee van D66 om studenten onder toezicht te laten hacken om de kwaliteit van de overheidsbeveiliging te testen. Blijft dit nou bij een publiciteitsstunt of gaan we het echt doen? «Don't try this at home», heeft de minister blijkbaar gezegd. Ik zou zeggen: do try this, minister. Ga er echt mee aan de slag. Ik sluit mij overigens aan bij de opmerking die mijn collega in dit opzicht maakte over responsible disclosure.
Cybersecurity is goed vergelijkbaar met fietsen: je kunt alle sloten openbreken, maar een extra slot maakt het wel onaantrekkelijker om dat te proberen. Met de overheids-ICT is het net zo. Het extra slot moet dan wel extra sterk zijn omdat de potentiële schade, diefstal van een overheidsvehikel, veel groter is. Het gaat zelfs nog verder, want gemeenten hebben toegang tot het complete wagenpark van de rijksoverheid en werken ook met data van de burger. De verantwoordelijkheid is dan extra groot. Die verantwoordelijkheid moet naar onze mening overeind staan en blijven staan.
De eerste vraag bij het denken over veiligheid en ICT bij de overheid is dan ook of het überhaupt wel noodzakelijk is om bepaalde data op te slaan. Elke database kun je immers beschouwen als een cybersecurityrisico. Naar de mening van D66 moeten bij overheids-ICT altijd drie woorden centraal staan: beschikbaarheid, integriteit en vertrouwelijkheid. Dat zijn de drie basiselementen voor informatiebeveiliging. Dit leert een eerstejaarsstudent informatica. De minister, die ook wetenschapper is, moet dat toch wel aanspreken. Het lijkt mij dan ook wenselijk dat deze drie kernelementen de basis vormen voor afwegingen die de overheid maakt. Het NCSC doet dat, maar hoe zit het met de rest van de overheid? Moet niet ook politiek worden afgewogen welke van de drie kernelementen voorrang krijgt? Mijn partij ziet dat het element «beschikbaarheid» toch wel vaak voorrang krijgt boven de andere twee. Kan de minister dat bevestigen? Welke afspraken zijn hierover gemaakt met de andere, lagere overheden?
In de reactie van de minister op het onderzoeksrapport van de Onderzoeksraad Voor Veiligheid schrijft hij dat het aspect informatiebeveiliging moet worden betrokken bij het inrichten en onderhouden van informatiesystemen. Daarmee zijn wij het eens, maar wij vinden ook dat dit een rol moet spelen bij het bedenken, het in gang zetten en het inrichten van een datasysteem. Opnieuw moet «beschikbaarheid» daarbij niet blind voorrang krijgen. Ook integriteit en vertrouwelijkheid moeten gegarandeerd kunnen blijven. Kan de minister bevestigen dat hij deze redenering deelt en hier actief naar zal handelen?
Bij DigiNotar is er op een gegeven moment voor gekozen om beschikbaarheid voorrang te geven boven integriteit en vertrouwelijkheid. Mij is allesbehalve duidelijk hoe gelukkig die keuze is. De communicatie werd in stand gehouden om de dienstverlening in stand te houden terwijl de hele wereld wist dat deze communicatie niet veilig was. Microsoft stelde voor

de beschikbaarheid van Nederland zelfs een update uit. Hoe is dat afgedwongen? Ik krijg overigens nog steeds berichten die erop duiden dat dissidente Iraniërs hiervan het slachtoffer zijn geweest. Zij blijven communiceren via gekraakte certificaten van Nederland. Kan de minister daar wat meer informatie over verschaffen? Dat kan misschien in dit debat, maar anders mag de minister het ook schriftelijk afhandelen.
Bij het tijdig uit de lucht halen van DigiD is wel een goede keuze gemaakt. Een onbereikbare website is inderdaad heel vervelend, maar belangrijk is wel dat op dat moment niet de beschikbaarheid van de dienstverlening, maar de veiligheid vooropstond. Dat vinden wij een goede manier van redeneren.
Tot slot ga ik in op het vertrouwen in de lokale overheden. De minister heeft een taskforce ingesteld. Ik ben het met mevrouw Oosenbrug eens dat het wel heel erg lijkt op een kluwen van allerlei organisaties. Het versnipperen van de vindplaatsen van informatie vind ik wel een goede gedachte, want dat vergroot de veiligheid, maar het versnipperen van de beveiliging vind ik niet zo slim. Die zou je juist moeten bundelen. Graag hoor ik hoe de minister hiertegenover staat.
Wij gaan niet mee met hetgeen de minister schrijft in zijn brief van 22 maart 2013: «Iedere overheidslaag is en blijft zelf verantwoordelijk voor het op orde krijgen en houden van haar informatieveiligheid en om te komen tot die verplichtende zelfregulering.» Alle overheidslagen maken immers gebruik van gedeelde informatiesystemen, zoals DigiD en de gemeentelijke basisadministratie. De beveiligingszwakte van hen is dan ook de zwakte van andere overheden. Het is net een ketting waarvan de sterkte wordt bepaald door de zwakste schakel.
Indien centraal diensten worden afgenomen, is wel degelijk meer centrale sturing nodig. Ik stel voor om hierbij als eerste stap twee elementen te betrekken: stel een responsible disclosure verplicht bij alle gemeenten en zorg voor aansluiting bij de meldplicht voor veiligheidslekken.

Voorzitter: Gesthuizen

De heer **Van der Linde** (VVD): Voorzitter. Terugkijkend op de gebeurtenissen van 2011, moeten we constateren dat het risicobewustzijn binnen het openbaar bestuur onvoldoende was. Dat zien we vaker bij cybersecurity, maar in dit geval was het urgenter omdat het de burger direct raakte.
Integriteit rondom DigiD is essentieel om identiteitsfraude te voorkomen. Nederlanders moeten erop kunnen vertrouwen dat het openbaar bestuur alles doet om daaraan te werken. Het is evident dat er een omslag in het denken over veiligheid moet komen – die is overigens ook gaande – en dat we bouwen aan een veiligheidscultuur. Er is al het een en ander gezegd over de meldplicht. Die hoort bij de veiligheidscultuur. Het melden van incidenten biedt het Nationaal Cyber Security Centrum de kans om maatregelen te nemen. We moeten dit zorgvuldig benaderen. Naming and shaming is niet de goede weg. Bij een veiligheidscultuur hoort een veilige omgeving waarbinnen je incidenten kunt bespreken en van incidenten kunt leren.
In de tussentijd zullen we wel moeten nadenken over een betere veiligheid op het niveau van de gebruiker. In de brief van 29 oktober wordt al gesproken over een veiliger DigiD op niveau Midden, met een tussenstap per sms. De voor de hand liggende vraag is natuurlijk waarom we dat niet gewoon standaard verplicht stellen. De combinatie van iets wat je weet met iets wat je hebt, biedt extra veiligheid en is gemakkelijk toe te passen.
Ik wil mij verder beperken tot drie concrete vragen.

1. Hoe gaan we nu verder met het rapport van Fox-IT? Een aantal aanbevelingen, zoals het assessment, is of wordt al opgevolgd. Neemt de minister nu alle aanbevelingen over? Worden deze gewoon afgevinkt?

2. Het uit de lucht halen van DigiD is een zeldzaamheid. Het was een noodzakelijke zeldzaamheid, maar het roept wel de vraag op wat de gevolgen zijn voor de mensen en bedrijven die daarmee te maken hebben. Ik noem de belastingaangifte, maar ik denk bijvoorbeeld ook aan studenten die voor hun inschrijving aan een universiteit of voor hun studiefinanciering gebruikmaken van DigiD.
3. Kan de minister inzicht geven in de directe financiële gevolgen van alles wat er in 2011 is gebeurd? Wat heeft dit de belastingbetaler nu gekost?

Voorzitter: Van der Linde

De **voorzitter**: Het woord is aan de minister.

Minister **Plasterk**: Voorzitter. Uit het aantal bezoekers op de publieke tribune leid ik af dat er veel interesse is voor dit onderwerp, en dat is goed. Het klinkt technisch, maar het is reuze belangrijk.
Een groot deel van ons bezit, en in feite ook een deel van onze identiteit, is inmiddels digitaal geworden. Met «identiteit» doel ik niet op identiteit in spirituele zin. Wat ik bedoel is dat, als je bijvoorbeeld iets bestelt, degene bij wie je het bestelt weet dat je werkelijk degene bent die je zegt te zijn en dat, als je verplichtingen aangaat, bekend is dat jij de betrokkene bent die de verplichting is aangegaan. Dat een groot deel daarvan digitaal is geworden, betekent dat de beveiliging van ons bezit in digitale zin niet minder belangrijk is dan de beveiliging van ons bezit in een andere vorm, zoals een huis, een auto of iets anders in de persoonlijke levenssfeer. Het is werkelijk een belangrijk onderwerp. Dat het een hoge vlucht heeft genomen, realiseerde ik mij eigenlijk pas toen de heer Verhoeven mij uitdaagde door te zeggen dat ik dat als wetenschapper in mijn eerstejaars-colleges toch allemaal geleerd zou moeten hebben. Nou zijn die eerste-jaarscolleges alweer een paar jaar terug. Toen deden we wel iets met computers. Toen liep ik met van die dikke pakken met ponskaarten rond. Dat was de enige realistische drager van informatie. Internet had je toen nog niet. De voordelen daarvan, maar ook de risico's ervan, bestonden op dat moment nog niet. Alle organisaties en alle personen moeten zich realiseren dat naarmate de mogelijkheden van digitale media groter worden, de risico's daarvan toenemen. Dat betekent dat het bezien vanuit de techniek logisch is om in de genoemde drieslag – beschikbaarheid, integriteit en vertrouwelijkheid – in eerste instantie de nadruk te leggen op een grote beschikbaarheid. Hiermee geef ik meteen een reactie op het punt van de heer Verhoeven. Een grote beschikbaarheid is immers een groot gemak voor iedereen en het illustreert hoe machtig een digitaal medium kan zijn. Wij moeten een inhaalslag maken en ervoor zorgen dat de twee andere aspecten even belangrijk worden gevonden als de beschikbaarheid. Als iets mogelijk is, kan er pas een reden zijn om het ook te gaan doen als je weet dat de vertrouwelijkheid en de veiligheid gegarandeerd zijn. Dat moet echt vooropstaan.
Dit algemeen overleg is in zekere zin voortgekomen uit het incident met DigiNotar. Ik dank mevrouw Oosenbrug voor de goede woorden die, via mij, gericht zijn aan de mensen die voor mijn voorgangers hebben gewerkt. Zij hebben het op een goede manier opgevangen. Zij hebben laten zien dat er ook weleens wat werkt en dat dingen die hier worden verzonnen en in de praktijk worden uitgevoerd, ook het effect kunnen hebben dat wordt beoogd.
Laat ik een paar onderwerpen langslopen en dan per spreker bekijken of ik nog punten heb gemist.
Mevrouw Gesthuizen en mevrouw Oosenbrug vroegen naar het ethisch hacken. Ethisch hacken is hacken met de bedoeling om aan te tonen dat er ergens een lek zit. Dat gebeurt dus niet om er rijk van te worden of om informatie te achterhalen die vertrouwelijk is. Ik kan mij ook voorstellen

dat er een zeker sportief element voor de ethische hacker in zit: het is stoer om te bekijken of je in staat bent om die en die site te kraken. De bedoeling daarvan is echter niet om daar beter van te worden. Misschien wordt vervolgens zelfs trots gezegd: kijk wat ik heb gehackt, daar zit een lek. Dat is op zichzelf goed bedoeld, maar hacken is inbreken en inbreken mag niet: laten we dat vooropstellen. Dat is het uitgangspunt. Als er opeens iemand bij jou in de keuken staat en zegt «ik wilde aantonen dat de achterdeur niet op slot zat», dan zeg je ook: je hoort hier niet, want niemand heeft je gevraagd om dat aan te tonen.
Het kan in ieder geval wel gebeuren met wederzijds goedvinden. Vorige week hebben wij dat in een demonstratie laten zien. Die was overigens inderdaad te herleiden naar een suggestie van D66, die wij met dank hebben opgepakt. Daarbij sprak de gemeente Haarlemmermeer met een aantal studenten af dat zij zouden laten zien of de site van de gemeente te hacken viel. Dat mag. Dan moet van tevoren een non-disclosure agreement worden gesloten. De partijen die de hack uitvoeren, moeten daarbij verklaren dat zij de informatie die zij verkrijgen, niet met anderen zullen delen. Ik was erbij. Ik vond het wel mooi om te zien dat zij zelfs voor de pers de beeldschermen afschermden; er zou immers iets op kunnen staan.
Daarnaast heeft minister Opstelten in januari een leidraad naar de Kamer gestuurd voor responsible disclosure. Daarbij wordt organisaties geadviseerd om geen aangifte te doen tegen hackers die op eigen initiatief hebben gehackt met het enkele doel om de organisatie bewust te maken van de kwetsbaarheden in de beveiliging, mits de hacker zich daarbij houdt aan de regels die in deze richtlijn zijn geformuleerd. Er is dus wel een opening geboden. Hierover zijn wel een aantal vervolgvragen gesteld. Uiteindelijk gaat dit dus over de manier waarop je wel en niet mag inbreken. Dat is niet meer de portefeuille van degene die gaat over de digitale overheid. Dat wordt op een gegeven moment de portefeuille van Justitie. Als de leden op dat punt indringend willen doorvragen, dan is mijn suggestie om dit punt aan de orde te stellen bij mijn collega van Veiligheid en Justitie.
Mevrouw Gesthuizen en anderen vroegen aandacht voor het grote aantal fouten dat was gevonden. Ik kan hierover nog wel wat informatie delen. Ik zag dat op Webwereld wordt vermeld dat BZK niet wil melden wie de zes grootverbruikers waren bij wie er nog wel wat mis was. Ik kan ze wel noemen. Het zijn: de Belastingdienst, UWV, DUO, Studielink, SVB en CZ. Geen van de zes had een zo acuut beveiligingsprobleem dat dit onmiddellijk risico's met zich zou brengen. De bevindingen zijn wel aan de organisaties doorgegeven, opdat zij daar iets mee kunnen doen.
Ik dacht, naïef op het gebied van hacken, dat je probeert om iets te hacken en dat je dan in een keer «binnen» bent. Dat zie je ook altijd in films. Dan gebeurt er iets, dan verandert het beeld op het scherm en dan ben je binnen; dan kun je alle e-mails lezen en dan kun je zien wat iedereen op zijn computer heeft staan. Dat is, zo bleek mij, een te simpel beeld. Wat veel hackers doen, is niet erin slagen om binnen te komen, maar signaleren dat ergens software of een bepaalde encryptiemethode verouderd is en dat daar dus een potentieel risico zit. Men heeft dan niet de meest recente versie en daardoor dus niet de meest veilige versie. Dat viel mij in die zin een beetje tegen. Ik wilde ook weleens de site van Haarlemmermeer van binnen zien, maar dat was niet het soort zwakke punten dat de hackers aantroffen. Veilig of niet veilig is dus niet helemaal een zwart-witverhaal. Dat geldt ook voor de genoemde organisaties. Er zijn zwakke punten aangetoond.

De heer **Verhoeven** (D66): Ik ben het eens met de minister over het juridische deel. Dat moet worden besproken met de minister van Justitie. Dit is echter wel de kern: het gaat erom of je een gat vindt of dat je een gat maakt. Er zijn veel criminele hackers die gaten maken en daar hun

voordeel mee willen doen. Er zijn echter ook hackers die iets zien wat er al is en daarop willen wijzen. In de digitale wereld is de situatie niet zo zwart-wit als een sleutel die in het slot zit. Een sleutel kun je uit het slot halen, je kunt hem gebruiken om mee naar binnen te gaan en je kunt hem ook door de brievenbus gooien en ervoor zorgen dat de persoon die de sleutel in het slot heeft laten zitten, de volgende keer die sleutel er niet meer in laat zitten. Hoe gaat de overheid daarmee om? Natuurlijk moet juridisch worden vastgelegd wat bij ethisch hacken wel en niet kan, maar de overheid moet toch ook goed nadenken over de manier waarop zij gebruik wil maken van de mogelijkheden om de veiligheid te vergroten door middel van het inzetten van hackers.

Minister **Plasterk**: Daar ben ik het mee eens. Laat ik vooropstellen dat als men de bedoeling heeft om te hacken, het de voorkeur verdient om tevoren vast te stellen dat het met wederzijds goedvinden gebeurt. Dan is iedereen veilig. Dan weten ook de hackers dat zij zich op veilig terrein begeven en dat er niks gebeurt wat zich tegen hen kan keren. Ik vind toch dat wij daar vrij ver in gaan, want daarnaast hebben wij geadviseerd om geen aangifte te doen als mensen zich aan de instructie houden. Dat gaat redelijk ver, want het uitgangspunt is dat hacken inbreken is, en inbreken is verboden. Alleen al het feit dat de minister van Justitie deze instructie heeft gestuurd, duidt er al op dat wij er veel positiever tegenover staan. Wij erkennen dat het echt meerwaarde heeft als de ethische hacker zich ervoor inzet om gaten op te sporen. Ik vind dat wij daarbij een positieve grondhouding aannemen. Mensen kunnen goede intenties hebben, maar intenties kunnen ook veranderen. Het is ook mogelijk dat mensen goede intenties hebben en dat anderen met slechtere intenties over hun schouder meekijken. We zullen altijd op moeten blijven passen met deze tak van sport.

Mevrouw **Gesthuizen** (SP): Ik heb specifiek gevraagd hoe het komt. De uitleg van de minister begrijp ik maar al te goed. Als er ergens een muizengaatje is, betekent dat niet dat je meteen het hele systeem kunt overnemen. De portee van mijn vraag was echter dat ik uit de informatie die we hebben gekregen, opmaak dat een groot deel, ongeveer de helft, van de fouten komt door verouderde software of door relatief eenvoudig te voorkomen programmeer- of instellingsfouten. Ik noem het maar beginnersfouten. Hoe kan dat eigenlijk?

Minister **Plasterk**: Er werd net gevraagd of het gebeuren van vorige week met de hackers een stuntje was. Ja, dat was een stuntje, want we willen aandacht trekken voor het onderwerp en bewustzijn creëren bij organisaties. Ik heb die mooie gelegenheid dus bewust aangegrepen om iedereen erop te wijzen. Uit de berichtgeving van de pers na afloop bleek ook dat men inderdaad dat soort zaken had gevonden, bijvoorbeeld dat er al een update is, maar dat deze nog niet wordt gebruikt. Dat is nalatigheid. Daarnaast is er het idee dat men goed zit omdat men het drie jaar geleden door professionals heeft laten aanleggen en het toen helemaal state of the art was. Ik heb daar ook benadrukt dat er een voortdurende strijd aan de gang is tussen mensen die binnen proberen te komen en mensen die proberen te beveiligen. Die strijd duurt voort. Als het twee jaar geleden op orde was, wil dat niet zeggen dat het klaar is. We doen echt een appel op mensen om het goed te doen. Daar kan die taskforce ICT een grote rol in spelen. Ik heb ook niet al die 408 gemeenten aan een touwtje. Ik moet dus via de VNG proberen om het bewustzijn op dat terrein binnen gemeentelijk Nederland te vergroten.

Mevrouw **Gesthuizen** (SP): Wat is het toch jammer dat we ze niet allemaal aan een touwtje hebben. Nee hoor. Het is echter niet niks waar we het over hebben. Dat meen ik wel serieus. Als iemand denkt dat een

systeem dat drie jaar geleden goed is geïnstalleerd de komende tien of vijftien jaar hacker- of crimineelproof zal zijn, snapt hij eigenlijk niet zo goed waar hij mee bezig is. Dan snapt hij ICT niet. Daar maak ik me nog het meeste zorgen over. Het is namelijk wel erg zorgelijk als er bij overheidsinstanties mensen werken die eigenlijk niet goed snappen wat ze aan het doen zijn.

Minister **Plasterk**: Daar ben ik het helemaal mee eens. Dat moet ook door eenieder worden opgepakt. Ik denk dat de taskforce daarin een grote rol kan spelen. De overheid heeft ook nog de doelstelling om alles in 2017 zo veel mogelijk digitaal te hebben. Dat betekent dat we met ons hele hebben en houden digitaal zijn. Dat kan natuurlijk alleen maar wanneer de beveiliging hiermee gelijke tred houdt. Ik deel het appel dus.
Mevrouw Gesthuizen en mevrouw Oosenbrug vroegen of het niet wat te vrijblijvend is. Moeten we het misschien dwingender opleggen? Ik ben binnen het ministerie aan het analyseren welke regelgeving aanwezig is, zoals de standaarden voor de beveiliging, en hoe deze kan worden ingezet. Er zijn normen, ISO 27001 en ISO 27002. Deze worden breed nageleefd en zijn ook vastgelegd door het College Standaardisatie. Op rijksniveau zijn er een aantal normen. We willen hierover binnen de taskforce dwingende afspraken maken met de partners. Hierin zitten bijvoorbeeld de waterschappen en de provincies. Er komt een systeem om een en ander te auditen en om te kijken of het allemaal deugt. Daartoe is grote bereidheid. Er is inmiddels een overleg gestart met de verantwoordelijken voor het borgen hiervan. Dat moet dan leiden tot een strategie voor de hele overheid. Mijn voorkeur gaat ernaar uit om dit traject te bewandelen en te zeggen: dames en heren, dit is niet vrijblijvend; we vinden eigenlijk dat u dit moet doen. Als ze zich daarin zullen voegen, wil ik even wegblijven van het maken van nieuwe wetten. Die wetten zijn er natuurlijk ook niet morgen. In die zin is het beter als iedereen er de logica van inziet en zich realiseert dat het niet vrijblijvend is. Ik ben pas bij één sessie geweest, maar ik heb de indruk dat iedereen ervan doordrongen is dat het niet vrijblijvend moet zijn. Ik hoop dat de Kamer het goed vindt dat wij dit dringend en dwingend, maar zonder wetgeving, oppakken.

Mevrouw **Gesthuizen** (SP): Ik maak me daar zorgen over. Ik wil bovendien voorkomen dat deze minister straks zelf onderzoeker is en dat de taskforce pas over jaren wordt geëvalueerd. We willen juist snelheid. Ik snap dat we morgen geen wet- en regelgeving hebben, maar ik breng nogmaals de ergernis in herinnering van een groot deel van de Kamer naar aanleiding van het gesprek met mensen die op de een of andere manier betrokken waren geweest bij het DigiNotar-incident. Ze waren eigenlijk niet bij het incident betrokken, maar ze waren degenen die van tevoren verantwoordelijk waren. Er was veel ergernis over de uitspraak van de mensen aan tafel dat hun verantwoordelijkheid niet zo ver strekte. Zij zeiden dat zij op papier een zoveelstelijnstoezicht hadden en dat zij dat hebben uitgevoerd. Of het echt veilig was, daar gingen zij niet over. Dat kan een kwestie zijn van bewustwording, en dat is prima, maar uiteindelijk moet je mensen ook ergens op kunnen afrekenen. Ik maak me er zorgen over als er geen regels komen die aangeven waar de verantwoordelijkheid precies ligt en wie er dus in gebreke blijft als die verantwoordelijkheid niet wordt genomen.

Minister **Plasterk**: Mag ik het als volgt zeggen, mevrouw Gesthuizen? Ik vind dat het niet acceptabel is dat men ervoor wegloopt en zegt dat men er niet over gaat. Er moet altijd iemand gaan over de beveiliging. Ik zeg u toe dat ik iemand die duikt voor de verantwoordelijkheid, hierop zal aanspreken en de Kamer hierover zal melden. We zitten op het

vinkentouw en we doen alles wat we kunnen binnen het huidige stelsel om ervoor te zorgen dat die vrijblijvendheid ervan afgaat.

Mevrouw **Gesthuizen** (SP): Het is uitgebreid onderzocht. De Onderzoeksraad Voor Veiligheid vraagt de rijksoverheid actiever gebruik te maken van haar regelgevende bevoegdheid ten aanzien van de stelselverantwoordelijkheid. De OVV zegt dit niet voor niets. Ik lees daarin een oproep om wel met regelgeving te komen. Pak die kans nu die er is.

Minister **Plasterk**: De taskforce heeft de opdracht om te bekijken of het goed geregeld is. Als een gemeente hier niet aan voldoet, sluiten we DigiD voor die gemeente gewoon af. Dat kan ik toezeggen. De heer Verhoeven zei hier ook iets over. Misschien heb ik de indruk gewekt dat ik vind dat gemeenten autonoom zijn en het verder maar moeten zien. Dat kan echter niet als er via DigiD allerlei risico's worden gecreëerd. Als beheerder van DigiD heb ik dus de mogelijkheid om een gemeente af te sluiten, als er sprake is van een open gat in het netwerk.
Er is gevraagd waar de verantwoordelijkheid ligt voor het ethisch hacken. Daar heb ik al antwoord op gegeven, maar deze ligt uiteindelijk bij de collega van V en J.
Ik dank mevrouw Oosenbrug voor de goede woorden over Ruby on Rails. Ze sprak over een kluwen aan organisaties. Daar ben ik het mee eens. Er moet meer samenhang en eenduidigheid in komen. Samen met mijn collega's werk ik aan een samenhangende structuur en governance, met speciale aandacht voor het toezicht, dus de relatie tussen OPTA en Logius, en voor respons en herstel bij crisis. Hier werken BZK, Veiligheid en Justitie en het NCSC samen aan.
De opdracht van de taskforce heb ik al genoemd, namelijk om ook met andere overheidslagen te komen tot beveiligingsdiensten van de medeoverheden. Men werkt samen in een interbestuurlijke werkgroep. Het wordt helemaal georganiseerd. Dat moet ook, want dit is een grote kwestie. Het gaat ook over de baseline informatiebeveiliging en het stroomlijnen van het toezicht. We proberen de boel te stroomlijnen.
Ik heb de heer Verhoeven al bedankt voor het idee om studenten in te zetten. Het is hier nog niet genoemd, maar daar zit ook een opleidingsaspect aan. Mensen worden in zo'n opleiding natuurlijk niet opgeleid tot hacker. Een groot deel van de mensen zal uiteindelijk juist aan de andere kant staan. They don't join the dark side, maar gaan ergens werken als beveiligingsfunctionaris om de gaten te dichten.

De heer **Verhoeven** (D66): Aan zijn toon begrijp ik dat de minister het goed bedoelt. De term «the dark side» suggereert echter mijns inziens net iets te veel dat de hackers the dark side zijn en de overheid the white side is. Het gaat juist om het grijze gebied daartussen. Dat is ontzettend kansrijk, maar ook ontzettend ingewikkeld. Ik denk dat de minister dat ook wel begrijpt, maar ik zeg het voor de zekerheid.

Minister **Plasterk**: Daar ben ik het mee eens, maar er is ook een dark side. Die beveiliging is er niet voor niets. Er zijn mensen die dit soort zaken echt met slechte bedoelingen doen. Er zijn bijvoorbeeld gevallen geweest van mensen die moesten bewijzen dat ze iets niet hadden besteld. Uiteindelijk werkt het in de rechtbank natuurlijk zo dat de bewijslast ligt bij degene die meent een aanspraak op iemand te kunnen maken, maar in het traject daarvoor lopen heel veel mensen rond die een grote indruk kunnen maken op een eenvoudige burger. Mensen schrikken daarvan, bijvoorbeeld als een of ander inningsbedrijf claimt dat zij nog zoveel duizend euro krijgt. Dat levert een hoop ellende op. Daar zijn we het over eens. Met de term «the dark side» duidde ik op de mensen met de echt slechte bedoelingen, niet op mensen met goede bedoelingen.

Ik ben het eens met de heer Verhoeven dat een en ander nauw luistert. In principe zijn er in onze gedecentraliseerde eenheidsstaat verschillende, autonome, bestuurslagen. Daarnaast zijn we ook elektronisch verknoopt. Die autonomie betekent dus niet dat het Rijk de andere kant op kijkt als een lagere bestuurslaag, een gemeente of een provincie, de veiligheid niet op orde heeft. Ik onderstreep hier dus nog maar eens dat het niet vrijblijvend is.
Voor het verplicht melden van gaten is V en J verantwoordelijk. Er ligt een voorstel bij V en J om dit vast te leggen. De behandeling hiervan zal aan de V en J-kant plaatsvinden.
Dan kom ik bij de vragen van de heer Van der Linde. Het Fox-IT-rapport is meegenomen in de aanbevelingen in het OVV-rapport. Die aanbevelingen volg ik allemaal op. Dat is een gemakkelijk antwoord.
Waarom maken we DigiD Midden niet verplicht? Als burger kun je hiervoor kiezen. Het gaat om een gebruikersnaam, wachtwoord en sms-code. Dit hogere niveau is niet voor alle diensten nodig, maar we stimuleren het wel. We gaan stapsgewijs naar het hogere niveau toe. Steeds meer mensen gebruiken DigiD Midden. Ik wil geen conflicten krijgen met de VVD, die vindt dat we niet nodeloos moeten reguleren. Nu het de goede kant opgaat, denk ik dus dat we het moeten aanmoedigen. Dan kunnen we altijd nog zien of een verplichting per se nodig is. Ik meen dat iedereen er het nut en de noodzaak van inziet.
Hiermee heb ik alle vragen beantwoord. Excuus, ik hoor dat ik een vraag van de heer Verhoeven ben vergeten. Het beste paard van stal. Volgens mij heb ik al antwoord gegeven op de vraag of beschikbaarheid uitstijgt boven integriteit en vertrouwelijkheid.
Dan is er nog de vraag over de Iraniërs. De certificaten van DigiNotar zijn overal vervallen, dus ze kunnen nu niet meer worden gebruikt voor veilig internetverkeer. Microsoft heeft op verzoek van Nederland de aanpassing van de browsers, waardoor certificaten van DigiNotar ongeldig zouden worden, uitgesteld. Dat geldt ook voor andere browserleveranciers, zoals Firefox. De reden hiervoor is dat de hele dienstverlening stil zou komen te liggen als dit direct zou gebeuren. De kwetsbaarheid door de DigiNotar-affaire zat overigens niet zozeer bij DigiD. Dat hebben we al eerder besproken.

Mevrouw **Gesthuizen** (SP): Omwille van de tijd heb ik in mijn inbreng een punt buiten beschouwing gelaten, namelijk de manier waarop men bij DigiD omgaat met meldingen van misbruik. Ik krijg af en toe mails van mensen. Dat zijn individuele gevallen en daarom stel ik er niet meteen een vraag over. Ik heb een voorbeeld van een inbraak in een account terwijl iemand zelf met een sessie bezig was. Er is huur- en kinderopvangtoeslag aangevraagd. Die persoon heeft dat toen direct gemeld, onder andere ook omdat hij werd gewaarschuwd. De toeslag ging naar een voor die persoon onbekend rekeningnummer toe. Toen hij dat wilde melden, werd hij steeds van de een naar de ander doorverbonden. Op een gegeven moment kwam hij in contact met de afdeling fraude van DigiD. Het opheffen kon alleen maar schriftelijk. Zo was hij weer een paar dagen verder. Die persoon heeft op een gegeven moment voor de zekerheid maar aangifte gedaan bij de politie. Dat is heel verstandig. Ik vraag me af of de minister ook dat soort signalen krijgt en of een en ander echt op orde is. Het kan misgaan. Volgens mij weten we dat. Wordt dit echter voldoende opgepakt?

Minister **Plasterk**: De betrokkene heeft het goede gedaan door aangifte te doen. Dat moeten we ook aanmoedigen. Dat zou standaard moeten gebeuren. Met de FIOD bekijken we hoe het gaat met de toeslagen en DigiD. Dat is dus opgepikt.

Mevrouw **Gesthuizen** (SP): Heeft de minister er iets aan als ik dit specifieke voorbeeld doorstuur?

Minister **Plasterk**: Graag.

Mevrouw **Gesthuizen** (SP): Dan zal ik dat ook melden aan degene die dit gemaild heeft. U krijgt het van mij onderhands. Dank u wel.

Minister **Plasterk**: Logius zal dit oppikken.

De **voorzitter**: Is er behoefte aan een korte tweede termijn? Ik zie dat dit het geval is.

Mevrouw **Gesthuizen** (SP): Voorzitter. Ik dank de minister voor zijn beantwoording. Volgens mij is er maar één punt waarover we het niet helemaal eens zijn, namelijk dat er regelgeving moet komen. De minister heeft echter wel gesproken over «dringende of dwingende» afspraken binnen de taskforce. Ik houd me vast aan die combinatie, dringend en daarmee ook dwingend. Ik zal de vinger aan de pols houden. Mijn voorkeur gaat er natuurlijk naar uit dat de minister nu begint met het formuleren van wetten en regels, maar we zullen het zien.

Mevrouw **Oosenbrug** (PvdA): Voorzitter. Allereerst dank aan de minister voor zijn beantwoording. Dat waren de antwoorden waar ik naar zocht. Over de ethische hackers worden we het waarschijnlijk niet eens. Op 30 maart is er een open dag van de hackerspaces, waarbij hackerspaces in Nederland, twaalf stuks, hun deuren openzetten en laten zien wat ze daar doen. Je kunt dan zien dat ze heel goed omspringen met technologie. Zaken als ethisch hacken of knuffelhackers worden heel goed uitgelegd. Ik kan het de minister aanraden en het is ook leuk voor de mensen thuis die zich afvragen wat dit is. Het is op internet te vinden: hackerspaces.nl. Voor de wat meer gevorderden is er elke vier jaar een hackcongres. Dit jaar begint het congres, genaamd OHM, op 31 juli. OHM staat voor Observe, Hack, Make. Ook daarbij wordt heel positief gekeken naar hackers. Het gaat om de «witte» kant van het hacken, de goede kant. Met hacken word je uiteindelijk natuurlijk een informatiespecialist. Je kunt het op een negatieve manier doen, maar je kunt het ook vanuit je werk of als hobby doen. XS4ALL is bijvoorbeeld ontstaan vanuit de hackerscommunity en is uiteindelijk een heel gerenommeerde internetprovider geworden. Marktplaats heeft mensen aangemoedigd om zijn website te hacken. De mensen die dat gelukt is, zijn in dienst genomen. Ik wil toch vragen, ook omdat mijn hart daar ligt, om er positief naar te kijken. Benadruk niet de donkere kant, maar bekijk juist hoe het positief kan worden ingezet. Ik ben daarom blij dat de minister zich op dit gebied geprofileerd heeft, ook in de krant, en met de groep studenten heeft laten zien hoe hacken gaat en dat je er iets positiefs uit kunt halen. Dat wil ik nog even benadrukken.
Over DigiD en webrichtlijnen zullen we volgende week spreken. Ik zal er nu niet te veel over zeggen, maar ik wil wel het volgende meegeven. Als er een extra beveiligingsstap wordt ingevoerd, is dat voor visueel gehandicapten heel lastig. Misschien wil de minister dit meenemen, ook in voorbereiding op het ICT-overleg van volgende week.

De heer **Verhoeven** (D66): Voorzitter. Ik dank de minister voor zijn beantwoording. Eigenlijk zegt de minister op alles wat wij inbrengen dat hij het ermee eens is. Dat is prettig, maar ook zorgelijk. Er moet dus wel iets mee gebeuren. Er zijn drie zaken. Ten eerste zegt de minister dat beschikbaarheid bij de drie elementen niet altijd blind voorop moet staan. Ten tweede kunnen gemeenten in het digitaal verknoopte veld, waarin zij ook een speler zijn, niet altijd volledig vrij handelen. Ten derde gaf de

minister aan dat hij ook vindt dat er sprake is van een kluwen. Hoe gaat de minister die eenstemmigheid vormgeven? Wat doet hij voor de gemeenten? Wat doet hij aan de kluwen? Wat gaat hij doen in de afweging tussen de drie elementen? Hoe wordt hierin een prioriteit gesteld? Dat is namelijk de volgende stap.
Het is prettig dat de minister op deze manier in de materie zit en zijn zelfbenoemde naïviteit grotendeels heeft verloren. Ik ben het eens met mevrouw Oosenbrug, die heel gepassioneerd omgaat met de hackerswereld. Dat is prachtig. Ik geef toe dat een deel van de achterban van mijn partij weleens een te roze bril op heeft en de donkere kant in het grijze gebied daardoor mist. In die balans komen we elkaar een heel eind tegemoet.
Over de meldplicht en responsible disclosure zal ik in de volgende debatten met de collega van deze minister op Veiligheid en Justitie, verdere vragen stellen.

De **voorzitter**: Ik heb alleen nog het verzoek om mijn laatste vraag te beantwoorden over de financiële gevolgen van de affaire in 2011.

Minister **Plasterk**: Voorzitter. Ik begin met de opmerking van de heer Verhoeven dat het opvallend is dat ik het met het meeste eens ben. Het is ook opvallend dat de leden van de Kamer het grotendeels met elkaar eens zijn. Dat geeft aan dat de behoefte aan veiligheid niet politiek betwist wordt. Dat geldt bijvoorbeeld ook voor de dijken. Politieke preferenties spelen misschien wel een rol in de mate waarin men bereid is iets meer decentraal of meer centraal te regelen.
De politieke verschillen zijn hier ook niet het punt. Het gaat erom of we de punten waarover we het eens zijn, ook werkelijk in de praktijk bij mensen tussen de oren kunnen krijgen. In de uitvoering is het namelijk toch zorgwekkend, zoals mevrouw Gesthuizen net zei, dat mensen denken dat het allemaal wel snor zit. Hiermee realiseren ze zich niet dat ze niet alleen de poorten naar zichzelf, maar ook naar een heel netwerk te wijd openzetten. Over wat er moet gebeuren, zijn we het grotendeels wel eens.
Ik dank mevrouw Gesthuizen omdat ze vooralsnog genoegen neemt met de termen «dringend» en «dwingend». Het helpt mij in zekere zin ook wel. De mensen van de taskforce – de voorzitter zit op de tribune – en anderen zullen het verslag krijgen. Dat kan gezien worden als een melding vanuit de Kamer dat er geen sprake kan zijn van vrijblijvendheid. Als men het niet zachtkens oppakt, staat de Kamer klaar om te constateren dat het niet goed genoeg gaat. Dan moet het harder worden aangezet. Iedereen heeft dat gehoord en kan dat in zijn oren knopen.

Mevrouw **Gesthuizen** (SP): Kan de minister toestemming geven aan geïnteresseerde Kamerleden om een keertje mee te lopen met de taskforce? Is dat een idee?

Minister **Plasterk**: Natuurlijk. Ik moet het nog vriendelijk en beleefd vragen, maar er wordt geknikt, dus consider it done.
Ik dank mevrouw Oosenbrug voor de data van de verschillende hackfestijnen. Ik zal de pizza's en de Red Bull-blikjes klaarzetten. Daar bevestig ik weer het beeld mee dat hackers alleen maar jonge mannen zijn en dat is niet zo.
Mevrouw Oosenbrug had het over bedrijven die hackers uitdagen om hen te hacken. Dat doet Logius ook regelmatig. Dat is een heel verstandige aanpak om de gaten te vinden.
De heer Verhoeven sprak over het terugdringen van de kluwen in de taskforce. Daar geldt hetzelfde voor. Ik hoop dat iedereen die meeluistert of op de hoogte wordt gesteld van dit debat, zich zal realiseren dat de Kamer vindt dat er een einde moet worden gemaakt aan de wildgroei. Er

moet enige normering, transparantie en eenduidigheid in komen. Ik hoop dat men daaraan mee zal werken.
De heer Van der Linde heeft gevraagd wat de kosten waren van het incident destijds. Alleen voor de rijksoverheid zijn de cijfers bekend. De schatting is dat het 10 miljoen euro gekost heeft. Dat is toch een fors bedrag. Er zijn inbraken waarbij minder wordt verloren. Het benadrukt het belang om dit in de toekomst te voorkomen.

De **voorzitter**: Ik dank de minister voor zijn beantwoording. Ik dank zijn collega's voor de ondersteuning. Vriendelijk dank voor de uitnodiging om binnenkort bij de taskforce langs te komen.

Sluiting 13.23 uur.