Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2014–2015

26 643 Informatie- en communicatietechnologie (ICT)

Nr. 340

VERSLAG VAN EEN ALGEMEEN OVERLEG

Vastgesteld 19 december 2014

De vaste commissie voor Binnenlandse Zaken heeft op 11 november 2014 overleg gevoerd met Minister Plasterk van Binnenlandse Zaken en Koninkrijksrelaties over:

- **de brief van de Minister van Binnenlandse Zaken en Koninkrijksrelaties d.d. 10 juli 2014 over de voortgang van de uitvoering van de ICT-Beveiligingsassessments DigiD (Kamerstuk 26 643, nr. 323);**
- **de brief van de Minister van Binnenlandse Zaken en Koninkrijksrelaties d.d. 16 oktober 2014 over aanhoudingen voor fraude met DigiD (Kamerstuk 26 643, nr. 329);**
- **de brief van de Minister van Binnenlandse Zaken en Koninkrijksrelaties d.d. 3 november 2014 over een lek in gemeentelijke websites (Kamerstuk 26 643, nr. 331);**
- **de brief van de Minister van Binnenlandse Zaken en Koninkrijksrelaties d.d. 7 november 2014 over de Versterkingsagenda DigiD (Kamerstuk 26 643, nr. 332);**
- **de brief van de Minister van Binnenlandse Zaken en Koninkrijksrelaties d.d. 7 november 2014 met antwoorden op vragen van de vaste commissie voor Binnenlandse Zaken inzake veiligheid van DigiD (Kamerstuk 26 643, nr. 333).**

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

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

De waarnemend griffier van de vaste commissie voor Binnenlandse Zaken,
Hendrickx

kst-26643-340
ISSN 0921 - 7371
's-Gravenhage 2014

Voorzitter: Berndsen-Jansen
Griffier: Hendrickx

Aanwezig zijn vijf leden der Kamer, te weten: Berndsen-Jansen, Gesthuizen, Moors, Oosenbrug en Verhoeven,

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

Aanvang 16.10 uur.

De **voorzitter**: Ik heet de leden welkom. Er zullen ongetwijfeld nog wat meer leden komen, maar het debat in de plenaire zaal liep wat uit. Ik heet de Minister en zijn staf van harte welkom, evenals de mensen op de publieke tribune. De spreektijd is vier minuten per fractie, met twee interruptiemogelijkheden.

De heer **Moors** (VVD): Voorzitter. De fractie van de VVD vindt dat de incidenten betreffende DigiD zorgwekkend zijn. Met regelmaat lezen wij in de krant of horen wij van de Minister over fraude en misbruik. Fraude en misbruik bij digitale dienstverlening zijn zeer schadelijk. Ze leiden tot financiële schade voor betrokkenen en de overheid en ondermijnen het vertrouwen in de overheid. Er zijn regelmatig beveiligingsincidenten bij gemeenten en andere organisaties met een DigiD-aansluiting. Het beleid is om bij grote risico's zo'n organisatie tijdelijk af te sluiten van DigiD. In hoeverre wordt dit beleid daadwerkelijk uitgevoerd? Er worden weliswaar diverse maatregelen genomen op incidenten, maar dat is de brand blussen in plaats van aan brandpreventie doen. De VVD-fractie zou graag zien dat meer aan preventie werd gedaan. Ik kom daar straks nog op terug.
De Minister schrijft in zijn antwoorden op de vragen van de commissie dat er in het geval van de twaalf gemeenten met een lek in hun website geen reden is gevonden om te vrezen dat DigiD-gegevens in handen van derden zijn gevallen. Is dat met volledige zekerheid uitgesloten? Het is zeer zorgwekkend dat er gedurende veertien maanden een lek is geweest. Hoe kan dit, als er jaarlijks een ICT-beveiligingsassessment wordt gedaan? Waarom is het lek niet gevonden bij dat assessment? Zijn de reikwijdte en de normen van het assessment wel voldoende? Zou het niet beter zijn om voor nieuwe versies van software onmiddellijk een beveiligingsaudit te doen? Kan de Minister dit wellicht verplicht stellen? De Minister geeft in zijn brief aan dat bij beveiligingsaudits is gebleken dat er in 62% van de gevallen bevindingen zijn geconstateerd. Worden deze gevallen na afloop van de verbetertermijn opnieuw geaudit? Kan de Minister de Kamer dan opnieuw informeren over de resultaten?
Ook vraagt de VVD-fractie zich af waarom niet alle gemeenten dezelfde software of zelfs gecentraliseerde systemen gebruiken voor hun digitale dienstverlening. Natuurlijk hebben gemeenten hun eigen autonomie, maar zouden standaardisatie en centralisatie niet leiden tot een verbetering van de veiligheid? Waarschijnlijk is het ook kostenefficiënter. Het geld van de bespaarde kosten zou dan kunnen worden ingezet voor het vergroten van de aandacht voor security en voor frequentere en uitgebreidere beveiligingsassessments. Kan de Minister in overweging nemen om voor dit soort kwetsbare digitale dienstverlening standaardsoftware voor te schrijven, die dan vooraf goed getoetst kan worden op beveiligingsrisico's?
Ik kom op het punt van de gespoofte DigiD-websites en de valse e-mails. De Minister geeft aan dat Logius op de DigiD-website advies geeft over het veilig gebruik van DigiD. Is het niet verstandiger om hierover naast of samen met de campagne Alert Online een bredere voorlichtingscampagne te voeren? Het zou ook al helpen om bij het inloggen met DigiD aan

te geven waar gebruikers op moeten letten om zeker te weten dat zij op de DigiD-website zitten. Graag krijg ik hierop een reactie van de Minister.
Als DigiD-gegevens in verkeerde handen vallen, zijn er vele vormen van fraude mogelijk, die zowel de burger als de overheid veel geld kunnen kosten en die het vertrouwen in de overheid ondermijnen. Volgens de VVD-fractie zou de hoogste prioriteit moeten worden gegeven aan het voorkomen hiervan. Zou het niet beter zijn om per direct de sms-code verplicht te stellen, op zijn minst bij het wijzigen van gegevens? Hoe kijkt de Minister hiertegenaan? De Minister heeft ook aangegeven dat in risicogebieden, waar DigiD-brieven uit brievenbussen zijn gevist, de DigiD-activeringscodes worden thuisbezorgd per koerier. Het ligt voor de hand dat het probleem zich daarmee zal verplaatsen naar een ander gebied. Is het niet mogelijk om in alle gevallen activeringscodes voortaan te laten afhalen op het gemeentehuis of aangetekend te verzenden, al dan niet naar keuze van de burger? Zou daarmee niet een groot aantal fraudegevallen kunnen worden voorkomen?
Ik heb een aantal mogelijke preventieve maatregelen genoemd. Er zijn er zeker meer mogelijk. Ik roep de Minister ertoe op om meer in te zetten op preventie opdat de digitale communicatie met de overheid veiliger wordt en het vertrouwen van de samenleving in de digitale dienstverlening van de overheid niet verder geschaad wordt. Graag krijg ik hierop een reactie van de Minister.

De heer **Verhoeven** (D66): Voorzitter. Gemeenten hebben privacy nog niet in hun systeem zitten, zo schreef de Minister laatst aan de Kamer. Twee weken geleden, bij Opgelicht, bleek het nog veel erger te zijn. Twaalf gemeentelijke sites bleken veertien maanden lang onveilig te zijn geweest, omdat gemeenten de standaardinlogcodes van hun eigen content management system (CMS) niet hadden gewijzigd, waardoor DigiD-gegevens van honderdduizend inwoners gekaapt hadden kunnen worden. In tegenstelling tot wat de Minister schrijft, was DigiD dus wel degelijk onveilig. Het ging daarbij niet om het systeem zelf, maar om een lek via de gemeente. Het maakt eigenlijk niet uit waardoor, maar het was onveilig. Fijn dat de Minister knikt. Opgelicht heeft zojuist openbaar gemaakt om welke twaalf gemeenten het gaat. Waarom heeft de Minister dat niet gedaan? Waarom is er zo lang gewacht, waarom is er zo veel geheimzinnigheid en welk veiligheidsbelang was er gediend met deze geheimhouding? Het lek was immers toch allang dicht? Wanneer wisten de gemeenten zelf hoe het precies zat? Het lijkt er immers op dat zij gedurende lange tijd niet wisten wat er aan de hand was. Zij communiceerden heel diffuus richting hun eigen bewoners. Hoe grondig was het onderzoek dat de Minister beschrijft? Voor een grondig onderzoek waarin wordt nagegaan of het echt allemaal veilig was, zou volgens ons veel meer tijd nodig zijn geweest. Mijn laatste vraag naar aanleiding van de uitzending van Opgelicht is of de Minister zonder twijfel kan bevestigen dat er geen andere organisaties dan de twaalf gemeenten zijn met eenzelfde soort lek.
Het DigiD-systeem wordt door 600 gemeentes en instanties gebruikt en is dus zo sterk als zijn zwakste gebruiker. De fractie van D66 wil een steviger stok achter de deur. Zij wil dus een grotere en actievere controle door het ministerie, een snellere waarschuwing bij onveiligheid en daarna ook het afsluiten van de gemeente of instantie van DigiD. Collega Moors zei het net al: dat is staand beleid, dus het zou al moeten kunnen. Waarom is het dan toch niet gebeurd bij deze twaalf gemeentes, die meer dan een jaar hebben «opengestaan» en waarvoor de assessmentperiode langer heeft geduurd? Wij snappen dat inwoners dan langs de balie moeten en zaken niet meer online kunnen afhandelen. Die afweging maken wij. Wij hebben liever dat er veiligheid is dan dat mensen denken dat zij het via hun DigiD kunnen regelen en later met een rekening komen te zitten waarvan zij de

dupe zijn. Gaat de Minister in de praktijk de controle aanscherpen en gaat hij gemeentes ook sneller afsluiten van DigiD?
Naast blunderende gemeenten zijn er ook schrijnende fraudegevallen. Hoe kan het dat er geen belletje gaat rinkelen als een jongen van 15 in korte tijd ineens drie kinderen op zijn naam heeft en allerlei toeslagen aanvraagt? Dat is daadwerkelijk gebeurd. De situaties van mensen bij wie fraude heeft plaatsgevonden worden nu door het Centraal Meld- en Informatiepunt Identiteitsfraude en -fouten (CMI) onderzocht, maar waarom was er een televisie-uitzending nodig om dit in gang te zetten? Veel van die mensen hebben echt het idee dat zij van het kastje naar de muur gestuurd worden. Ook de Rekenkamer heeft geconstateerd dat het corrigeren van onjuiste gegevens bij meerdere overheidsinstanties een vrijwel onmogelijke opgave is. Bij wie ligt nu eigenlijk de bewijslast? Hoe zorgen wij ervoor dat er een veel laagdrempeliger manier komt om dit soort klachten snel en daadkrachtig af te handelen? De Minister schrijft zelf immers, en terecht, dat het heel belangrijk is dat het probleem van die mensen erkend wordt en dat zij niet het gevoel moeten hebben dat zij niet gehoord worden.
Dan kom ik op de veiligheid van DigiD. De Minister zegt dat DigiD aan alle moderne veiligheidseisen voldoet, maar Security.NL stelt dat DigiD nog steeds een voorkeur heeft voor het encryptiealgoritme RC4. Dat algoritme is ondertussen gekraakt. Het Nationaal Cyber Security Centrum waarschuwt hier al sinds maart 2013 voor. In het net verschenen rapport ICT-beveiligingsrichtlijnen voor Transport Layer Security (TLS) van hetzelfde NCSC staat bijvoorbeeld het volgende. Ik geef drie citaten: RC4 dient niet gekozen te worden; RC4 is een onvoldoende veilig algoritme; RC4 is een verouderd algoritme voor bulkversleuteling. Dat rapport staat dus vol passages waarin RC4 als algoritme wordt afgeraden. Een voorbeeld van een andere omgeving, die wel veilig is, is de omgeving die gebruikt wordt voor het internetbankieren. ING.nl gebruikt bijvoorbeeld AES-256, een methode die volgens het NCSC als veel veiliger wordt aangemerkt. Graag krijg ik hierop een reactie van de Minister.

De **voorzitter**: U bent al door uw spreektijd heen.

De heer **Verhoeven** (D66): Mag ik nog twee vragen stellen?

De **voorzitter**: Als ze kort zijn, mag dat.

De heer **Verhoeven** (D66): Ja, ze zijn heel kort. Waarom geldt er nog steeds een voorkeur voor de 128-bits-RC4? Waarom is de versleuteling van een bankomgeving van een hoger niveau dan die van DigiD? Moet de bank veiliger zijn dan de Staat?

Mevrouw **Gesthuizen** (SP): Voorzitter. Ik doe het even chronologisch. Eerst ontvingen wij een brief van de Minister waarin stond dat er niet zulke grote acute veiligheidsrisico's waren. Van de 500 organisaties die zijn aangesloten bij DigiD, liep er niet één een acuut veiligheidsrisico; 5% van die organisaties liep een groot, maar niet acuut veiligheidsrisico. In een latere brief rapporteerde de Minister echter veel meer gevallen van fraude. 5.000 DigiD's waren mogelijk onbevoegd gebruikt; de financiële schade bedroeg € 50.000; twee personen waren aangehouden. Uiteindelijk kwam dan, zoals mijn collega's al zeiden, de openbaring via het programma Opgelicht. Daaruit bleek dat ook veel gemeentes de zaak zelf niet handig hebben aangepakt en het gebruik van DigiD zelf niet goed hebben afgeschermd. Als de Minister hierop reflecteert, wat is dan zijn reactie? In de uitzending van Opgelicht meldde Fox-IT bovendien dat er slechts bij een heel beperkt aantal van de kwetsbare gemeenten onderzoek heeft plaatsgevonden en dat wij dus niet met zekerheid kunnen

zeggen dat er geen misbruik heeft plaatsgevonden. Weet de Minister daar nu meer over te vertellen?
In dit debat moeten wij het hebben over de zwakke plekken die gemeld zijn bij het gebruik van DigiD bij gemeentes. Eerder waren er problemen met de opslag van DigiD's bij de Belastingdienst. Steeds gaat het om de privacygevoeligheid van het inlogsysteem en de kwetsbaarheid van de techniek en het gebruik door de burger. De overheid wijst nu eigenlijk steeds naar de burger. De verschillende Ministers die hiermee te maken hebben, zeggen dat de burger moet worden opgevoed en zorgvuldiger met zijn of haar DigiD moet omgaan. Daar zijn campagnes voor opgestart. Dat is natuurlijk prima, want burgers hebben daarin zeker ook een eigen verantwoordelijkheid. Maar zelfs als blijkt dat er lekken zijn in het systeem van DigiD spreekt de overheid van calamiteiten die verholpen moeten worden, maar dan wel door de burgers.
Ik denk echter dat de problemen met DigiD niet alleen maar met onwetendheid van de burger te maken hebben. Dat is op zich ook niet zo gek. Wij hebben vandaag schriftelijke vragen ingediend naar aanleiding van het rapport van de commissie-Elias. Dat heb ik zojuist zelf ook gedaan. Ik weet wat erin staat. We moeten toch constateren dat er ook bij de overheid zelf een zorgwekkend gebrek aan kennis is. Daarbij gaat het niet slechts om het inkopen, opstarten of onderhouden van grote ICT-projecten; het gaat veel verder. Ik vrees dat wij daar bij deze problematiek ook mee geconfronteerd worden. De burger weet immers vaak dat DigiD kwetsbaar is en juist omdat het risico zo ondoorzichtig is – mensen weten niet precies wat de risico's zijn – gebruiken veel burgers DigiD liever niet. Ons bereiken veel berichten van bezorgde burgers die het systeem maar liever mijden. Zij maken zich vooral zorgen over hun afhankelijkheid van DigiD, terwijl zij er niet van kunnen uitgaan dat het systeem of het gebruik daarvan op de computer waterdicht is. Bij een inlogsysteem waarvoor de overheid verantwoordelijk is en waarvan het gebruik niet te vermijden is door de burger, moet de overheid garant staan voor voorkomende nadelige consequenties. Volgens de SP-fractie moet dat in alle gevallen zo zijn. De overheid schrijft in de brieven van 7 en 8 oktober over de grote hoeveelheden maatregelen die zij neemt om fraude en kwetsbaarheden tegen te gaan, maar zegt tegelijkertijd in de uitzending van Opgelicht: als die systemen in ketens worden gebruikt, toont de complexiteit daarvan aan welke gezamenlijke verantwoordelijkheid dit voor ketenpartners met zich brengt om te kunnen voldoen aan de steeds hogere eisen die door nieuwe bedreigingen ontstaan; het is duidelijk dat het werk nooit klaar zal zijn.
Nu het kabinet dit erkent, vraagt de SP-fractie de Minister om in alle gevallen zijn verantwoordelijkheid te nemen als de burger slachtoffer wordt van misbruik, hetzij door toedoen van een niet-functionerende overheid, hetzij door toedoen van criminelen. Wat denkt de Minister hiervan?
Zoals ik al zei, schrijft de Minister in zijn recente brieven over bewustwordingscampagnes en cursussen waarin mensen kunnen leren hoe zij moeten omgaan met DigiD. In de brief over de versterkingscampagne schrijft hij het volgende: «Het programma Digitaal 2017 streeft naar het digitaal mogelijk maken van het doen van allerlei zaken met de overheid. Voor sommige mensen vormt daarbij het gebruik van DigiD toch een drempel. Om die reden heb ik de Stichting Digisterker gevraagd een oefenmiddel te ontwikkelen: de DigiD oefentool. Mensen die een digivaardigheidscursus volgen kunnen in een veilige omgeving een DigiD leren aanvragen en gebruiken. Door te oefenen, wordt de drempel lager om DigiD aan te vragen en goed te gebruiken. De oefentool is naar verwachting in januari 2015 operationeel.» Ik denk dat een DigiD-vaardigheidscursus lang niet voldoende zal zijn. Mensen die veronderstellen dat zij de computer toch niet snappen, zullen heel terughoudend zijn met deelname aan een dergelijke cursus. De SP-fractie wil daarom dat

de overheid in alle gevallen ook toegankelijkheid via het loket of de telefoon blijft garanderen.

De **voorzitter**: Het woord is aan mevrouw Oosenbrug. Zij kwam wat later binnen, dus voor de duidelijkheid merk ik op dat wij een spreektijd van vier minuten hebben afgesproken.

Mevrouw **Oosenbrug** (PvdA): Zo veel tijd heb ik niet nodig. Ik ben de laatste in de rij en het gras is al een beetje voor mijn voeten weggemaaid. DigiD is ontzettend belangrijk, want als burgers worden wij min of meer gedwongen om dit te gebruiken. Als overheid zullen wij er dus ook voor moeten zorgen dat dit voor iedereen werkt. DigiD moet door de burgers zelf beter beveiligd worden. Daar worden wij als burgers constant op gewezen. Gemeenten en andere afnemers hebben echter diezelfde verantwoordelijkheid. Collega Verhoeven van D66 noemde dit al en ik vind dat een goed punt. Ik vind het zelf echter een beetje vervelend dat je zo'n gemeente dan afsluit van DigiD, waardoor er even niet meer mag worden ingelogd op DigiD; daar wordt de burger immers de dupe van. Daar ben ik het niet mee eens. Is het niet mogelijk dat in zo'n geval bijvoorbeeld Logius het beheer overneemt van zo'n gemeente, ervoor zorgt dat het probleem, dat wij geen lek noemen maar een softwarefout, wordt opgelost en daarvoor een rekening stuurt aan de gemeente? Zo ligt de rekening echt bij de gemeente en niet bij de burger. Ik vind dat de burger moet kunnen vertrouwen op DigiD. Dat is geen keuze, dat is opgelegd, dus dat moet je gewoon gebruiken.
Ik dank de Minister voor zijn antwoorden op mijn schriftelijke vragen. Ik heb dat relaas een paar keer doorgelezen. Ik kwam steeds weer op het punt dat op 18 september ontdekt is dat er een fout zat in het CMS, in het content management system. De softwareleverancier zegt dat hij dat lek gelijk gedicht heeft, maar dat kunnen wij niet controleren. Op 25 september heeft hij dit gemeld bij Logius, die ermee aan de slag is gegaan en het verder heeft opgepakt. Verder lees ik in de beantwoording dat het aan het softwarebedrijf zelf is of het al dan niet mensen gaat inlichten. Wij zijn bezig met een meldplicht voor datalekken. Het zou mooi geweest zijn als die wet al in werking was getreden, want ik vind het echt onbehoorlijk dat ik niet actief geïnformeerd word als ik kwetsbaar ben geweest door een fout in een systeem waar ik als burger gebruik van moet maken. Ik wil de Minister meegeven dat dit echt niet kan. Je kunt mensen niet verplichten om iets te gebruiken en, als er een kwetsbare plek blijkt te zijn, zeggen: wij als softwarebedrijf weten wel wat goed voor u is. Ik wil het gewoon weten. Ik wil weten, als ik over een halfjaar, een jaar of desnoods twee jaar ineens een rare rekening krijg, dat dit toen gebeurd kan zijn. Ook hiervoor vraag ik de Ministers aandacht.
Een tijdje geleden hebben wij gesproken over het reclamebureau Digi-D. Dit reclamebureau twittert nu dat het in het bezit is van 45.000 inlogcodes. Ik vind dat echt kwalijk. Dat is echt onwenselijk. Mensen gaan in goed vertrouwen naar die site en geven die inlogcodes af; vervolgens zijn zij kwetsbaar. Ik wil van de Minister graag horen wat de vervolgstappen zijn geweest na het laatste AO. Wat is de stand van zaken?

De heer **Moors** (VVD): Mevrouw Oosenbrug stelt voor dat, als zich bij een gemeente problemen voordoen met DigiD, Logius het beheer overneemt en het probleem oplost. Vindt zij niet dat in zo'n geval, bij een ernstig risico, DigiD desalniettemin zou moeten worden afgesloten totdat het probleem daadwerkelijk is opgelost, of vindt zij het voldoende dat Logius ernaar kijkt?

Mevrouw **Oosenbrug** (PvdA): Dat zijn twee verschillende zaken. Het een betreft een fout in het softwaresysteem van de beheerder van een website van een gemeente. Het ander betreft DigiD zelf en een kwetsbare plek in

DigiD. De mogelijkheid dat er een kwetsbare plek in DigiD zit, hebben wij al... Dat wordt niet beheerd door externe bedrijven. De websites van gemeenten mogen wel beheerd worden door externe bedrijven. Dat is mijn punt.

De heer **Moors** (VVD): Dat was niet mijn vraag. Volgens mij stelde mevrouw Oosenbrug voor dat Logius het beheer overneemt van zo'n externe partij op het moment dat er een bedreiging is voor de burger in verband met zijn DigiD-login, omdat er wellicht een lek is. Dat probleem is niet onmiddellijk opgelost. Vindt mevrouw Oosenbrug dat zo'n gemeente zou moeten worden afgesloten van DigiD, zolang Logius het probleem nog niet heeft opgelost?

Mevrouw **Oosenbrug** (PvdA): Ik denk dat je de oplossing moet zoeken waar het probleem ligt. Het probleem ligt niet bij de burger zelf, want die gaat in goed vertrouwen naar een website. Op zich zijn er heel veel zaken die je via de overheid kunt regelen, bijvoorbeeld via de website van je eigen gemeente. Wellicht moeten gemeenten dan toch meer gaan samenwerken met elkaar, zodat ik als ik in Lansingerland, waar ik woon, niet meer kan inloggen omdat mijn gemeente een probleem heeft met de website, zou kunnen uitwijken naar bijvoorbeeld Rotterdam. Er moet een oplossing voor te bedenken zijn. Ik ben van het zoeken naar oplossingen. Je moet het probleem niet terugleggen bij de burger, die er niet om gevraagd heeft. Wij moeten sancties gaan opleggen. Blijkbaar werkt het gewoon niet op dit moment, want die plicht is er al, maar er gaan nog steeds te veel dingen mis. Ik denk bijvoorbeeld aan websites van gemeenten die niet goed beveiligd zijn. Daar moeten wij wat meer druk op gaan uitoefenen. Geld, het opleggen van een bestuurlijke boete, schijnt toch altijd de grootste druk te geven.

De heer **Verhoeven** (D66): Ik ben blij dat mevrouw Oosenbrug ook wil dat zaken worden aangescherpt en dat mensen meer gecontroleerd worden op hun ICT-kwaliteiten. Het punt is dat het content management system van de websites van die gemeenten openstond, waardoor hackers veel makkelijker toegang konden krijgen tot DigiD, via die zwak beveiligde websites van gemeenten. Hoe kun je dan Logius de websites van die gemeenten laten overnemen? Dat lijkt mij een lastig punt.

Mevrouw **Oosenbrug** (PvdA): Het gaat mij niet zozeer om het beheer van de websites, als wel om het aanpakken van de kwetsbaarheid. Blijkbaar zijn er bij Logius nu ook ingrepen. Uit de beantwoording heb ik begrepen dat Logius heeft gezegd: wacht even, dit is de kwetsbaarheid, deze gemeentes maken hier gebruik van, wij gaan die gemeentes benaderen. Blijkbaar is er een link, al zie ik die niet terug in de beantwoording van de vragen, tussen Logius, de gemeentes en de beheerder van het content management system achter het beheer van de website. Daar ligt ergens een link, want anders had het bedrijf dat het CMS beheerde, niet een week later Logius geïnformeerd. Aan hun eigen kant is het wel opgelost. Daar zit een hiaat tussen van een week. Ik vind dat lastig.

De heer **Verhoeven** (D66): Dat snap ik. Volgens mij zegt mevrouw Oosenbrug: dwing gemeenten meer om digitaal veilig te zijn. Met dat pleidooi is volgens mij de hele Kamer het wel eens. Vervolgens zegt zij: dwing de burger niet om een week lang of twee weken lang naar de balie te gaan, maar bied hem een oplossing. Ook die gedachte vind ik heel goed – ik ben dus heel benieuwd naar het antwoord van de Minister – maar mijn punt is het volgende. Als je Logius de websites van gemeentes laat beheren – daar komt het dan toch op neer – loop je misschien weer tegen allerlei andere rare verhoudingen aan. Hoe ziet mevrouw Oosenbrug dit voor zich?

Mevrouw **Oosenbrug** (PvdA): Dat vind ik lastig. Ik probeer een oplossing te bedenken om ervoor te zorgen dat de burger zo min mogelijk last heeft van dat probleem. De website moet op dat moment wel goed onderhouden worden, of goed aangepakt worden. Als er een softwarelek zit, is er vaak ook wel meer aan de hand, zo heb ik inmiddels gemerkt. Zorg er nu voor dat die website op orde is. Dat pleidooi heb ik al eerder gehouden. Als burger ben je afhankelijk van die website. Ik wil best iedereen stimuleren om digitaal vaardig te worden, maar dan kan het niet zo zijn dat zo'n enorm digitaal vaardig persoon naar een website gaat die niet veilig is. Dan houdt het op. Dan kun je niet meer zeggen: u bent de burger en u bent zelf verantwoordelijk. Dat is de vergroting die ik wil tonen.

De **voorzitter**: Hiermee zijn we gekomen aan het eind van de eerste termijn van de commissie. Ik geef het woord aan de Minister van Binnenlandse Zaken en Koninkrijksrelaties voor zijn eerste termijn.

Minister **Plasterk**: Voorzitter. Mijn beantwoording is als volgt opgebouwd. Ik zal allereerst kort iets zeggen over DigiD in zijn algemeenheid, ook om de indruk weg te nemen dat het stelsel als zodanig niet goed zou zijn. Dan ga ik in op het verbetertraject. Ik heb daarover ook al een en ander schriftelijk aan de Kamer meegedeeld, maar ik denk dat het belangrijk is om een aantal elementen specifiek naar voren te brengen. Vervolgens ga ik in op het lek in het content management system van de gemeenten, inclusief de vraag hoe daarbij met de informatie richting de burgers is omgegaan. Daarna zal ik ingaan op de vraag wat te doen tegen gemeenten die niet doen wat ze zouden moeten doen. Dan zal ik nog iets zeggen over het eenmansbedrijf Digi-D. Vervolgens zal ik de resterende vragen van de leden beantwoorden.
We praten hier terecht over gevallen waarin er dingen niet goed zijn gegaan of niet goed gaan en wat we er aan moeten doen om in de toekomst misbruik en fraude te voorkomen. De indruk zou daarmee gewekt kunnen worden dat het DigiD-stelsel niet goed is, maar die indruk zou ik dan hierbij willen wegnemen. Het gebruik van DigiD is ontzettend toegenomen. We verwachten dat er in 2014 170 miljoen authenticaties worden uitgevoerd. Er zijn 600 organisaties aangesloten bij het systeem en de beschikbaarheid van DigiD is hoog, hoger dan bijvoorbeeld bij banken en hoger ook dan wat er is voorgespiegeld, namelijk 99,95%. Dus aan die kant werkt dat goed. Het DigiD-stelsel zelf is nooit gehackt. Nog nooit heeft iemand ingebroken op dat stelsel of heeft iemand dat stelsel gekraakt. Dat wil natuurlijk niet zeggen dat er nooit wat misgaat. Dat kan bijvoorbeeld gebeuren op een heel primitieve manier, namelijk dat een password naar iemands huisadres wordt gestuurd en het vervolgens door iemand anders uit de brievenbus wordt gevist die dan met die informatie aan de haal gaat. Daar hebben we ook maatregelen op genomen. Het kan ook verder gaan, namelijk dat er bij gemeenten een lek ontstaat in het computersysteem waardoor het in ieder geval theoretisch mogelijk zou zijn dat mensen het volgen als iemand daar inlogt, waardoor ze die informatie zouden kunnen verzamelen. Dus dat zijn geen fouten in DigiD zelf, maar dat wil niet zeggen dat er geen fraude mee gepleegd zou kunnen worden. Ook daar moeten we natuurlijk op bedacht zijn.
Bij fraude geldt dat er voortdurend sprake is van een ratrace, waarbij hackers slim zijn en steeds weer nieuwe dingen proberen waar we vanuit het belang van de burgers weer nieuwe dingen tegenover moeten stellen. Dus we moeten niet de illusie hebben dat het op enig moment klaar is; er zullen altijd wel weer nieuw achterdeurtjes verzonnen of gevonden kunnen worden en daar moeten we dan actief op inspelen. De huidige stand van zaken heb ik de Kamer inmiddels schriftelijk meegedeeld, maar ik wil nu een paar dingen noemen uit de Versterkingsagenda. Op dit moment log je in met je naam en je password dat je ooit via de post hebt

ontvangen. We zullen gaan kijken naar, wat dan heet, DigiD-midden, zijnde een hoger beveiligingsniveau waardoor je via sms een code krijgt toegestuurd. Daar mogen burgers nu al voor kiezen, op elk moment, maar het is wel kostbaar omdat het allemaal per sms gaat. We kijken nu naar de mogelijkheid om volgend jaar een app te lanceren waarmee mensen kunnen inloggen. Dan zou deze drempel omlaag kunnen en kun je het beveiligingsniveau wat algemener invoeren en zou je het op enig moment voor bepaalde handelingen wellicht verplicht kunnen maken. We moeten echter wel eerst weten of het werkt. Sommige gemeenten vragen al om de DigiD-code als je een afspraak wilt maken met iemand op het stadhuis. Dus ik kan mij voorstellen dat er wat betreft het geven van de DigiD-code een verschil is tussen studiefinanciering aanvragen – dan zal je eerder een hoger veiligheidsniveau willen hebben – en het maken van een afspraak met een ambtenaar.

De heer **Moors** (VVD): De Minister geeft aan dat het gebruik van die sms-code heel duur zou kunnen uitpakken. Ik zou dan weleens willen weten wat het zou kosten en hoe die kosten zich verhouden tot het aantal problemen en de kosten die je ermee voorkomt. Op dit moment zouden alle burgers al kunnen kiezen voor die methode. Dan zit je dus ook met die kosten. Mijn vraag is dan ook of je het gebruik ervan niet meer moet stimuleren, zeker in gevallen waarin je gegevens wijzigt. Ik snap dat een minder hoog beveiligingsniveau is vereist waar het gaat om het maken van een afspraak, maar een heleboel problemen waarmee we de afgelopen tijd zijn geconfronteerd, hadden volgens mij voorkomen kunnen worden als de die sms-code was gebruikt.

Minister **Plasterk**: Het landelijk verplicht stellen van zo'n sms-verificatie zou de overheid op dit moment 17 miljoen per jaar kosten en als het gebruik toeneemt omdat men zich veiliger acht, dan zou het kunnen oplopen tot naar schatting 37 miljoen in 2017. Dus het gaat wel om forse bedragen. Het is misschien ook niet nodig omdat elk DigiD-gebruik niet even zwaarwegend is en omdat we kunnen proberen het via de app op te lossen. Dat zijn de twee redenen waarom ik er voor zou willen pleiten om er wel voortvarend mee aan de gang te gaan, omdat ik het nut er wel van inzie, maar om het nu niet op voorhand verplicht te stellen.
Mede naar aanleiding van de aanbevelingen van de Algemene Rekenkamer zijn we bezig om bij alle 600 afnemers een nieuwe handreiking authenticatieniveaus onder de aandacht te brengen zodat men weet dat er voor verschillende handelingen ook verschillende niveaus van authenticatie zijn. Verder is er voortdurend sprake van assessments en wordt er uitvoering gegeven aan een actieplan ten aanzien van de bevindingen met de DigiD-voorziening. Daarnaast zijn we bezig met een traject richting eID, waar we bij een volgende gelegenheid nog wel over komen te spreken.

De heer **Verhoeven** (D66): Ik heb dat ook gelezen. Gelet op het huidige papieren beleid, is mijn vraag hoe het kan gebeuren dat die assessments wel elk jaar plaatsvinden maar bij bepaalde gemeenten de beveiliging totaal niet voldoet aan de Logius-standaard en waarom zoiets gewoon veertien maanden kan voortduren. Dat is toch waar het om gaat. We kunnen wel allemaal dingen afspreken maar als het in de praktijk zo gemakkelijk mis kan gaan, is toch aanscherping nodig.

Minister **Plasterk**: De gemeenten waar dit is misgegaan, waren bij de assessment beoordeeld als groen. Dus de verbazing van de heer Verhoeven is terecht. Kennelijk is het bij dat assessment toen niet opgemerkt. Deze check op het CMS zullen we de volgende keer dus wel moeten meenemen bij het assessment zodat de ezel zich in het gemeen niet nogmaals aan diezelfde steen stoot. Dat assessment dat overigens aan alle kanten is getoetst en met iedereen is besproken, kun je alleen

maar zo streng en zo scherp maken conform de stand van de kennis en de inventiviteit op dat moment. Ik kan echter niet op voorhand garanderen dat alle mogelijke nieuw hacks en achterdeurtjes kunnen worden afgevangen. We kunnen alleen maar leren van wat er fout gaat.

De heer **Verhoeven** (D66): Dat snap ik. Natuurlijk kun je niet alles uitsluiten en zal er altijd sprake zijn van een ratrace, maar we hebben het hier niet over een bizar slimme hacker die het systeem van een paar gemeenten heeft gekraakt, maar over het content management system, waarbij de standaard login-codes niet overschreven waren en dus nog bruikbaar waren. Dat is echt wel een open-deurlek. Dat is niet een ingenieus gaatje waar je briljante ICT-kennis voor moet hebben. Mijn punt is eigenlijk dat dit toch wel minimaal door zon assessment eruitgehaald zou moeten kunnen worden. Dit gaat niet om hogeschool ICT-kennis maar om basisveiligheid en dan niet bij één gemeente maar bij alle gemeenten die het CMS gebruiken. Dus hebben we een toetsdrempel van niveau 3, terwijl we op zoek moeten naar een 8.

Minister **Plasterk**: Ik kan alleen maar bevestigen dat het natuurlijk niet zo zou moeten zijn dat je een assessment doet en dat dan naderhand blijkt dat er toch iets in dat content management system niet goed is. Dus zullen we nog beter naar die assessments moeten kijken. Overigens, toen dat probleem aan de orde kwam, is dat aan die gemeenten medegedeeld en die hebben het toen onmiddellijk gerepareerd. Er is toen onderzoek gedaan. Er is door Logius geen reden gevonden om te denken dat er door dat lek DigiD-gegevens naar buiten zijn gekomen. Dat had je dan namelijk af kunnen meten aan toename van fraude in die regio of aan digitale sporen dat er iets zou zijn gebeurd. Er is dus goed naar gekeken.
Dat raakt dan meteen aan de vraag van mevrouw Oosenbrug en anderen hoe wordt omgegaan met het informeren van burgers. Dat betreft een afweging die in de eerste plaats bij de gemeenten ligt. Overigens begrijp ik wel de afweging die toen is gemaakt en vanuit Logius is er ook niet anders geadviseerd. Het informeren is met name nuttig als er handelingsperspectief is en mensen iets kunnen doen. Maar goed, het was inmiddels gerepareerd en er was geen reden om te denken dat er fraude was gepleegd, terwijl je aan de andere kant mensen niet wilt attenderen op de mogelijkheid dat er iets mis zou kunnen gaan. Mevrouw Oosenbrug wil in zijn algemeenheid nog een discussie – ik geloof dat die ook al binnen de justitieportefeuille plaatsvindt – over de vraag of niet sprake zou moeten zijn van een informatieplicht. Die discussie moeten we dan op dat moment misschien met elkaar voeren.
Als er sprake is van een acute dreiging of als gemeenten weigeren zich aan de regels te houden, moeten ze worden afgesloten van DigiD. Dat is ook al gebeurd. Bij zestien gemeenten zijn er afsluitingen geweest. Ik heb mij net laten vertellen dat de provincie Zuid-Holland die de zaak niet helemaal op orde heeft, ook is afgesloten van DigiD. Ik moet er aan toevoegen dat er niet zo heel veel handelingen voor burgers zijn bij de provincie Zuid-Holland waar je per se DigiD voor zou moeten gebruiken, maar de meeste provincies hebben wel degelijk DigiD-toegang. Sommige gebruiken het voor het maken van simpele afspraken. Hoe dan ook, als de grootste provincie van Nederland dat zou willen, moet de zaak eerst op orde zijn. Ik ben dan ook bereid om op dat punt actie te ondernemen. Mijn ervaring tot dusverre is dat als we tegen gemeenten zeggen «het klopt niet wat u daar doet» ze onmiddellijk tot verandering overgaan. Ik vind het overigens ook vanzelfsprekend dat ze dat doen. Als een gemeente DigiD gebruikt voor uitkeringen of wat dies meer zij, dan tref je de burgers als je laconiek zou afsluiten. Maar goed, ik zou eigenlijk helemaal niet in dat traject terecht willen komen. In het voorbeeld dat in Opgelicht naar voren kwam, hebben de desbetreffende gemeenten onmiddellijk gehandeld. In die uitzending werden overigens gevallen genoemd van mensen die

schade hadden opgelopen. De uitzending meldt wel dat dit niet het gevolg was van openstaande gemeentelijke systemen maar dat het ging om een echtgenoot die het had meegenomen; in feite is het dan een vorm van diefstal in de privésfeer, wat al akelig genoeg is. Overigens is er het Centraal Meld- en Informatiepunt Identiteitsfraude en -fouten dat mensen daarin kan bijstaan.
Het bedrijf Digi-D heeft eerder gevraagd om schadevergoeding voor het feit dat het de naam zou moeten veranderen. Het vroeg er aanvankelijk miljoenen voor. Omdat dat niet realistisch was, is dat bedrag heel snel naar beneden gebracht. Er is door Logius een bod gedaan dat niet is geaccepteerd. Daar is het bij gebleven. Ondertussen gaat het bedrijf door met het gebruikmaken van het misverstand door meer inloggegevens te verzamelen. Naar het lijkt gebruikt men dat nu tegen de overheid, hetgeen natuurlijk niet mag. Het gaat namelijk om privacygevoelige gegevens. Ik heb dat ook bij het College bescherming persoonsgegevens neergelegd dat uiteindelijk de bevoegdheid heeft om handelend op te treden en bestuurlijke boetes op te leggen. Daar ligt het nu en ik hoop en verwacht dat er nu snel wat gaat gebeuren, want het is niet bonafide om het op die manier te doen, aangezien je dat soort privacygevoelige gegevens niet mag verzamelen.

De heer **Verhoeven** (D66): Het gaat mij om het volgende. De Minister heeft desgevraagd door de Kamer een soort feitenrelaas naar ons gestuurd. Ik heb bijvoorbeeld geluiden gehoord dat het niet op de 18de gemeld is maar op de 11de. En zo zijn er meer gevallen waarbij het zeer twijfelachtig is of alle informatie waarover de Minister schrijft, wel klopt. Verder wordt gemeld dat de Minister pas op 8 oktober is geïnformeerd. Dat is een maand of drie weken later, zo u wilt, nadat het bekend geworden is. Dat zijn wel zaken waardoor ik mij toch afvraag hoe het allemaal zo lang heeft kunnen duren. En dan heb ik het nog niet eens over de veertien maanden die het heeft geduurd om er überhaupt achter te komen dat dit basale lek er was. De Minister zegt wel dat een aantal dingen in gang is gezet, maar ik wil hier toch straks de zaal uit kunnen lopen met het gevoel dat we nu een aantal serieuze dingen op een rij hebben gezet om het allemaal veel scherper te kunnen controleren. Anders is dit toch een wat teleurstellende wisseling van woorden.

Minister **Plasterk**: Ik deel de verbazing dat het mogelijk is geweest dat het zo lang open heeft gestaan. Een slimme hacker heeft dat lek gevonden en heeft daarop gewezen, waarvoor dank aan hem of haar. Vervolgens is er onmiddellijk handelend opgetreden. Het is echter van alle tijden dat er nieuwe achterdeuren worden gevonden. De ontdekte kwetsbaarheid is toen binnen 24 uur opgelost. Dat vind ik adequaat. Logius heeft toen een eerste scan gedaan van de consequenties van het lek en van eventuele aanwijzingen dat mensen zijn gedupeerd. Enig weken later, ook omdat bleek dat het probleem onmiddellijk was opgelost en er geen reden was voor schade, heeft men mij geïnformeerd. Toen is ook zo snel mogelijk de Kamer daarover geïnformeerd. De langste periode in dat traject is geweest de periode waarin het systeem open heeft gestaan. Dat is inderdaad betreurenswaardig, maar ik kan niet garanderen dat er niet ooit weer een nieuw lek komt waarvan men dan constateert dat het er al een tijdje heeft gezeten.

De heer **Verhoeven** (D66): Laten we in dit geval uitgaan van drie periodes. Over de periode van veertien maanden hebben we het gehad. Er wordt aan gewerkt om die periode in te korten en om ervoor te zorgen dat er actiever gekeken wordt of gemeenten hun zaakjes op orde hebben en of ze voldoen aan de Logius-standaard et cetera. Dan hebben we de periode dat er binnen 24 uur gereageerd wordt en het probleem opgelost wordt. Welnu, ik vind dat de gemeenten heel wisselend communiceerden

richting hun burgers. Over het grondige onderzoek van de Minister heb ik een vraag gesteld waarop ik graag nog een antwoord krijg. Dan kom ik op de tussenliggende periode van 11 september tot en met 8 oktober waarop de Minister zegt geïnformeerd te zijn. Waarom heeft dat zo lang geduurd? Waarom is er in de periode waarin het lek wel bekend was en het is neergelegd bij diverse instanties, niet veel sneller gehandeld om het probleem op te lossen?

Minister **Plasterk**: Ik ben een paar weken geleden bij de afdeling geweest die zich met het beheer van dergelijke bestanden bezighoudt en daar zitten slimme lui die voortdurend lekken proberen op te sporen en te repareren. De uitvoeringsdienst Logius stelt mij niet elke keer op de hoogte als er een lek of potentieel lek wordt gevonden, maar treedt dan eerst handelend op en inventariseert of er reden is tot paniek of reden om te denken dat er iets gruwelijk mis is gegaan. Zodra die inventarisatie daar is – dat is binnen een paar weken – meldt men mij wat er aan de orde is. Ik vind dat, eerlijk gezegd, niet laakbaar. Met name die periode van 24 uur, dus de periode tussen het moment waarop je weet wanneer er iets openstaat en het moment van reparatie, vind ik heel belangrijk. Die periode was gelukkig heel erg kort en zo moet het ook zijn. Verder moet ik dan op de hoogte gesteld worden van de relevante feiten. Dan vind ik het ook wel plezierig dat men even op een rijtje zet wat er precies te melden is en dat men mij als het een acuut iets betreft onmiddellijk belt. Ik vind dat door de mensen is opgetreden zoals ik dat van ze verwacht.

Mevrouw **Oosenbrug** (PvdA): Ik heb een verhelderende vraag. Burgers gaan naar de website van hun gemeente en op die site wordt hun gevraagd in te loggen met hun DigiD-code. Als ze dat doen, worden ze doorgelinkt naar de site van DigiD. In het onderhavige geval waarover we nu spreken, zat een zwakheid in het content management system. Dat lek heeft er acht tot tien maanden gezeten. Er kan toen van alles gebeurd zijn. Wij krijgen er ook geen helderheid over of het bijvoorbeeld om session-ID's gaat of om gespoofte websites, waarvan er inmiddels 40 uit de lucht zijn gehaald. Schijnbaar is er dus een reden om dit soort dingen te doen. Het lastige van die hele tijdlijn is dat zo'n softwareleverancier gewoon kan zeggen: we hebben het wel ontdekt maar we gaan niet precies zeggen wat het is want we hebben nog meer klanten. Dus misschien moeten we dan toch kijken of er andere afspraken over gemaakt kunnen worden. In ieder geval moet worden nagegaan of het allemaal sneller kan. Als er een lek is geweest gedurende acht tot tien maanden en er vervolgens na ontdekking van dat lek wordt gezegd dat er eigenlijk niets is gebeurd, is mijn reactie daarop dat je dan niet beschikt over informatie betreffende die acht tot tien maanden. Ik denk dan ook dat het beter is dat mensen hun DigiD-code veranderen, maar goed, dat is mijn persoonlijke mening. De manier waarop het nu gaat, vind ik in ieder geval niet zorgvuldig genoeg.

Minister **Plasterk**: Mevrouw Oosenbrug pleit eigenlijk voor een algemene meldingsplicht. Dat is echter iets wat ligt op het terrein van V en J en zou dan ook in dat kader bediscussieerd moeten worden. Mijn duit in het zakje zou dan zijn de afweging tussen de vraag hoeveel paniek je veroorzaakt en de vraag hoeveel handelingsperspectief er is en hoeveel reden er is om te denken dat mensen er daadwerkelijk schade door hebben opgelopen. Daar zou je misschien toch een balans in moeten vinden. Dat zou dan nieuwe regelgeving op dat terrein moeten opleveren. In het onderhavige geval was het theoretisch denkbaar en dus praktisch ook mogelijk dat iemand van die zwakte gebruik heeft gemaakt om te proberen gegevens over mensen die inlogden te verkrijgen, maar is er geen enkele reden om te denken dat dit ook is gebeurd. Dat is toch de conclusie. Op de vraag of je dan volledig kunt uitsluiten dat het is gebeurd, zegt de wetenschapper

in mij: nee, dat kun je natuurlijk nooit uitsluiten. Alleen, we hebben geen enkele reden om te denken dat het is gebeurd. Je ziet in de regio en de desbetreffende gemeenten geen toename van fraude op dit punt. We krijgen er ook geen meldingen over, ook sindsdien niet. Ik denk wel dat we ervan moeten leren. Deze fout mag sowieso niet meer gemaakt worden. De opmerking dat het nog sneller aan de politiek gemeld had moeten worden, neem ik ook ter harte, maar ik wil dat niet in verwijtende zin doen. Zoals het is gebeurd, kan het wat mij betreft, namelijk onmiddellijk afsluiten, kort inventariseren wat de situatie is geweest en dan mij informeren waarna ik de Kamer heb geïnformeerd. Maar goed, hoe sneller hoe beter. Daar leren we dan ook weer van.
Op een aantal punten ben ik al bij interruptie ingegaan. Ik ben het met de heer Moors eens dat elk door hem genoemd incident zorgwekkend is. Over afsluiten heb ik gezegd dat dat moet gebeuren als het gaat om een acuut geval waarin men zich niet aan de regels houdt. Het CMS-lek zullen we aan het assessment toevoegen. Het zou een hoop problemen oplossen als alle gemeenten dezelfde software zouden krijgen. Maar de Kamer snapt al wat er dan gebeurt: dat stuit in eerste instantie op bezwaren in het kader van de gemeentelijke autonomie. Maar goed, we zijn hierover in gesprek met de VNG, ook met het oog op Digitaal 2017, waarvoor we een uitstekende commissaris hebben. Dit is typisch zo'n onderwerp waarbij we proberen via zachte, gevolgd door middelharde overreding gemeenten ertoe te brengen om gewenst verdrag te gaan vertonen, waarbij ik nog even afzie van de financiële voordelen die optreden als wordt voorkomen dat in alle gemeenten het wiel wordt uitgevonden. Er is gevraagd om bredere voorlichting, bijvoorbeeld over het inloggen. Die suggestie zal ik meenemen en ik zal er misschien bij een volgende gelegenheid op terugkomen. Ik zal laten onderzoeken of het mogelijk is dat je dat bij elke inlog moet doen of alleen bij de eerste inlog.
In een aantal postcodegebieden bleek opeens dat er met DigiD was gefraudeerd, omdat men de brieven met inlogcodes uit de brievenbussen viste. In die postcodegebieden worden die brieven nu per koerier thuisbezorgd. Dat kost ongeveer € 10 per keer. We hebben nog geen aanwijzingen dat er een waterbedeffect optreedt. Er zijn ook heel brave regio's waar dit nog nooit heeft gespeeld. Ik wil deze zaak goed in de gaten houden. Als deze problemen zich in een nieuwe regio voordoen, zullen we onmiddellijk overgaan op dat wat kostbaarder systeem van thuisbezorging. Als blijkt dat het probleem zich voortdurend verplaatst, komt er misschien een moment waarop we zeggen: ho, zo kan het niet meer. Wij verplichten DigiD min of meer en daarom wil ik proberen te voorkomen dat dat € 10 per keer kost als het niet hoeft. Maar ik ben het eens met de heer Moors, die stelt dat dat niet opgaat als het probleem zich van de ene wijk verplaatst naar een aanpalende wijk. Ik zeg toe dat we onmiddellijk een postcodegebied zullen toevoegen als er daarvoor aanwijzingen bestaan.
De heer Verhoeven stelde een vraag over het openbaar maken. Ik heb daar voor een deel op gereageerd. De betrokken gemeente is overigens onmiddellijk geïnformeerd. Dat fraudegeval van een jongen van 15 jaar is natuurlijk schrijnend. Die jongen zou dus drie kinderen hebben verwekt. Dan zou er in principe bij de betrokken instanties al een rode lamp moeten gaan branden. Dan kom je eigenlijk op de meer algemene vraag hoe je fraude moet zien te voorkomen. Minister Opstelten heeft het voortouw genomen voor een heel uitgebreid fraudebestrijdingsprogramma, waarbij ik volledig ben aangehaakt, om ook balie- en gemeentepersoneel fraudebewust te maken. Daarvoor worden cursussen georganiseerd. Nog niet zo heel lang geleden heb ik op de 36ste etage van een gebouw in dat kader wat diploma's uitgereikt aan een lichting baliemedewerkers die die cursus heeft gevolgd. Dat geval van die jongen van 15 jaar met drie kinderen is typisch een geval voor de schoolboekjes. Hierbij gaat het om het opstellen van risicoprofielen.

Dan kom ik toe aan een heel technische vraag over het certificaat SHA (Secure Hash Algorithm)-4. DigiD maakt gebruik van het moderne en veilige SHA-256. Wat is gesignaleerd over dat andere algoritme kan waar zijn, maar daarop is DigiD gelukkig niet te pakken. Verder is gevraagd of de authenticatie voor de Staat niet minstens het niveau van dat van de banken zou moeten hebben. Als je toegaat naar een SMS-authenticatie heb je in feite dezelfde authenticatie als bij een tancode. De burger kan daar nu al voor kiezen. We brengen de instellingen op de hoogte van die keuzemogelijkheid. Verder kijken we of we dat via een app zo toegankelijk kunnen maken dat we in 2015 het beveiligingsniveau «midden» – dat hanteren de banken immers in feite – algemener van toepassing kunnen maken. Als dan blijkt dat het gebruikersvriendelijk genoeg is, kun je het alsnog geheel of gedeeltelijk verplicht stellen. Maar ik zou dit eerst mogelijk willen maken voor burgers.
Ik heb gereageerd op de vraag van mevrouw Gesthuizen over het data management system. Zij zei terecht dat we niet moeten doen alsof het een probleem van de burger is. Het is niet zo dat, als we de burger maar goed informeren, het niet meer voorkomt. Het moet van twee kanten komen. Je kunt niet anders doen dan burgers te attenderen op de gevaren van verdachte e-mails. Dat doen banken ook. Maar tegelijkertijd moeten de gemeenten ook op de hoogte worden gebracht. Daar zijn we actief mee bezig.
Mevrouw Gesthuizen had aarzelingen over de oefentool. Op werkbezoek bij de sociale dienst in Rotterdam bleek mij dat sommige mensen niet weten hoe DigiD werkt. De sociale dienst heeft daarvoor oefenprogramma's opgezet, zodat deze mensen leren hoe ze zelf hun DigiD kunnen maken. Ik vond het interessant om dat mee te maken. Als ze er even de tijd voor nemen, vinden veel mensen dat ook interessant. Er zullen altijd mensen zijn die dat dan weer vergeten. Natuurlijk moet er dan iemand hulp bieden. Veel gemeenten hebben zogenaamd geen loketten meer, maar ze hebben wel een hulpplek, waar kan worden ingelogd op een virtueel loket. Maar het uitgangspunt dat DigiD nu zo belangrijk is dat iedereen zijn eigen DigiD moet kunnen aanmaken, vind ik eigenlijk wel goed. In mijn waarneming werken die cursussen ook wel.

Mevrouw **Oosenbrug** (PvdA): Ik werd getriggerd door dit mooie betoog van de Minister. U zult het niet geloven, maar mijn vader heeft noch een computer, noch een smartphone. Als hem om zijn DigiD wordt gevraagd, help ik hem meestal. Maar zo voeden wij de mensen niet op, dus u doet net alsof u dit niet hebt gehoord. Mijn vader staat daar natuurlijk niet alleen in. In de brief over digitale versterking heb ik een hoofdstuk gemist over mensen zonder computer en smartphone. Is daar al over nagedacht of moet ik daar binnenkort nog eens naar vragen?

Minister **Plasterk**: Deze vraag is eigenlijk onderdeel van een grotere vraag: als we toewillen naar Digitaal 2017, hoe gaan we dan om met mensen die geen computer hebben? Nederland is immers een vrij land. Ik wil dit in stappen opbouwen. Voorheen ging het schriftelijk, waarover je de vraag kunt stellen wat mensen doen die geen pen hebben. Op een gegeven moment wordt het – dat is stap één – onderdeel van burgerschap dat je op de een of andere manier toegang hebt tot het internet. Als we al het reguliere verkeer tussen overheid en burger digitaal willen maken, is het wel de bedoeling dat de burger die toegang heeft. Met die eerste stap zijn we inderdaad niet klaar. Als je geen computer of smartphone hebt, kun je overwegen er een aan te schaffen. Voor de meeste burgers wordt toegang tot het internet een van de gereedschappen waarover ze beschikken. Er zullen redenen zijn waarom mensen daar toch niet over beschikken – dat kan de leeftijd zijn, maar het hoeft niet – maar dan nog geldt voor veel mensen dat ze een slim iemand in de omgeving hebben die dat voor hen wil doen. Dat vind ik op zich een begaanbare weg. Als

dat er allemaal niet is – dat is stap drie – dan mag het niet zo zijn dat iemand geen AOW krijgt omdat hij niet digivaardig is en ook geen digivaardigheid in zijn omgeving heeft. Dan moet het mogelijk zijn om bij de gemeente aan te kloppen. Dan nog vind ik dat de gemeente aan betrokkene moet vragen of het niet beter is om een computer aan te schaffen. Maar als mensen dat om wat voor reden dan ook niet willen, moet er altijd een analoog vangnet zijn. Ik bouw het bewust in die volgorde op, want als je te snel wilt gaan, bereik je minder snel de doelstelling om in principe zo veel mogelijk digitaal te regelen.
Mevrouw Oosenbrug vraagt of, los van de vraag wie de schuldige is, de overheid altijd moet opdraaien voor de schade. Ik vind dat de overheid, als mensen onverstandige dingen hebben gedaan en zich melden bij het Centraal Meld- en Informatiepunt Identiteitsfraude en -fouten, beschikbaar moet zijn om te vertellen wat ze daaraan moeten gaan doen. Ik zou het een verkeerde prikkel vinden om te stellen dat de overheid altijd opdraait voor de schade. Als iemand zijn huissleutels ergens laat liggen, geldt ook een eigen verantwoordelijkheid. Zo algemeen als mevrouw Oosenbrug het zegt zou ik het niet willen stellen, maar de overheid moet burgers daarin wel steunen.

De heer **Moors** (VVD): Voorzitter. Ik heb nog geen antwoord gehad op mijn vraag of de Minister ook assessments wil houden nadat er nieuwere softwareversies zijn verschenen. Dan voorkom je dat iets langere tijd niet wordt geconstateerd. Ik heb wel gehoord dat de Minister de reikwijdte wil uitbreiden tot het CMS. Zou de veiligheid van DigiD niet onafhankelijk moeten zijn van de veiligheid van systemen bij gemeenten? Als een website niet veilig is, wordt iDEAL ook niet gehackt. Het systeem zou zo moeten worden ingericht dat beide aspecten onafhankelijk van elkaar zijn. Graag een reactie daarop.
De meeste problemen met DigiD hebben te maken met hack, lek of diefstal van gegevens. Met de drie door mij genoemde maatregelen kan dat worden opgelost. Ik doel om te beginnen op verbetering van het uitgifteproces, de Two-Factor Authentication, dus via een sms of een app en voorlichting om te voorkomen dat burgers gespoofte sites gebruiken. De Minister geeft heel kort door de bocht aan dat een sms veel te veel kost. Ik heb snel uitgerekend dat hij er daarbij vanuit gaat dat het € 0,10 per authenticatie kost als je alle authenticaties met een sms zou doen. Ik heb het gevoel dat het, gelet op de schaalgrootte, goedkoper kan. Welke in de afgelopen jaren voorgekomen schadegevallen zouden met de door mij genoemde drie maatregelen zijn voorkomen en welke schade zou daarmee gemoeid zijn geweest? Dat zouden we dan eens tegenover een realistische inschatting van de kosten van die maatregelen moeten zetten. Ik ben benieuwd naar de businesscase op dit punt. Hoewel ik het dan puur over het financiële aspect heb, lijken me zaken als vertrouwen in de overheid en de digitale dienstverlening ook heel wat waard. Dat bedoel ik ook in financiële zin, want als die digitale dienstverlening veel wordt toegepast, is dat ook een grote kostenbesparing op de bedrijfsvoering van de overheid. Graag een reactie, eventueel later in een brief.

De heer **Verhoeven** (D66): Voorzitter. Ik dank de Minister, hoewel hij toch een aantal belangrijke vragen van mij niet heeft beantwoord. Om te beginnen heb ik om een grondig onderzoek gevraagd. Ik wil toch echt weten of de Minister van mening is dat in zo'n korte tijd nooit een grondig onderzoek kan hebben plaatsgevonden op het niveau dat nodig is om hier zekerheid te bieden. Verder heb ik gevraagd of er naast de twaalf gemeenten ook nog andere organisaties zijn geweest met een vergelijkbaar lek. De Minister zegt, in antwoord op mijn vraag over algoritmes, dat DigiD SHA-256 heeft. Maar dat gaat over hashing, wat iets heel anders is dan bulkversleuteling, waarvoor inderdaad RC4 als algoritme wordt gebruikt. Als ik aan de groenteman vraag of hij lekkere appelen heeft, zegt

hij niet dat zijn peren heerlijk zijn. Ik wil weten hoe zijn appels zijn. Dat gaat over bulkversleuteling, het verschil tussen applicatie en de digitale vingerafdruk.
Wat gaat de Minister nou precies doen? Hij vindt ook dat een periode van veertien maanden te lang is. Maar wat gaat er in de praktijk veranderen om ervoor te zorgen dat dingen sneller worden waargenomen, dat gemeenten sneller druk zetten en sneller handelen, zodat de periode van veertien maanden korter wordt? Wat mij betreft geldt dat ook voor de periode waarin de Minister reageert op meldingen van bijvoorbeeld white hat hackers. Zij zijn te goeder trouw en hebben het gevoel dat er hautain en laconiek wordt gereageerd. Dat vind ik geen goed signaal.

Mevrouw **Gesthuizen** (SP): Voorzitter. Het is overduidelijk dat de Minister van zeer goede wil is. Daar schort het absoluut niet aan. Het kabinet doet twee zaken niet of juist te veel. Bij debatten over ICT dringen wij er steeds vaker op aan om degenen die diensten aanbieden – dat zijn heel vaak bedrijven – ervoor te laten zorgen dat die diensten ook echt veilig zijn. Er moet een soort veiligheidsassessment plaatsvinden, zodat het niet meer mogelijk is dat mensen bijvoorbeeld ingaan op phishing mails. Daar zijn verschillende manieren voor. Gaat de Minister bij alles wat hij laat ontwikkelen ervoor zorgen dat de resultaten daarvan op zo'n manier in de markt worden gezet dat we er niet van uit hoeven te gaan dat burgers continu wantrouwend en achterdochtig zijn? Mogen we ervan uitgaan dat dat, met een beetje basiskennis, gewoon goed komt?
Volgens mij heb ik geen antwoord gekregen op mijn vraag over compensatie. Banken gaan daar in het algemeen best netjes mee om: als mensen slachtoffer van fraude zijn geworden, worden ze gecompenseerd. Hoe ziet de Minister zijn verantwoordelijkheid hierin en waar legt hij precies de grens? Als je willens en wetens alles over jezelf hebt uitgeleverd, terwijl je beter had moeten weten, kan ik me voorstellen dat je daar als overheid vraagtekens bij zet, maar anders moeten slachtoffers niet zelf voor de kosten opdraaien.

Mevrouw **Oosenbrug** (PvdA): Voorzitter. Ik vind het een beetje tegenstrijdig dat we aan de ene kant via een rits maatregelen proberen fraude te bedwingen door de burger op te roepen zichzelf te versterken, terwijl we aan de andere kant ook iets van de overheid vragen. Ik noem nog een keer het voorbeeld van mijn vader, die inmiddels tegen de 80 loopt. Ik ga hem niet dwingen om nog een computer of een smartphone aan te schaffen, want hij kan prima uit de voeten met zijn huidige telefoon. Ik moet hem dan een bepaalde kant op gaan dwingen. Desnoods koop ik zelf een computer voor hem en leer ik hem hoe het werkt. Maar of hij ooit zo gehaaid wordt dat hij begrijpt dat er een «s»-je ontbreekt omdat een SSL-verbinding niet goed werkt, betwijfel ik. Je kunt dan wel zeggen dat je ook een pen moet hebben, maar dat vind ik toch wat anders dan een computer. Met een pen kan ik veel minder schade aanrichten dan met een computer. Wij vinden dat iedereen maar mee moet doen en als dat niet kan, moet je maar een cursus volgen. Wel zorgt de overheid voor een vangnet. Ik vind het zelf een beetje een negatieve boodschap, wat ik wel jammer vind. Ik ben zelf een ongelooflijke fan van alles wat digitaal is, maar ik weet ook dat een hele groep mensen moeite heeft om aan te haken. Die groep moeten we zorgvuldig begeleiden. Ik hoop dat de overheid daar oog voor heeft.

Minister **Plasterk**: Voorzitter. De heer Moors vraagt of het mogelijk is om ook een assessment te doen als er nieuwe softwareversies worden geïnstalleerd. Gehoord het debat denk ik dat we dat moeten doen. Ik zeg toe dat we dat zullen aankaarten bij de gebruikers. Dat is nieuw, omdat we dat tot nu toe eens per jaar hebben gedaan. Nu er zo veel aandacht voor is, wil ik voorkomen dat er tijdens een update tussendoor een aantal

maanden iets openstaat. Het mag niet zo zijn, vindt de heer Moors, dat afhankelijk van de kwaliteit van de website van een gemeente DigiD wordt gekraakt, want dat gebeurt bij iDEAL ook niet. DigiD is niet gekraakt; er zat een zwakte in het CMS, waardoor je kon zien wat mensen aan het invoeren waren. Daarmee kom je niet aan het hele DigiD-systeem als zodanig, maar potentieel zou je wel aan de invoergegevens van mensen op die site kunnen komen. Dat kan natuurlijk niet, zodat dat onmiddellijk gerepareerd moet worden. De heer Moors vroeg naar de businesscase op dit punt, uitgaande van € 10 per keer en een sms-verificatie van een dubbeltje per keer. Hij vroeg hoeveel ellende daarmee wordt voorkomen. Zijn derde stap is het geven van meer voorlichting.
Volgens mij doen we wat mogelijk is. De heer Moors zei dat hij de businesscase op papier wil krijgen. Ik zeg toe dat ik dit in een brief zal doen, maar dat zal even werk zijn. We moeten een en ander serieus onderbouwen. Dat kan ik dus niet volgende week doen. Ik denk aan het begin van het komende jaar. Dan hebben we een paar maanden. Mag dat? Ik wil het even serieus laten bekijken.

De heer **Moors** (VVD): Ik vind het redelijk ruim. Volgens mij zijn heel veel gegevens bekend. Het zal misschien even werk zijn om ze op een rijtje te zetten. De Minister geeft aan dat gegevens ook kunnen worden afgevangen door een kwetsbaarheid in de gemeentelijke websites. Volgens mij voer je je gegevens in op de website van DigiD. Als je goed voorgelicht bent, weet je dat je ze alleen daarop moet invoeren. Volgens mij kan de website van DigiD dan bij de gemeentelijke website aangeven: deze persoon is wie hij zegt te zijn. Dat kan volgens mij zonder dat er wachtwoorden te zien zijn in een kwetsbaar gemeentelijk systeem. Zo zou het moeten werken. Als dat niet zo is, klopt er iets niet. Volgens mij zou de businesscase wat sneller moeten kunnen. De meeste gegevens zijn bekend. Het is een kwestie van de gegevens nog eens goed op een rijtje zetten. Ik kan me voorstellen dat het nog wat eerder kan.

De **voorzitter**: Het is aan de Minister om een toezegging te doen.

Minister **Plasterk**: We hebben er nog even over nagedacht. Ik stel voor dat we het voor eind januari doen. Voor de kerst wordt een beetje krap. Dan moeten we het binnen een paar weken uit de grond stampen. Voor eind januari wil ik wel toezeggen. Ik kom zo op een ander punt dat ik nog moet uitzoeken en dat ik misschien kan meenemen in deze brief.
De heer Moors zei dat de schade groter is dan alleen maar de financiële schade. Het vertrouwen in de overheid erodeert namelijk ook. Daar ben ik het mee eens. Als de businesscase neutraal is en we hiermee het een en ander kunnen voorkomen, zullen we het er snel over eens zijn dat we het moeten doen. We moeten een kosten-batenafweging maken. Daar heb ik even tijd voor nodig. Het is niet zo dat ik het pakket dat de heer Moors voorstelt, afzet tegen niets doen. Ik wil het afzetten tegen hetgeen ik zojuist heb genoemd, namelijk het introduceren van een identificatie-systeem in twee stappen. We kunnen proberen om daar een app voor te ontwikkelen. Hierdoor kunnen we de kosten sowieso sterk reduceren. Dat is de andere businesscase. Er is dus geen sprake van niks doen. Daar zijn we het allen achter deze tafel over eens.
De heer Verhoeven vroeg naar het onderzoek. Nadat Logius ernaar heeft gekeken, heeft Fox-IT er ook nog uitgebreid onderzoek naar gedaan. We hebben er geen sporen van gevonden dat er misbruik is gemaakt van de zwakte in de systemen. We hebben ook geen aanleiding om te denken dat andere organisaties een vergelijkbaar lek hadden.
Ik kom even niet uit de vraag van de heer Verhoeven over SHA-256. De heer Verhoeven heeft er meer verstand van dan ik. Dat is nooit de bedoeling, maar het kan wel. Wordt SHA-256 wel voor hashing maar niet voor bulkversleuteling gebruikt? Dat moet ik even uitzoeken.

De heer **Verhoeven** (D66): Het staat gewoon in het rapport «ICT-beveiligingsrichtlijnen voor Transport Layer Security (TLS)». Alle verschillende handelingen met de daarbij behorende algoritmes, mogelijkheden en systemen staan hierin op een rij. Op pagina 16 wordt zowel hashing als bulkversleuteling genoemd. Op pagina 33 staat uitgelegd wat het is. Dat weet de Minister vast ook. Ik had een vraag over het ene onderwerp maar hij gaf een antwoord over het andere onderwerp. Daar ben ik niet mee geholpen. Ik wil er gewoon helderheid over. Is er bij bulkversleuteling nog steeds sprake van RC4? Ik weet zeker dat een van de ambtenaren hier aan tafel zo het antwoord kan geven. Ik denk alleen dat ze het niet willen. Het is echter aan de Minister.

De **voorzitter**: Nu gaat u te ver in uw enthousiasme. U kunt ambtenaren niet van iets betichten terwijl ze zich niet kunnen verdedigen.

De heer **Verhoeven** (D66): Excuus voorzitter, daar hebt u gelijk in.

Minister **Plasterk**: Ik dacht dat we het antwoord niet zo snel konden produceren, maar ik heb mijn medewerkers onderschat. Het antwoord luidt namelijk als volgt: de encryptie van het ...

De heer **Verhoeven** (D66): Ik had dus wel gelijk!

De **voorzitter**: U had gelijk wat het kunnen betreft, maar niet wat het niet willen betreft.

Minister **Plasterk**: Het certificaat is inderdaad SHA-256 (hashing). RC4 is een SSL-encryptieprotocol. DigiD gebruikt dit nog omdat circa 5% van de burgers oude besturingssystemen of browsers gebruikt. Per 8 december 2014 wordt RC4 op DigiD uitgezet. Dat is al heel snel. Dat is het antwoord op de vraag. Dat hoeven we dus niet meer schriftelijk te geven.
Ik heb al gezegd dat we ervan moeten leren en nog sneller moeten reageren als dat mogelijk is. Het is zeer te waarderen als mensen zwakten signaleren in overheidssystemen. Het is niet gepast als hier laconiek of hautain op gereageerd wordt. Ik bevestig hiermee overigens niet dat dit in dit geval gebeurd is. Hierop is namelijk onmiddellijk actie ondernomen. Het zal echter weleens gebeuren, maar dat moet niet. Als mensen zich melden, moet de overheid dankbaar zijn dat zij dat doen. Het is ook goed dat mensen het niet misbruiken. Dat mag ook niet.

De heer **Verhoeven** (D66): Het laatste wat de Minister zegt, is misschien wel een van de belangrijkste dingen, naast zijn toezegging, onder anderen aan mijn collega van de VVD, over een aantal aanscherpingen. Er zijn heel veel goedwillende mensen zonder winstbejag die in dat wereldje bezig zijn, tegen dingen aanlopen en dingen horen en daarmee vervolgens naar de organisaties gaan die een en ander voor de overheid beheren. Ik ben heel blij dat de Minister zegt dat men daar nog opener en zorgvuldiger mee om zal gaan dan misschien tot nu toe is gebeurd. Geheel in lijn met de voorzitter, wil ik ook niet zeggen dat zijn ambtenaren het niet goed hebben gedaan. De Minister is echter verantwoordelijk voor de wijze waarop zijn organisaties het doen. Ik heb geluiden gehoord dat het soms beter kan. Er zullen ook heel veel dingen goed gaan. Ik ben blij met de opmerking van de Minister, want hiermee kunnen we een soort cultuur creëren waarin we samen overheidssystemen versterken. De overheid kan dat namelijk niet alleen.

Minister **Plasterk**: Dat onderstreep ik. Om zichtbaar te maken dat we het op prijs stellen, ook omdat we er feitelijk wat aan hebben, hebben we in april dit jaar een hackathon georganiseerd. Mevrouw Oosenbrug zat daarbij in de jury. Hierbij hebben we mensen uitgenodigd om naar zwakke

plekken te kijken en om suggesties aan te dragen voor verbeteringen. Een aantal daarvan zijn vervolgens ook opgepakt en in de praktijk gebracht. Een voorbeeld daarvan is de KopieID-app, waarmee je je burgerservicenummer kunt doorhalen op een kopie van je identiteitsbewijs. Het is een heel simpele app. Vier jongemannen die aanwezig waren, hebben dit idee aangedragen als een van de mogelijkheden om een zwakte weg te nemen. Mensen maken snel een fotootje met hun smartphone en delen die. Dankzij die app kunnen ze nu hun bsn doorhalen.
In zijn algemeenheid juichen we dit soort initiatieven dus toe. Ik onderstreep dit nogmaals. Mocht het ergens in die heel grote overheid, in de verschillende overheidslagen, niet goed gaan, dan is het niet goed.
Mevrouw Gesthuizen vroeg of we de veiligheid niet veel meer voorop moeten stellen. Moeten we daar niet meer aan doen? Dat is ook de bedoeling van DigiD Midden, het nieuwe beveiligingsniveau waar we voor volgend jaar aan werken. We proberen het praktisch zo te maken dat je, net als bij het betalingsverkeer, meer moet doen dan alleen maar je password typen. We gaan er één beveiligingsniveau boven zitten. Het kan in ieder geval voor de vitale toepassingen op die manier gebeuren. Zo kun je die beschermen. Die kant willen we op.
Mevrouw Gesthuizen vroeg heel scherp wie de schade draagt in welk geval. Ik heb al gezegd dat mensen ondersteuning verdienen van bijvoorbeeld het CMI, ook als ze zelf onverstandige dingen hebben gedaan. Het CMI is er bij het ministerie actief mee bezig. Als het echter om schade gaat, is de digitale wereld niet anders dan de gewone wereld. Het hangt af van de vraag in welke mate iets verwijtbaar is en in welke mate iemand verantwoordelijk is. Als de gemeente iets fout heeft gedaan waardoor mensen gedupeerd zijn, ligt de verantwoordelijkheid, lijkt mij, bij de gemeente. Als mensen zelf iets fout hebben gedaan, ligt de verantwoordelijkheid misschien bij hen. Soms is er sprake van een gemengde verantwoordelijkheid. We gaan langzaam van de analoge wereld en het analoge handelen over op de digitale wereld, maar ik wil het civiel recht voor schadegevallen niet herschrijven. Dat blijft op dezelfde manier van toepassing.

Mevrouw **Gesthuizen** (SP): Ik kan er nog net geen genoegen mee nemen. Ik zei al dat de Minister van hartstikke goede wil is, maar wat gebeurt er als je als burger slachtoffer bent geworden van een fraudeur? Stel dat er bij een messengerservice iets is ingebouwd waardoor iemand met jou heeft kunnen meekijken? Wat gebeurt er als je op die manier gedupeerd bent?

Minister **Plasterk**: Ik begrijp de vraag. Stel echter dat je het woord «digitaal» weglaat en de vraag in het algemeen stelt: wat gebeurt er als je slachtoffer bent geworden van een fraudeur, bijvoorbeeld van iemand die aan de deur komt? Dan moet een rechter uiteindelijk bekijken of iemand het had kunnen voorkomen. Is het persoonlijk verwijtbaar of komt het door een ander? Ik kan niet in zijn algemeenheid toezeggen dat de schade altijd door de overheid wordt vergoed, ongeacht de persoonlijke verantwoordelijkheid. Dan neem je voor mensen de prikkel weg om de achterdeur op slot te doen, en dus ook de digitale achterdeur. Ik snap de vraag wel. Er zijn wel treurige situaties geweest. Die heb ik ook gezien. Vorige week waren er bij Radar ook mensen die slachtoffer waren geworden van digitale schade. Die hebben de schade overigens wel kunnen verhalen. Veel van die zaken zijn namelijk wel terug te draaien. Als er op jouw kosten dingen zijn besteld en je kunt aantonen dat je dat niet zelf hebt gedaan, is het uiteindelijk aan de leverancier om te bewijzen dat je het wel hebt besteld. Je kunt zeggen dat de leverancier zich er onvoldoende van heeft vergewist dat de betrokkene was wie hij zei te zijn. Dan moet de handeling worden teruggedraaid of moet het product terug.

Ik kan deze vraag echter niet in zijn algemeenheid beantwoorden, hoe graag ik dat ook zou doen.

Mevrouw **Gesthuizen** (SP): De Minister zegt heel veel, maar de bottomline is volgens mij dat de overheid minder toeschietelijk is op dit punt dan bijvoorbeeld de banken zijn.

Minister **Plasterk**: De vraag is ook anders. Laat ik het breder maken dan DigiD. Als mensen met de informatie die de overheid ter beschikking stelt voor hun identiteit, een product kopen bij een willekeurig bedrijf of een leverancier, kan de overheid niet op voorhand alle schade op zich nemen. Het CMI treedt op als regisseur en kan waar nodig andere instanties, zoals de politie, het Expertisecentrum Identiteitsfraude en Documenten van de Koninklijke Marechaussee, de Belastingdienst en Logius, attenderen op zaken, advies geven op maat en ervoor zorgen dat mensen krijgen waar ze recht op hebben. Ik kan echter niet, hoe graag ik het ook zou willen, in mijn beantwoording in tweede termijn het burgerlijk recht veranderen. Ik kan niet zomaar zeggen dat we de verantwoordelijkheid voortaan op een bepaalde plek neerleggen.

Mevrouw **Oosenbrug** (PvdA): Ik hoor heel veel en dan gaat het bij mij malen. Ik ken veel ethische hackers. Ik praat veel met hen. Ethisch hacken is een van de onderwerpen die ik warm omarm. Hierdoor weet ik dat er veel dingen kunnen gebeuren die vervolgens een tijdje weggestopt worden. Laat ik even terugkomen op een lek in DigiD. Stel dat men een file aanmaakt waarin de session-ID's opgeslagen zijn. Vervolgens gaat men pas na een jaar, als het rustig is geworden, proberen om dat filetje na te lopen en in te loggen. Hoe kan ik bewijzen dat mijn ID een jaar geleden tijdens een sessie gejat is? Ik sluit hiermee aan bij de vragen van de SP-fractie. De vraag wie hiervoor verantwoordelijk is, is veel lastiger te beantwoorden dan in het echte leven. Als er geen goede regels voor zijn en er geen goede afspraken over zijn, moeten we daarover misschien toch een keer debatteren. Het gaat om de schuldvraag. Mij overkomt iets, maar ik weet niet dat dit is gebeurd. Dat blijkt pas een jaar later. Moet ik dan vervolgens voor de schade opdraaien? Hoe kan ik bewijzen wat er is gebeurd?

Minister **Plasterk**: Volgens mij willen we allen hetzelfde. Mensen die zich netjes hebben gedragen en niks doms hebben gedaan, moeten geen schade ondervinden als er ergens anders een fout is gemaakt. Als mensen echter tegen alle adviezen in essentiële informatie al te gemakzuchtig delen, zal de overheid niet blind en op voorhand alle schade vergoeden. Er zijn veel voorbeelden van schadeloosstelling door de Belastingdienst en de Sociale Verzekeringsbank. Er zijn veel trieste gevallen bekend waarin een en ander voor de mensen is opgelost. Ik hoop echter dat er ook begrip voor is dat ik niet op voorhand kan zeggen dat mensen in alle gevallen schadeloos moeten worden gesteld. Ik ga niet over de aansprakelijkheid. Een gedupeerd bedrijf moet ook de mogelijkheid hebben om toch betaald te krijgen, bijvoorbeeld als iemand zijn huisgenoot telefoongesprekken heeft laten voeren. Dat had hij niet moeten doen. Die telefoongesprekken moeten toch betaald worden. Die persoon moet het dan zelf betalen of moet het met zijn huisgenoot oplossen. Ik geef een extreem voorbeeld. In ander gevallen kan het evident zijn dat iemand er niks aan kan doen. Dan moet het natuurlijk worden opgelost. Daartussen zitten grijstinten. Als er een zaak van komt, is het aan de rechter om erover te oordelen.

De **voorzitter**: Mijnheer Moors, u mag nog een korte vraag stellen, maar daarna gaat de Minister zijn beantwoording echt afmaken.

De heer **Moors** (VVD): We focussen nu op de vraag wat je allemaal kunt doen als er fraude wordt gepleegd. De Minister heeft het gehad over postcodegebieden, het uitbreiden ervan enzovoorts. Moeten we niet veel meer inzetten op het voorkomen in plaats van op het genezen?

Minister **Plasterk**: Ja. Daar heb ik ook over gesproken. In de schriftelijke voorbereiding heb ik ook geschreven over het verbeterprogramma voor DigiD. Er wordt continu gewerkt aan het voorkomen. Ik ging echter even mee in de casus dat er toch schade ontstaat, ondanks alle pogingen om deze te voorkomen. Schade kan ook ontstaan door onachtzaamheid. Dan ligt het niet aan de manier waarop een stelsel is ingericht, maar aan mensen die onverstandige dingen doen. Het ging om de vraag of die weging mag plaatsvinden voordat je besluit tot een schadeloosstelling of niet. Ik heb aan mevrouw Oosenbrug geantwoord dat je er volgens mij niet aan ontkomt om soms een weging te doen.
Dat brengt mij bij een andere vraag van mevrouw Oosenbrug. Hoewel zij voorstander is van het digitale stelsel en het digitale tijdperk, blijft zij eraan twijfelen of je dit allemaal van burgers kunt vragen. Ik heb geprobeerd om een en ander in drie trappen in te delen. Voor de derde trap ben ik het ermee eens. Uiteindelijk moet er altijd een achtervang zijn. Je kunt wel vragen van mensen dat ze het op een bepaalde manier doen, maar soms gebeurt het niet. Dat mag dan niet betekenen dat ze hun burgerrechten verliezen. Dat is duidelijk. Ik hoop dat er ook begrip voor is dat we niet te snel zeggen dat het digitale niet hoeft als mensen daar niet zo van zijn. Dan kunnen mensen als ik ook denken: ik heb een druk leven; ik wacht wel tot het in de bus komt. Op die manier laten we de doelstelling los, maar die wil ik behouden. Als het kan, moeten mensen zo veel mogelijk zelf digitale interactie met de overheid hebben. Als ze het niet zelf kunnen, moeten we accepteren dat iemand in hun omgeving hen erbij helpt. Als dat ook niet kan, moeten we van overheidswege ervoor zorgen dat mensen niet in de kou blijven staan. Langs die drie trappen wil ik het opbouwen. Ik kijk even of ik mevrouw Oosenbrug overtuigd heb.

De **voorzitter**: Mevrouw Oosenbrug, het is niet de bedoeling dat we de hele tijd heen en weer blijven praten. Ik wil toch de orde van de vergadering hanteren. U krijgt nog de gelegenheid voor een korte vraag.

Mevrouw **Oosenbrug** (PvdA): Dank u wel, voorzitter. Het is niet zo zwart-wit: mensen willen het wel of willen het niet. Soms willen mensen wel, maar kunnen ze het gewoon niet. Dat moeten we hier een keer helder zeggen. De wereld wordt al de hele tijd verdeeld in twee partijen, maar het is niet zo zwart-wit. Mijn vader wil het volgens mij ook wel, maar ik doe het liever zelf. Ik laat hem liever niet los op internet. Dat heeft ook met zijn ogen en met andere zaken te maken. Ik wil in ieder geval duidelijk maken dat het niet zo zwart-wit is. Daar moeten we wel oog voor blijven houden.

Minister **Plasterk**: Daar ben ik het helemaal mee eens. Ik probeerde alleen het dilemma te delen. We kunnen alle druk van Digitaal 2017 afhalen en zeggen: bij die loketten spreek je nog eens iemand. Als je er zo laconiek over spreekt, zul je je doelstelling niet behalen. Tegelijkertijd wil je dat mensen alles krijgen waar ze recht op hebben, ook wanneer ze niet zelf, of met mensen in hun omgeving, in staat zijn digitale interactie te organiseren. Ik probeer het juist niet zwart-wit te behandelen. Ik heb drie trappen aangegeven. De derde categorie bestaat uit mensen die er op de een of andere manier niet toe komen. Ze willen het misschien wel, maar het komt er niet van. Voor hen moet je een mogelijkheid creëren. Daar ben ik het helemaal mee eens. Ik wil echter niet de doelstelling loslaten. Ik heb de indruk dat mevrouw Oosenbrug die ook niet wil loslaten. Mensen moeten even een drempel over, maar als ze eroverheen zijn, is het uiteindelijk ook weer gemakkelijk. Dat geldt voor een heel grote categorie

van mensen. Je houdt echter altijd een groep mensen over voor wie het anders moet.

De **voorzitter**: Dat was de beantwoording van de Minister in tweede termijn. Mevrouw Gesthuizen mimede naar mij dat zij een VAO wil. Ik kijk even of we dit wellicht nog met een vraag aan de Minister kunnen voorkomen.

De heer **Verhoeven** (D66): Nee.

De **voorzitter**: Mijnheer Verhoeven, u hebt het VAO niet aangevraagd. Mevrouw Gesthuizen heeft dat gedaan. Mijn opdracht als voorzitter is om in ieder geval een poging te doen. Daarom vraag ik mevrouw Gesthuizen of dat mogelijk is. Zo niet, dan zal er een VAO gepland worden, met als eerste spreker mevrouw Gesthuizen.

Mevrouw **Gesthuizen** (SP): De Minister en ik hebben net uitvoerig van gedachten gewisseld over de vraag waar de grens ligt bij frauderen. Ik heb het gevoel dat de Minister hierbij wel een steuntje in de rug kan gebruiken vanuit de Kamer. Daar zal het dus over gaan.

De **voorzitter**: Ik kijk naar de Minister. Ik denk niet dat het VAO te voorkomen is.

Minister **Plasterk**: Ik kan het niet repareren. Ik ben wel verantwoordelijk voor het digitaliseren van de overheid maar niet voor de aansprakelijkheid. Als ik mevrouw Gesthuizen goed begrijp, richt zij zich daarop. Dat is echt een kwestie van civiel recht. Ik kan hier onmogelijk de toezegging doen, zelfs niet met een steuntje in de rug van de Kamer, dat de overheid voortaan alle schade in fraudegevallen op zich neemt. Dat zullen we dan maar plenair met elkaar moeten bespreken.

Mevrouw **Gesthuizen** (SP): Uitstekend. Daar zal ik bij de formulering van een eventuele motie ook zeker rekening mee houden.

De **voorzitter**: Er wordt dus een VAO aangemeld, met als eerste spreker mevrouw Gesthuizen.
Wij zijn gekomen aan het einde van dit algemeen overleg, met de toezegging van de Minister dat hij eind januari een brief zal sturen waarin de businesscase beveiligingskosten nader zal worden uitgewerkt. Ik dank de leden voor hun inbreng. Ik dank de Minister en zijn staf voor de beantwoording en ik dank de mensen op de publieke tribune voor hun belangstelling.

Sluiting 17.45 uur.