Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2011–2012

26 643 Informatie- en communicatietechnologie (ICT)

Nr. 230

BRIEF VAN DE MINISTER VAN BINNENLANDSE ZAKEN EN KONINKRIJKSRELATIES

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 14 maart 2012

In het najaar van 2011 werd Nederland, en de Nederlandse overheid, opgeschrikt door een incident bij DigiNotar. DigiNotar was een bedrijf dat certificaten leverde waarmee elektronisch berichtenverkeer via internet werd beveiligd. Over de maatregelen die toen zijn getroffen om de gevolgen van het incident te bestrijden, bent u geïnformeerd middels twee brieven[1] en tijdens een plenair debat met uw Kamer op 13 oktober 2011. Om van het incident te kunnen leren, heb ik samen met collega's, een aantal onderzoeken laten uitvoeren. Ik heb u in mijn brief van 2 februari jl.[2] over de voortgang van deze onderzoeken geïnformeerd. Ter voorbereiding op het geplande Algemeen Overleg met uw Kamer op 20 maart 2012 bied ik u, mede namens de minister van EL&I, de resultaten van een drietal onderzoeken aan.[3]

Twee onderzoeken zijn onder mijn verantwoordelijkheid uitgevoerd:

1. Onderzoek naar de opzet, werking van en toezicht op de twee gereguleerde Public Key Infrastructure (PKI) stelsels: PKIoverheid en het stelsel van gekwalificeerde certificaten, alsmede het toezicht hierop. Dit onderzoek is mede in opdracht van de minister van Economische Zaken, Landbouw & Innovatie uitgevoerd. Onderzocht is welke risico's de stelsels bevatten, of de normenkaders nog toereikend zijn, of de toezichtarrangementen adequaat functioneren en of er alternatieve technologieën voor PKI zijn. Dit onderzoek is uitgevoerd door Logica.
2. De Rijks Audit Dienst heeft onderzocht of de betrokken overheidspartijen in de PKI-stelsels gegeven de bestaande taken en verantwoordelijkheden alert gereageerd hebben inzake DigiNotar.
3. Daarnaast is onder verantwoordelijkheid van de minister van Economische Zaken, Landbouw & Innovatie onderzoek gedaan naar de veiligheid van de diensten in de Digitale Agenda.nl. Dit onderzoek is uitgevoerd door Collis/HEC. Gelet op de samenhang met de andere onderzoeken, doe ik u hierbij ook dit rapport toekomen ten behoeve van een integrale behandeling door uw Kamer.

[1] Kamerstukken II, 2011–2012, 26 643, nr. 188 en189
[2] Kamerstukken II, 2011–2012, 26 643, nr. 222
[3] Ter inzage gelegd bij het Centraal Informatiepunt Tweede Kamer

kst-26643-230
ISSN 0921 - 7371
's-Gravenhage 2012

In het vervolg van deze brief zal ik per onderzoek ingaan op de onderzoeksvraagstelling, de belangrijkste bevindingen en de maatregelen, die te nemen of nader te onderzoeken zijn.

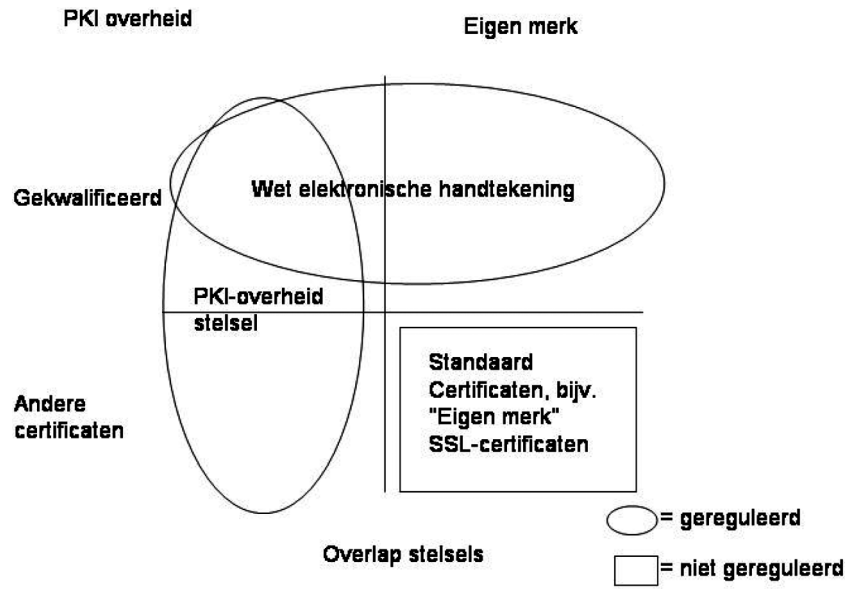
Onderzoek 1: Gereguleerde PKI-stelsels in Nederland

Vraagstelling en bevindingen

PKI is een techniek die wordt gebruikt om een betrouwbare elektronische infrastructuur te realiseren. Binnen Nederland zijn er twee stelsels voor PKI die gereguleerd zijn:

– het stelsel van gekwalificeerde certificaten waarmee rechtsgeldige elektronische handtekeningen kunnen worden gezet. Dit stelsel is ontstaan vanuit de intentie om elektronische handel te bevorderen en een digitale of elektronische handtekening te creëren waaraan dezelfde juridische waarde kan worden toegekend als aan de «klassieke» geschreven handtekening. Hiervoor werd in 1999 een richtlijn van kracht die in 2003 geïmplementeerd is in Nederland via de Wet op de elektronische handtekening.
– Daarnaast is het PKIoverheid stelsel door het ministerie van BZK ingericht voor de veilige elektronische communicatie van en met de overheid. Binnen dit stelsel worden ook andere certificaten gereguleerd, zoals bijvoorbeeld SSL-certificaten voor overheidsgebruik.

De overlap van de stelsels wordt in onderstaande figuur getoond.



Het doel van het door Logica uitgevoerde onderzoek is het verschaffen van inzicht in de risico's bij deze stelsels. Daarbij ging het uitdrukkelijk niet om het DigiNotar incident als zodanig maar om een analyse van de zwakheden in de stelsels, waarbij de inbraak bij DigiNotar de aanleiding was voor het onderzoek. Het onderzoek richt zich op de toekomst en geeft handvatten om, daar waar er een overheidsverantwoordelijkheid is, deze verantwoordelijkheid beter in te richten. Daardoor kan het Nederlandse certificatenstelsel betrouwbaarder en robuuster worden gemaakt. De lessen van het onderzoek zijn ook waardevol bij de herziening van de Europese Richtlijn Elektronische Handtekeningen (1999/93/EG).

De onderzoekers merken in hun rapport op dat van een bedrijf dat haar bestaansrecht ontleent aan het leveren van diensten op het gebied van

vertrouwensinfrastructuur mag worden verwacht dat informatiebeveiliging een topprioriteit krijgt. Het management van DigiNotar is hierin volgens de onderzoekers tekortgeschoten. Daarnaast zijn vereenvoudiging en verbeteringen in de certificatenstelsels mogelijk die de betrouwbaarheid en transparantie kunnen vergroten.

Belangrijkste conclusies en aanbevelingen:

Een van de belangrijke conclusies van het onderzoek is dat er geen sprake is van het falen van beide stelsels op één enkel aspect; de onderzoekers hebben geen zogenaamde «silver bullet» gevonden. Wel constateren zij dat er licht zit tussen het niveau van vertrouwen dat in deze tijd nodig is en verwacht mag worden van de stelsels en het feitelijk op dit moment gerealiseerde vertrouwen. Door de opkomst en het wereldwijde gebruik van internet is de dreiging van een digitale inbraak bij een certificatiedienstverlener de afgelopen jaren aanzienlijk toegenomen. De onderzochte stelsels zijn destijds consciëntieus opgezet, op een manier die paste bij toen bekende dreigingen en risico's. Om de betrouwbaarheid van de stelsels aan te passen aan de werkelijkheid van nu, zijn aanscherpingen en verbeteringen nodig en mogelijk op een vijftal onderdelen:

1. De *normenstelsels* kunnen concreter, explicieter en eenvoudiger, onder meer door de overlap tussen de stelsels aan te pakken. Ook moeten geconstateerde afwijkingen van de normen sneller worden opgevolgd door maatregelen.
2. Het *toezichtsarrangement* moet op een aantal fronten worden verbeterd. In de audits moet meer aandacht geschonken worden aan de IT-werkelijkheid (naast de aandacht voor managementsystemen). Een wettelijke meldplicht voor incidenten helpt de toezichthouder bij het uitoefenen van zijn taak omdat de impact van een incident sneller wordt onderkend en er vervolgens effectiever kan worden opgetreden. De samenwerking tussen auditor en toezichthouder dient te worden verbeterd. Daarnaast dient onafhankelijke en adequate signalering te worden georganiseerd. Dit kan worden bereikt door intensivering van de samenwerking tussen de OPTA, Logius en het Nationaal Cyber Security Centrum (NCSC).
3. *Risicobeheersing* binnen de stelsels moet verbeterd worden. Door aan de uitvoering en opvolging van risicoanalyses van certificatiedienstverleners een grotere rol toe te kennen, kan worden aangesloten bij de snel veranderende dreigingprofielen. Risicobeheersing over de stelsels heen kan voorkomen dat elk incident met maatschappelijke impact een crisis wordt.
4. Er is meer aandacht nodig voor de *transparantie en eenduidigheid* van de stelsels ten aanzien van de betrouwbaarheid van de geleverde certificatiediensten en het toezicht daarop.
5. Ten slotte moet blijvende aandacht zijn voor de ontwikkeling en instandhouding van een concurrerende (*grensoverschrijdende*) markt voor deze diensten.

Logica heeft ook alternatieven voor het gebruik van PKI-technologie onderzocht. De onderzoekers concluderen dat er internationaal vooral naar andere vormen van toepassing van deze techniek wordt gekeken maar dat voor PKI-technologie als zodanig voorlopig geen vervanging in zicht is.

Appreciatie van het onderzoek en te nemen maatregelen

Het Logica rapport geeft goede handvatten om tot een robuuster en voor de gebruiker meer betrouwbaar certificatiesysteem te komen. Voor zover dat noodzakelijk is, zal hiervoor tevens wet- en regelgeving worden

aangepast. Puntsgewijs volgen hieronder niet-limitatief de belangrijkste maatregelen die ik reeds heb genomen of nog zal nemen:

a. Ik onderschrijf de constatering dat de normenstelsels complex en deels overlappend zijn. Deze complexiteit kan wellicht worden verminderd door de overlap in beide stelsels ten aanzien van de gekwalificeerde handtekening los te laten. Ik zal onderzoeken in hoeverre het PKIoverheidsstelsel voor wat betreft gekwalificeerde handtekeningen losgelaten kan worden, zodat toezicht op deze PKI functionaliteit volledig binnen het wettelijk kader van de OPTA zal gaan plaatsvinden. Dit onderzoek zal nodig zijn om rekening te houden met de reeds in gebruik zijnde gekwalificeerde certificaten binnen het PKIoverheidstelsel en zal tevens moeten bezien welke termijnen voor een dergelijke overgang gehanteerd zouden kunnen worden.
b. Op korte termijn zal de minister van EL&I nagaan of het gehanteerde certificatieschema een volledige en correcte uitwerking vormt van de wettelijke eisen aan certificaten en certificatiedienstverleners.
c. Tevens zullen aanbevelingen van de onderzoekers waar dat passend is, worden ingebracht in de betreffende raadswerkgroep in Brussel die zich buigt over de herziening van de Richtlijn Elektronische Handtekeningen (1999/93/EG). Dit betreft onder meer de complexiteit van normen, risicobeheersing en het gebruik van audits. De richtlijn beperkt zich tot gekwalificeerde certificaten die voor elektronische handtekeningen worden gebracht. Het ontbreken van enige vorm van normering en toezicht op webservercertificaten zal eveneens bij de raadswerkgroep worden ingebracht.
d. De rollen van normbeheerders, auditors en toezichthouders en hun instrumenten zullen opnieuw en duidelijker gedefinieerd worden.
e. Bij audits moet duidelijk zijn welke norm is getoetst en wat het resultaat was van deze toetsing. Op deze wijze worden toezichthouders voorzien van de informatie die zij nodig hebben om hun taak goed uit te kunnen voeren. De huidige situatie, waarbij alleen afwijking van normen wordt gemeld, is niet langer voldoende. Daarnaast is tijdens controles meer aandacht nodig voor de IT-werkelijkheid bij certificatiedienstverleners. De management systems audit zal vergezeld moeten worden van elementen van een IT-audit.
f. De termijn, waarbinnen bij audits geconstateerde afwijkingen opgelost kunnen worden, wordt verkort. Normenstelsels zullen sneller dan voorheen aangepast moeten worden aan nieuwe risico's en dreigingen. Hiervoor is nauwere samenwerking tussen de beheerders van de normenkaders, auditors, toezichthouders en organisaties met een signalerende taak, zoals het NCSC, nodig.
g. De OPTA zal bedrijfsbezoeken bij certificatiedienstverleners afleggen en daarbij het systeem ter plaatse controleren. Ook voor het PKIoverheidstelstel zullen door de Policy Authority dergelijke bezoeken afgelegd gaan worden. Hiermee wordt tegelijkertijd invulling gegeven aan de aanbeveling van de onderzoekers en aan de wens van uw Kamer[1]. Een volledige overname van de audit-taak door de overheid achten wij niet noodzakelijk en ook niet wenselijk omdat dat de instandhouding en ontwikkeling bedreigt van de noodzakelijke en toch al schaarse expertise op dit terrein binnen het Nederlandse bedrijfsleven.
h. Het algemene stelsel van webcertificaten[2], die de echtheid van websites moeten garanderen, is niet gereguleerd[3]. Daardoor heeft de toezichthouder ook geen bevoegdheden ten aanzien van deze certificaten, die zowel binnen als buiten de overheid, veel worden gebruikt. Nederland zet zich er voor in dat er in de Richtlijn Elektronische Handtekeningen een wettelijke basis voor webcertificaten komt waardoor toezicht houden mogelijk wordt. Gelet op de grote vlucht

[1] Motie Elissen, Kamerstukken 2, 2011–2012, 26 643, nr 221
[2] Webcertificaten worden ook wel Secure Socket Layer (SSL) certificaten genoemd.
[3] Certificaten binnen het PKIoverheidsstelsel voor webertificaten zijn uiteraard wel gereguleerd, via het Programma van eisen PKIoverheid.

van het gebruik van webcertificaten wereldwijd en de grote rol van veelal Amerikaanse private browserleveranciers, heeft dit een sterke Europese en wereldwijde dimensie. Wij zullen de bevindingen van Nederland naar aanleiding van het DigiNotar incident zoveel mogelijk delen met andere landen en inbrengen in Europese en mondiale gremia die hierbij betrokken zijn.

i. Vooruitlopend op de resultaten van de onderzoeken heeft Logius, in de rol van de Policy Authority van PKIoverheid, naar aanleiding van het DigiNotar incident het Programma van Eisen aangescherpt. Zoals gemeld in mijn eerdere brief[1] betreft het vooral nader invullende eisen op het gebied van netwerkbeveiliging, computerbeveiliging en logging. Een eerste eis heeft betrekking op het voorkomen van ongeautoriseerde toegang tot PKI-overheid-diensten van certificatiedienstverleners. Certificatiedienstverleners moeten een fysieke en logische scheiding van omgevingen hebben en/of sterkere authenticatie per afzonderlijk PKI-proces gebruiken. Een tweede eis legt certificatiedienstverleners op om de afnemers van certificaten te wijzen op de maatregelen die afnemers zelf moeten nemen om de continuïteit van hun dienstverlening (op het gebied van het gebruik van certificaten) te waarborgen. Verdere eisen betreffen functiescheiding, een hoger niveau van beveiliging van webtoegang, automatische maandelijkse security scans, verplichte jaarlijkse penetratietesten, en uitgebreide logging en monitoring van de PKIoverheid omgeving.

Genoemde maatregelen zijn een eerste aanzet om het certificatenstelsel robuuster en betrouwbaarder te maken. Andere maatregelen, waarmee reeds een aanvang is gemaakt, zijn het intensiveren van de samenwerking tussen Logius en OPTA, het intensiveren van het rijkstoezicht op de certificatiedienstverleners, het inrichten van een proces voor het regelmatig actualiseren van het dreigingsbeeld en het aanhaken van het PKI-Overheidcalamiteitenplan op het crisismanagement op nationaal niveau. Tot slot zal ik onderzoeken of het gebruik van PKI-overheid voor overheidsorganisaties verplicht kan worden,

Daarnaast zal actief overleg gezocht worden met certificaatleveranciers binnen het PKIoverheidstelsel, om te onderzoeken hoe het betrouwbaar en ongestoord functioneren van deze markt vergroot kan worden. Met de afnemers van certificaten zal tevens een gesprek op gang worden gebracht. Daarbij zal direct geput kunnen worden uit de ervaringen met Diginotar en de uitkomsten van de assessments, die bij DigiD-afnemers worden uitgevoerd. In dit gesprek zullen ook mede-overheden worden betrokken.

Onderzoek 2: Het onderzoek van de Rijks Audit Dienst naar handelen van overheidspartijen

Vraagstelling
Door de Rijks Audit Dienst (RAD) is naar aanleiding van het DigiNotar-incident een onderzoek ingesteld met de volgende hoofdvraag:
Hebben de betrokken overheidspartijen in het stelsel van PKIoverheid (betreft zowel gekwalificeerde als niet-gekwalificeerde certificaten) gegeven de bestaande taken en verantwoordelijkheden van die partijen binnen genoemd stelsel, alert gereageerd inzake DigiNotar?

Belangrijkste conclusies

Door de RAD wordt geconstateerd dat er bij de rijksoverheid een trendbreuk is opgetreden. De wijze van denken over en omgaan met veiligheidsrisico's bij elektronisch verkeer is veranderd. De samenwerking

[1] Kamerstukken II, 2011–2012, 26 643, nr. 222.

van zowel private, publieke als internationale organisaties heeft een belangrijke impuls gekregen. Daarnaast wordt wel geconstateerd dat er voorafgaand aan de digitale inbraak bij Diginotar geen extra alertheid was. Er werd in hoge mate vertrouwd op de Audit-rapporten.
De RAD concludeert dat door de overheid snel en adequaat gehandeld is, waardoor verdere schade is voorkomen. De RAD constateert verder dat het DigiNotar incident wel gefungeerd heeft als een «uitstekende en levensechte oefening om partijen samen te brengen op het complexe gebied van de beveiliging van de digitale infrastructuur».

Verbeterpunten

Door de RAD wordt aangegeven dat, terwijl er een aantal zaken goed gingen tijdens de afhandeling van de crisis, er ook een aantal zaken zijn die voor verbetering vatbaar zijn. Pijnlijk duidelijk is geworden dat de continuïteit van de elektronische dienstverlening in het gedrang komt bij het ongeldig verklaren van certificaten. Het PKI-stelsel is zowel nationaal als mondiaal dermate belangrijk geworden, dat meer aandacht besteed zal moeten worden aan continuïteitsmaatregelen. Deze maatregelen, zoals het paraat hebben van een reservecertificaat van een andere leverancier, zijn de verantwoordelijkheid van de gebruiker. In de reeds uitgevoerde aanpassing van het nieuwe Programma van Eisen van PKIoverheid wordt hiervoor uitdrukkelijk aandacht gevraagd.

In algemene zin wordt de PKI problematiek nu in een breed kader besproken, wat moge blijken uit de al uitgevoerde verbeteringen in het Programma van Eisen van PKIoverheid en de in deze brief aangekondigde verdere acties.

De RAD concludeert dat over het algemeen sprake was van goede en tijdige communicatie naar burgers en instanties. Punt van aandacht bij een toekomstige crisis situatie is wel dat de overheid in haar communicatie duidelijker de precieze status aangeeft als nog geen volstrekte zekerheid is over de aard en impact van de calamiteit. Enerzijds bestaat de behoefte om zo snel mogelijk duidelijkheid te geven, anderzijds moeten de nodige voorbehouden worden gemaakt als nog sprake is van een lopend onderzoek. Dit punt wordt zeker meegenomen.

Onderzoek 3: veiligheid diensten in de Digitale Agenda.nl

Vraagstelling en bevindingen
In de Digitale Agenda.nl[1], die de Minster van Economische Zaken, Landbouw & Innovatie 17 mei 2011 aan uw Kamer zond, is een negental voorzieningen aangekondigd ten behoeve van de elektronische dienstverlening aan bedrijven. Om ondernemers hier zo veilig mogelijk gebruik van kunnen laten maken is door Collis/HEC onderzoek gedaan naar de veiligheid hiervan. Hierbij is zowel gekeken naar het ontwerp (inrichting, proces en beheer) als de feitelijke werking (voor zover reeds van toepassing).

Zoals reeds op basis van de tussenrapportage aan uw Kamer was gemeld in de Digitale Uitvoeringsagenda.nl[2], zijn bij de onderzochte diensten geen blokkerende tekortkomingen geconstateerd door Collis/HEC. De diensten kunnen daarmee als voldoende veilig worden beschouwd.
Wel werd aanbevolen om voor een aantal diensten de veiligheid op termijn beter te borgen, zowel qua governance als qua verdeling van verantwoordelijkheden. Een deel van deze aanbevelingen heeft te maken met het feit dat de diensten zich nog op het snijvlak van ontwikkeling en beheer bevinden.

[1] Kamerstukken II, 2010–2011, 29 515, nr. 331
[2] Kamerstukken II, 2011–2012, 26 643, nr. 217

Zo werd tijdens het onderzoek geconstateerd dat voor een dienst de benodigde veiligheidsmaatregelen zijn getroffen, maar dat hierop geen monitoring plaatsvond.

Aanbevelingen

In het algemeen doen de onderzoekers van Collis/HEC een vijftal aanbevelingen:

1. Zorg van een goede verdeling van verantwoordelijkheden tussen ministerie, ontwikkel- en beheersorganisaties en marktpartijen en maak deze afspraken transparant. Hierbij dient tevens (politieke) verantwoordelijkheid de Minister van Economische Zaken, Landbouw & Innovatie geëxpliciteerd te worden, zowel de ontwikkel- als de beheersfase. Detailafspraken over audits en penetratietesten dienen onderdeel van deze afspraken te zijn.
2. Zorg voor voldoende monitoring van de getroffen veiligheidsmaatregelen.
3. Maak duidelijk wat het restrisico is dat door belanghebbende als acceptabel wordt beschouwd.
4. Laat opdrachtgever van de diensten bepalen welke scope en diepte gewenst is bij uit te voeren audits ten behoeve van de veiligheid van de dienst.
5. Maak voor diensten die een hoog niveau van veiligheid vereisen niet alleen gebruik van audits en penetratietesten maar gebruik ook andere technische maatregelen om operationele risico's te verkleinen.

Deze aanbevelingen worden gedeeld en zullen verder worden uitgewerkt. Daarnaast is per dienst een aantal aanbevelingen gedaan. Deze zijn te vinden in bijgevoegde rapportage. De Minister van Economische Zaken, Landbouw & Innovatie heeft de implementatie hiervan reeds ter hand genomen.

Tenslotte

Dat uit de onderzoeken verbeterpunten naar voren komen staat buiten kijf. Deze punten heb ik aangegeven en ik heb u ook gemeld welke acties ondernomen zullen worden. Wij zullen uw Kamer tevens, nadat de twee onderzoeken van de Onderzoeksraad voor de veiligheid en de Inspectie Openbare Orde en Veiligheid beschikbaar komen, nader informeren over de daaruit voortkomende inzichten[1]. De resultaten van deze onderzoeken worden verwacht rond de zomer.

Rode draad bij de verbeterpunten is dat digitale veiligheid onze blijvende aandacht moet hebben. Ontwikkelingen in ICT gaan snel. Wat tien jaar geleden state of art was, is nu hopeloos verouderd; wat toen ondenkbaar was, wordt nu algemeen gebruikt. De technische vooruitgang en voortdurende verandering van ICT is zo vanzelfsprekend dat we niet altijd voldoende stil staan bij de veranderingen die dat vraagt van onze organisaties en processen. Het DigiNotar incident heeft duidelijk gemaakt dat veranderingen in de rol van de overheid, met name op het gebied van normering en toezicht noodzakelijk zijn. Onderzoek van Logica laat zien dat normen en toezicht permanent moeten worden bijgesteld. Kennis van dreigingen uit het verre verleden is ontoereikend voor beheersing van situaties en de risico's van nu. Logica geeft aan dat er achterstallig onderhoud verricht moet worden. Daarnaast blijft de menselijke factor een rol spelen bij beveiliging en is 100% zekerheid nooit te geven. Daarom moet ook worden geanticipeerd op situaties waar het toch mis dreigt te gaan. Met de aangekondigde verbeteracties levert het kabinet hieraan een bijdrage. Daarmee is reeds een begin gemaakt en gaan we verder aan de slag. Het is bemoedigend om te constateren dat voor een aantal belang-

[1] Deze onderzoeken gaan over de werking van de crisisinfrastructuur bij het DigiNotar incident (IOOV) en de vraag aan de OVV om onderzoek te doen naar DigiNotar en mogelijk andere incidenten, en in meer algemene zin het stelsel te beoordelen waarin betrokken partijen de digitale veiligheid waarborgen van (internet)communicatie tussen burgers en overheid Deze onderzoeken zijn mede genmeld in mijn brief onder nummer (Kamerstukken II, 2011–2012, 26 643), nr. 222

rijke elektronische diensten voor bedrijven de veiligheid momenteel voldoende is, hoewel ook daar voor de langere termijn nog een aantal aanbevelingen moet worden omgezet in daden.

Het Kabinet blijft werken aan het verbeteren van de veiligheid van haar elektronische voorzieningen. Digitale veiligheid verdient onze permanente aandacht, omdat het een wedloop zal blijven tussen kwaadwillenden en beveiligers.

De minister van Binnenlandse Zaken en Koninkrijksrelaties,
J. W. E. Spies