Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2011–2012

26 643 Informatie- en communicatietechnologie (ICT)

Nr. 214

BRIEF VAN DE MINISTER VAN BINNENLANDSE ZAKEN EN KONINKRIJKSRELATIES

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 9 november 2011

Begin september kreeg het Kabinet onmiskenbare signalen dat de uitgifte van PKI overheid certificaten van DigiNotar mogelijk gecompromitteerd was, als gevolg waarvan de overheid het vertrouwen in het bedrijf opzegde en direct noodmaatregelen heeft getroffen. Door de inbreuk werd het vertrouwen in de veilige communicatie aangetast, waardoor risico's ontstonden voor de bedrijfsvoering van de overheid en de maatschappij. Het Kabinet heeft daarop gereageerd door het incident op te schalen tot nationale crisis (Kamerstuk 26 643, nr. 188).
Uiteindelijk mag voorzichtig geconcludeerd worden dat de gevolgen van dit incident overzichtelijk zijn gebleven, mede dankzij intensieve, constructieve samenwerking met private partijen en het crisismanagement van de overheid. Wel onderstreept het kabinet het belang van blijvende alertheid op dergelijke incidenten, alsmede de reflectie op de afhankelijkheid van de overheid van dergelijke systemen.
Het kabinet maakt serieus werk van de vervolgacties die er toe moeten leiden dat incidenten als deze zoveel mogelijk voorkomen worden en die borgen dat overheden toegerust zijn om een adequaat beveiligingsniveau te bieden. In het kader daarvan is bij KPN/Getronics een onregelmatigheid geconstateerd. KPN/Getronics pakt dit incident voortvarend op en heeft maatregelen getroffen in afstemming met de departementen BZK en V&J. Het nader onderzoek is inmiddels bekend en heeft ertoe geleid dat er geen compromitering is vastgesteld van de PKI overheidscertificaten. Zoals aangegeven in mijn brief van 9 november heeft KPN de uitgifte van certificaten onder het PKI overheidsstelsel hervat.
Met deze brief informeer ik u, mede namens de Minister van Veiligheid en Justitie, over de uitvoering van de moties die 25 oktober 2011 zijn aangenomen, inzake DigiNotar en ICT-problemen bij de overheid. Daarnaast wordt ingegaan op een aantal acties die relatie hebben met de aangehouden moties. Dit sluit aan bij de brief van 16 oktober (Kamerstuk 26 643, nr. 189) waarmee het kabinet uw Kamer geïnformeerd heeft over de 3 sporen aanpak van de DigiNotar crisis.

kst-26643-214
ISSN 0921 - 7371
's-Gravenhage 2011

Aangenomen moties

Motie Hennis-Plasschaert c.s. (26 643, nr. 202) over een security breach

Verzoek aan de regering over te gaan tot een wettelijke meldplicht van een «security breach» die geldt voor organisaties die betrokken zijn bij voor de samenleving vitale informatiesystemen.
Op dit moment is geen sprake van een wettelijke verplichting tot het melden van een security breach. De in het regeerakkoord aangekondigde meldplicht biedt niet voldoende mogelijkheden voor het voorkomen of het beperken van schade bij incidenten zoals het DigiNotar incident. Bij een wettelijke meldplicht, de zogenaamde security breach notification, waarbij het melden van een security breach bij het Nationaal Cyber Security Centrum (NCSC) verplicht wordt gesteld voor organisaties betrokken bij voor de samenleving vitale informatiesystemen, is het van belang dat het juiste evenwicht wordt betracht waar het gaat om het vertrouwelijke karakter van de melding en de noodzakelijke waarborgen voor de commerciële belangen van de meldende partij. ICT-infrastructuur, -producten en -diensten worden voor het grootste deel geleverd door private sectoren. Wederzijds vertrouwen tussen publieke en private partijen is dan ook essentieel om samen te werken en informatie met elkaar te delen. Onverlet de meldplicht, is het dan ook van groot belang dat zo min mogelijk drempels voor effectieve samenwerking worden ingebouwd en de te bieden hulp voorop staat. De wijze waarop de meldplicht in het NCSC wordt ingericht, wordt meegenomen in de brief van de minister van V&J over inrichting van het NCSC aan uw Kamer voor het einde van dit jaar.

De motie Elissen c.s. (26 643, nr. 204) over gegevensbescherming burgers

Verzoek aan de regering om jaarlijks te onderzoeken, onder andere met behulp van penetratietesten, hoe goed verschillende overheidsonderdelen gegevens van burgers beveiligen en de resultaten van het onderzoek naar de Tweede Kamer te sturen, zodat deze een adequaat beeld van gegevensbescherming in Nederland krijgt.
Op verschillende wijzen wordt de beveiligingskwaliteit van informatiesystemen bij de rijksoverheid onderzocht. Ik wijs in dit verband op de keuze voor informatiebeveiliging als een van de twee de thema's voor het horizontaal bedrijfsvoeringsonderzoek in het Rijksjaarverslagen 2011. De Algemene Rekenkamer is reeds met dit onderzoek gestart. Ten aanzien van het specifieke punt van penetratietesten met betrekking tot het tegengaan van spionage heeft de minister van V&J reeds in de kabinetsreactie op de Kwetsbaarheidanalyse Spionage (KWAS) aangegeven dat binnen de overheid, onder verantwoordelijkheid van de hoogste managementraden en hun Beveiligingsambtenaren, security audits en systeempenetratietesten worden gehouden, waarin nadrukkelijk aandacht wordt besteed aan spionagerisico's (Kamerstuk 30 821, nr. 13). Met de uitkomsten van deze testen wordt vanzelfsprekend vertrouwelijk omgegaan.
Aan overheidorganisaties worden op het gebied van gegevensbescherming via regelgeving eisen gesteld aan gegevensbescherming. Artikel 13 van de Wet bescherming persoonsgegevens (Wbp) schrijft ook voor de overheid voor dat de verantwoordelijk passende technische en organisatorische maatregelen treft ter beveiliging van persoonsgegevens tegen verlies of vormen van onrechtmatige verwerking. Bij die maatregelen moet onder meer de stand van de technische ontwikkeling in acht worden genomen. De verantwoordelijke moet deze verplichting zelf nader invullen en daarbij rekening houden met veranderingen in de stand van de techniek. Toezicht daarop geschiedt door het College bescherming persoonsgegevens (Cbp).

Wat de informatiesystemen van de overheid betreft, geldt dat penetratietests een eigentijdse aanvulling zijn op de reeds genomen informatiebeveiligingsmaatregelen. Ik vertrouw erop dat de bestuurders en uitvoerders hun verantwoordelijkheid nemen, mede in het licht van de aangewakkerde maatschappelijke aandacht voor de informatiebeveiliging. Voorzover er geen regelgeving van toepassing is benut ik ook de mogelijkheden om vanuit een contractuele basis eisen te stellen aan beveiliging. Eerder heb ik uw Kamer geïnformeerd over het beleid dat gevoerd wordt rondom de veiligheid van systemen, die gebruik maken van DigiD (Kamerstuk 26 643, nr. 193). Alle DigiD-gebruikende organisaties dienen uiterlijk voor het einde van het eerste kwartaal van 2012 hun ICT-beveiliging getoetst te hebben op basis van een ICT-beveiligingsassessment. Ik zal uw Kamer daarover nader informeren. Aan de hand van de ervaringen zal ik bekijken of dit instrument kan worden ingezet bij andere centrale voorzieningen van de rijksoverheid.

Motie Hachchi en Elissen (26 643, nr. 207) over verbeteren ICT kennis

Verzoek aan de regering de ICT-kennis binnen de overheid te verbeteren zodat zij meer gelijkwaardige contractpartners zijn en de Kamer hierover voor de jaarrapportage van het Rijk te informeren.

Ik zal binnenkort uw Kamer informeren over de I-strategie van het Rijk. Onderdeel daarvan is het verder verbeteren van de kwaliteit van het ICT-personeel bij het Rijk. Als voorbeeld daarvan is de inrichting van I-Interim Rijk, een rijksbrede pool voor ICT-professionals die in oktober 2010 opgezet om voor het Rijk cruciale expertise op te bouwen en te behouden. Voor opdrachtgevers en het topmanagement wordt uitbreiding van het opleidingsportfolio voorzien. Voorts wordt een opleiding voorzien ten aanzien van (Europees) aanbesteden alsook het stimuleren van *digivaardigheid:* het besef bij medewerkers van het Rijk ten aanzien van beveiligingsissues.

In het kader van de Nationale Cyber Security Strategie zal op 1 januari 2012 het Nationaal Cyber Security Centrum van start gaan. Het Nationaal Cyber Security Centrum vervult een verbindende rol naar alle betrokken publieke en private partijen, wetenschap en kennisinstituten. Daarnaast zal het Nationaal Cyber Security Centrum expertise opbouwen op het gebied van cybersecurity en een adequate respons bij dreigingen en incidenten leveren. GOVCERT, het Cyber Security & Incident Response Team van de overheid, maakt daarvan een belangrijk onderdeel uit. Govcert bestaat uit experts op het gebied van ICT-beveiliging en maakt onderdeel uit van een groot internationaal netwerk van responseorganisaties. Tijdens een ICT-crisis zal het Centrum de nationale crisisstructuur ondersteunen en adviseren. Voor het einde van het jaar zal uw Kamer door de minister van V&J meer concreet over het takenpakket van het Centrum worden geïnformeerd.

Er wordt extra expertise ingezet bij de politie om het aantal zaken door het team high tech crime te laten stijgen tot 20 in 2014, de kinderporno te bestrijden en de regiokorpsen in staat te stellen cybercrime aan te pakken. Hierover is uw Kamer geïnformeerd (Kamerstuk 33 000 VI, nr. 2).

Voor de gemeenten geldt dat de VNG samen met het Kwaliteits instituut Nederlandse Gemeenten (KING) voor wat betreft de gemeentelijke informatievoorziening de gemeenten ondersteunt door:

- Het aanreiken van methoden voor verhogen van efficiency en kwaliteit;
- Standaardisatie van architectuur waaronder, processen, berichten, registraties en ketenuitwisseling (GEMMA);
- Ondersteuning bij gelijksoortige implementaties van (NUP)-bouwstenen;
- Bevorderen van ICT-samenwerking in ketens en tussen gemeenten in de vorm van shared service centra en het bevorderen van een gemeenschappelijke basisinformatievoorziening (de Basisgemeente);

– Bevorderen van het opdrachtgeverschap naar leveranciers.
KING heeft hiervoor experts op het gebied van e-dienstverlening en GEMMA in huis die de gemeente hierbij kunnen helpen. KING werkt daarbij nauw samen met Logius, Govcert, Ketenpartners en ministeries.

Motie Hachchi en El Fassed (26 643, nr. 208) over een certificaat systeem

Verzoek aan de regering om op internationaal niveau de urgentie van herziening van het certificaatsysteem aan te kaarten.
Het certificaatsysteem is op te delen in een aantal subcategorieën, zoals gekwalificeerde certificaten (waaronder elektronische handtekening, PKI-overheid certificaten) en niet gekwalificeerde certificaten (waaronder SSL certificaten). Voor de eerste categorie is Europese richtlijn elektronische handtekening van toepassing (1999/93/EC). Voor de tweede categorie geldt zelfregulering door de markt.
Het is vooralsnog niet aangetoond dat het certificaat systeem als geheel onvoldoende betrouwbaar is ondanks het feit dat DigiNotar is gekraakt. Daarnaast is het de vraag of op korte termijn alternatieven beschikbaar zijn. Deze vraag wordt meegenomen in een lopende evaluatie, waarover ik later in de brief nader informeer. Overigens heeft EU Commissaris Kroes naar aanleiding van vragen van het Europees Parlement geantwoord dat er geen overeenstemming bestaat over beschikbare technologieën die een vergelijkbaar betrouwbaarheidsniveau bieden, maar daarmee wil ik niet vooruitlopen op de uitkomsten van het eigen onderzoek. Om meer zicht te krijgen op alternatieven voor het SSL-stelsel is in het kader van ICA (International Council of ICT in Administrations) op initiatief van Nederland een werkgroep opgericht.
Commissaris Kroes heeft tevens aangegeven de richtlijn op de elektronische handtekening in 2012 te herzien. Ze heeft aangekondigd hierbij mee te nemen hoe het toezicht op de Certification Service Providers kan worden vergroot.[1] Mede op basis van de uitkomsten van de bovengenoemde evaluatie zal de noodzaak van een herziening op het gebied van toezicht van de richtlijn elektronische handtekeningen (1993/93/EG) specifieker bij de Europese Commissie worden aangekaart. Voor deze herziening is het ministerie van EL&I samen met het ministerie van V&J verantwoordelijk. Vanuit de verantwoordelijkheid voor PKI overheid zijn in samenspraak met het ministerie van EL&I zijn de eerste contacten gelegd met de verantwoordelijken bij de Europese Commissie voor de herziening van de richtlijn elektronische handtekeningen. Daarbij is aangeboden om Nederlandse ervaringen in het kader van DigiNotar te delen.

De motie van Elissen (26 643, nr. 209) over privacy en safety by design

Verzoek aan de regering om bij de ontwikkeling van alle nieuw te starten ICT-projecten privacy by design en safety by design toe te passen, zodat nieuwe ICT-systemen veiliger zijn en beter berekend op misbruik en slechts privacygevoelige gegevens bevatten als dat strikt noodzakelijk is.
Voor safety by design zijn de beveiligingskaders van het Rijk een verplicht uitgangspunt voor ieder informatiesysteem. Daartoe behoort reeds het Voorschrift Informatiebeveiliging Rijksdienst 2007 (VIR2007), het Voorschrift Informatiebeveiliging Rijksdienst – Bijzondere Informatie (VIR-BI) en departementale basisbeveiligingsafspraken (baselines). Begin volgend jaar zal een rijksbrede baseline van kracht worden (BIR). De BIR, evenals de meeste departementale baselines, is gebaseerd op de Code voor Informatiebeveiliging. Dat is een internationale standaard die ook in de markt veelal de basis vormt voor de eigen informatiebeveiliging van de organisatie. Voor de safety zal via het instrument van DigiD gebruik worden gemaakt van jaarlijkse beveiligingsassessments.
In de brief van de Staatssecretaris van V&J en ondergetekende van 29 april 2011 en de daarbij behorende Notitie privacybeleid (Kamerstuk

[1] http://www.europarl.europa.eu/sides/getAllAnswers.do?reference=E-2011–008086&language=EN; http://www.europarl.europa.eu/sides/getAllAnswers.do?reference=E-2011–007985&language=EN

32 761, nr. 1) is uiteengezet dat privacy by design in Nederland in meer algemene zin nog niet zoveel wordt toegepast, maar dat die ontwikkeling wel moet worden gestimuleerd. Om meer inzicht te krijgen in de meest effectieve methode voor deze stimulering, zal TNO de Minister van EL&I rapporteren over onderzoek naar de drijvende en remmende krachten die van invloed zijn op de beslissing van bedrijven om privacy by design toe te passen. In het debat naar aanleiding van deze brief in de Eerste Kamer is reeds toegezegd dat het onderzoeksrapport aan beide Kamers wordt toegezonden.

Motie Elissen c.s. (26 643, nr. 210) over een notitie integrale privacybescherming

Verzoek aan de regering om een beleid te ontwikkelen dat toeziet op de integrale bescherming van privacy, te beginnen met een notitie integrale privacybescherming waarin, analoog aan hoe dat binnen de crisisbescherming gebruikelijk is, gebruikgemaakt wordt van een keten van proactie, preventie, preparatie, repressie en nazorg, zodat gegevens van Nederlanders nu en in de toekomst beter beschermd blijven.
Deze motie is ondersteuning van beleid. Wat in deze motie wordt gevraagd betreft een versterking van de gegevensbescherming van de burger, vooral door meer dan tot dusverre het geval is geweest het niveau van informatiebeveiliging in beleid, wetgeving en uitvoering beter te verankeren. Privacybeleid omvat immers veel meer dan louter het beveiligen van gegevens. Bij eerder genoemde brief van 29 april 2011 hebben de Staatssecretaris van V&J en ondergetekende een Notitie privacybeleid aan beide Kamers gezonden. Die notitie is onderwerp geweest van een beleidsdebat in de Eerste Kamer op 17 mei 2011 en van een algemeen overleg in de Tweede Kamer op 15 september 2011.
In de notitie zijn tal van maatregelen in het vooruitzicht gesteld. Deze maatregelen zijn vooral gericht op de wetgeving. In de notitie werd een brede meldplicht voor datalekken – gericht op de bescherming van persoonsgegevens – in het vooruitzicht gesteld. In het algemeen overleg is aangekondigd dat dit onderwerp met voorrang in een wetsvoorstel wordt opgenomen. De verwachting is dat dit wetsvoorstel eind november 2011 ter consultatie aan adviesorganen en belanghebbenden kan worden aangeboden.
Tot slot verwijs ik in dit verband ook naar de recent aangenomen motie Gesthuizen-Verhoeven (24 095, nr. 294) over een visie op de bescherming van privacy op het internet. De Minister van EL&I zal u hier, in samenspraak met de Staatssecretaris van V&J en ondergetekende, per brief over informeren.

Aangehouden moties

Naast de aangenomen moties wordt in deze brief stil gestaan bij een aantal acties die het kabinet heeft genomen in relatie met de DigiNotar affaire en die antwoord kunnen geven op vragen die in uw Kamer leven, mede gelet op de strekking van een aantal aangehouden moties.

Motie Gesthuizen en El Fassed (26 643, nr. 194) over een parlementair onderzoek

Het kabinet heeft het initiatief genomen om middels interne en externe onderzoeken de DigiNotar crisis van meerdere kanten te belichten om daaruit lessen te trekken.
Zoals in het kamerdebat van 13 oktober 2011 is aangegeven, is de Onderzoeksraad voor Veiligheid gevraagd een onderzoek uit te voeren naar de beveiliging van de bestaande informatie- en ICT-systemen in zijn algemeenheid. De minister van VenJ en ondergetekende zullen de Onderzoeksraad voor Veiligheid verzoeken het Diginotar incident en andere incidenten te onderzoeken, en in meer algemene zin het stelsel te

beoordelen waarin betrokken partijen de digitale veiligheid waarborgen van (internet)communicatie tussen burgers en de overheid.
De ministeries van EL&I en BZK hebben gezamenlijk opdracht gegeven voor een evaluatie van het stelsel van PKI overheid en het stelsel van gekwalificeerde certificaten. Mochten de resultaten van het onderzoek hiertoe aanleiding geven dan zal ik met de minister van EL&I in overleg treden over de wijze waarop het systeem van toezicht aangepast dient te worden en in hoeverre hierbij onderscheid moet zijn tussen PKI-Overheid certificaten en de overige gekwalificeerde certificaten. Hierover wordt uw Kamer in het voorjaar van 2012 nader geïnformeerd.
Verder is een audit gestart met de vraag of de organisaties in het PKI stelsel alert hebben gereageerd, zowel in de fase voor als de fase na het bekend worden inbreuk op DigiNotar. De lessen hieruit zullen worden meegenomen in de reactie op de evaluatie van het PKI stelsel.
Het ministerie van EL&I onderzoekt de veiligheid van de voorzieningen in het kader van de Digitale Agenda, en bericht hierover separaat aan uw Kamer.
Op verzoek van de Cyber security raad heeft op 14 en 28 oktober 2011 een tweetal brainstormsessies plaatsgevonden. Het centrale thema was verbetering van beveiligde digitale gegevensuitwisseling. Een brede groep deelnemers uit bedrijfsleven, wetenschap en overheid heeft daaraan actief deelgenomen. De verslaglegging is rond 7 november beschikbaar en zal worden gebruikt bij het verder aanscherpen van de Nationale Onderzoeksagenda Digitale Veiligheid.
Tot slot zal de Inspectie voor de Openbare Orde en Veiligheid een onderzoek verrichten naar de crisisbeheersingaspecten rond het DigiNotar incident.

Motie Gesthuizen (26 643, nr. 195) over een «crashteam»
Govcert, het Cyber Security & Incident Response Team van de overheid, maakt per 1 januari 2012 deel uit van het Nationaal Cyber Security Centrum (NCSC). Govcert bestaat uit experts op het gebied van ICT-beveiliging en maakt onderdeel uit van een groot internationaal netwerk van response-organisaties. Zoals aangekondigd in de Nationale Cyber Security Strategie zal Govcert worden versterkt. Een kernactiviteit van het NCSC is het verzorgen van een snelle en adequate response bij incidenten. Voorop staat echter dat de eigenaren van de informatiesystemen zelf eindverantwoordelijk zijn voor de veiligheid van hun eigen systemen en websites. Organisaties moeten dan ook zelf ingrijpen als er sprake is van een veiligheidsprobleem of een lek. Uiteindelijk is het de eigen verantwoordelijkheid van organisaties om adviezen ter harte te nemen. Iedereen dient te investeren in kennis en kunde. Wanneer er een incident plaatsvindt wordt er gehandeld volgens het nationaal handboek crisisbesluitvorming. Specifiek voor ICT-crises bestaat de de ICT-Response Board, die per 1 januari onderdeel zal zijn van het Nationaal Cyber Security Centrum. Daarnaast kan er bij kleinere crises ondersteuning worden geboden bij sectorspecifieke Computer Emergency Response Teams, zoals bijvoorbeeld Surfnet voor de academische sector. Hiermee is feitelijk invulling gegeven aan de functie die wordt voorgesteld in de motie zoals ook effectief is gebleken tijdens de Diginotar casus. Op basis van de evaluatie na incidenten zal de werkwijze voortdurend worden aangepast/verbeterd (zie ook reactie op motie 194).

Motie El Fassed (26 643, nr. 200) over een speciaal gezant
Er is gevraagd aan de regering op korte termijn een speciaal gezant te benoemen, bijvoorbeeld uit de financiële sector, om de overheid door te lichten op basis van de vraag in hoeverre een cultuuromslag nodig is op het gebied van ICT, veiligheid en privacy en aanbevelingen te doen.
«Het besef een iOverheid te zijn, is geen rustig bezit, maar een permanente opgave», aldus de Wetenschappelijke Raad voor het Regerings-

beleid (WRR). De rijksoverheid dient zich daar in ieder geval als eerste van bewust te zijn en ernaar te handelen. In de kabinetsreactie op het rapport iOverheid van de WRR wordt dit onderschreven. Op alle niveaus in de besluitvorming worden nu al beleidsdoelen meegewogen met privacy- en informatiebeleidsbeginselen. Het maken van dit soort van afwegingen is voor de betreffende verantwoordelijke bestuurder of uitvoerder als zodanig niet nieuw. Het kabinet vindt dat er een cultuuromslag nodig is. De afweging tussen die beginselen zal bewuster, meer geëxpliciteerd en transparanter moeten plaatsvinden. Bovendien moeten bepaalde soorten van informatieverwerking meer aandacht krijgen, omdat ze in het riskant zijn voor de kwaliteit en betrouwbaarheid van gegevens; namelijk als er sprake is van het «vernetwerken», het verrijken of het voeren van proactief beleid op basis van informatie. Die soorten verwerking moeten een «waarschuwingsvlag» krijgen in de bestaande toetsingskaders. In de kabinetsreactie zijn al concrete maatregelen voorgesteld op het institutionele en operationele vlak om deze cultuuromslag te bewerelligen. Deze cultuuromslag vergt internalisatie van de bovengenoemde afweging bij de betrokken bestuurders en uitvoerders. Het kabinet heeft geen vertrouwen in een speciaal gezant als instrument hiervoor, en meent dat deze mogelijkerwijs zelfs contraproductief kan zijn.

Motie El Fassed en Hachchi (26 643, nr. 201) over transacties of mutaties via DigiD

Er zijn vragen gesteld over de mogelijkheid te onderzoeken of het mogelijk is het beveiligingsniveau van transacties of mutaties via DigiD te verhogen naar eenzelfde niveau als banken hanteren bij internetbankieren, bijvoorbeeld door het gebruik van een e-identifier. Er wordt op dit moment gewerkt aan de besluitvorming over de wenselijkheid en de haalbaarheid van de invoering van een geheel nieuw (hoger) zekerheidsniveau binnen DigiD, waarbij nadrukkelijk ook het kostenaspect zal worden betrokken. Het betreft hier de ontwikkeling van een elektronische Identiteit (eID), die geplaatst kan worden op meerdere wettelijke identiteitskaarten, zoals de Nederlandse Identiteitskaart (NIK) genoemd, de zogenaamde elektronische Nederlandse Identiteitskaart (eNIK). De Tweede Kamer zal hierover binnenkort geïnformeerd worden.

Motie Elissen (26 643, nr. 205) over eerstelijnstoezicht

Tevens heeft uw Kamer vragen gesteld over het eerstelijnstoezicht voor kritische ICT systemen. De rol en het belang van ICT voor de bedrijfsvoering en continuïteit komt tot uiting in het beleid voor bescherming van vitale infrastructuur. Elke vier jaar wordt een integrale analyse uitgevoerd naar de weerbaarheid en bescherming van de vitale infrastructuur, laatstelijk in 2010. Binnen infrastructuren als energie, telecom, water en financiën zijn de ICT-systemen ondersteunend aan het kunnen (blijven) leveren van vitale producten, diensten en processen. Belangrijk uitgangspunt bij het waarborgen van de continuïteit van die vitale producten, diensten en processen is het streven naar redundantie en het hebben van terugval opties en noodvoorzieningen in geval van bedreiging van deze vitale producten, diensten en processen. Sinds eind 2009 loopt een traject dat specifiek inzet op het vergroten van de weerbaarheid van vitale infrastructuur tegen aantasting of uitval van ICT. In dit traject wordt nauw samengewerkt door overheid, vitale sectoren en leveranciers van ICT en telecomdiensten.

Concluderend, we staan aan het begin van een onontkoombare ontwikkeling van verdergaande digitalisering. Een ontwikkeling die grote kansen biedt, maar die daarnaast ook nieuwe risico's met zich mee brengt. Het kabinet kan niet garanderen dat in de toekomst geen nieuwe incidenten voorkomen. Iedereen dient zijn eigen verantwoordelijkheid te nemen. Wel kan het kabinet maatregelen nemen om de risico's te managen en lessen

te trekken uit de incidenten. De in deze en eerdere brieven aangekondigde acties geven hieraan invulling. Tot slot, het is waardevol dat uw Kamer goed tegenspel biedt, opdat we gezamenlijk optimaal voor deze reis geëquipeerd zijn.

De minister van Binnenlandse Zaken en Koninkrijksrelaties,
J. P. H. Donner