Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2011–2012

26 643 Informatie- en communicatietechnologie (ICT)

Nr. 246

BRIEF VAN DE MINISTER VAN VEILIGHEID EN JUSTITIE

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 6 juli 2012

Mede namens de minister van Binnenlandse Zaken en Koninkrijksrelaties, de minister van Defensie, de minister van Buitenlandse Zaken en de minister van Economische Zaken, Landbouw en Innovatie (EL&I) bied ik uw Kamer hierbij de voortgangsbrief betreffende de implementatie van de Nationale Cyber Security Strategie (NCSS) aan. Voorts ontvangt uw Kamer vóór het zomerreces een separate brief over de invulling van de motie Hennis-Plasschaert[1] en de interventiemogelijkheden voor het Rijk bij crisis (Kamerstuk 26 643, nr. 247). De nu voorliggende voortgangsbrief heeft tot doel uw Kamer te informeren over de voortgang van de NCSS sinds haar lancering in 2011 en volgt hierbij de actielijnen zoals deze in de strategie zijn uitgezet. De implementatie van de NCSS ligt op koers. Sinds de lancering van de NCSS zijn grote stappen gezet in het weerbaarder maken van overheid, maatschappij en bedrijfsleven tegen cyberdreigingen. Daarbij is ook de interdepartementale, civiel-militaire, publiek-private en internationale samenwerking op het gebied van cybersecurity versterkt.

Inrichting Cyber Security Raad en Nationaal Cyber Security Centrum

In het kader van de NCSS is op 30 juni 2011 de Cyber Security Raad ingesteld. Deze Raad, onder voorzitterschap van Eelco Blok (CEO KPN) en Erik Akerboom (Nationaal Coördinator Terrorismebestrijding en Veiligheid), met in totaal veertien leden uit wetenschap, bedrijfsleven en overheid, adviseert de regering op het terrein van digitale veiligheid. Naast haar reguliere vergaderingen in 2011 en 2012 is de Raad enkele malen bijeengeweest naar aanleiding van specifieke digitale incidenten in 2011 en 2012. Leden van de Raad hebben vanuit hun afzonderlijke expertise ervaringen gedeeld in diverse (inter)nationale fora en informatie gedeeld met relevante partijen, waaronder het bedrijfsleven, wetenschap en maatschappij. Bij het Cyber Security Beeld Nederland 2011 en rondom de in de Tweede Kamer voorgestelde meldplicht, de *security breach notification* (motie Hennis-Plasschaert) heeft de Raad advies uitgebracht

[1] Kamerstuk 26 643, nr. 202.

kst-26643-246
ISSN 0921 - 7371
's-Gravenhage 2012

aan de minister van Veiligheid en Justitie. De Raad heeft voor de korte termijn vijf prioriteiten vastgesteld, waar zij samen met de spelers in het veld aandacht aan besteedt: (1) bewustwording van het brede veld van digitale veiligheid, (2) een beter besef van de digitale dreigingen en kwetsbaarheden, (3) meer capaciteit voor respons na digitale incidenten, (4) een houding die van preventie verschuift naar proactie en (5) het gezamenlijk werken aan een nationale onderzoeksagenda digitale veiligheid die haar beslag heeft gekregen in de Nationale Cyber Security Reasearch Agenda (NCSRA). De Cyber Security Raad wordt in haar werkzaamheden ondersteund vanuit de directie Cyber Security van de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) en door de Afstemmingsgroep Cyber Security, waarin een brede vertegenwoordiging van overheid, bedrijfsleven en wetenschap zitting heeft.

In januari 2012 is het Nationaal Cyber Security Centrum (NCSC) van start gegaan als incident-respons organisatie en als platform voor samenwerking tussen publieke en private partijen op het gebied van cyber security. In het NCSC wordt kennis en expertise samengebracht van private partijen en overheidsorganisaties. Het NCSC werkt samen met de aangesloten partners aan de versterking van de digitale weerbaarheid van Nederland. Daarbij heeft iedere partij zijn eigen verantwoordelijkheid. Het NCSC heeft hierin, naast uiteraard de inbreng van eigen expertise, een ondersteunende rol. Het NCSC werkt momenteel aan de verdere uitbreiding van de eigen personele capaciteit.

Partijen delen, op basis van hun eigen taken en binnen wettelijke mogelijkheden, relevante informatie in het NCSC, zodat inzicht kan worden verkregen in ontwikkelingen, dreigingen en trends. Ook zijn er vanuit publieke en private organisaties liaisons geplaatst in het NCSC om de samenwerking en kennisdeling optimaal te faciliteren. Dit zorgt voor een unieke kennispositie, die benut kan worden bij (dreiging van) een grootschalig cyberincident.
De AIVD, het OM, de OPTA, Defensie, het KLPD en het NFI hebben een liaison in het NCSC geplaatst. Tevens wordt de participatie van de vitale sectoren opgebouwd, zoals de recente detachering vanuit de private sector in het kader van de versterking van de publiek-private samenwerking.

Naast zijn kennisfunctie treedt het NCSC ook zelf op of biedt ondersteuning bij crises of incidenten die kunnen leiden tot maatschappelijke ontwrichting. Om een goed besluit te kunnen nemen over de responsactiviteiten in tijden van een ICT-crisis, is een goed begrip van de situatie onontbeerlijk. Hierin mag kennis vanuit de private sector niet ontbreken. Daarom is afgelopen periode gewerkt aan de inrichting van de ICT Response Board (IRB). De IRB is een samenwerkingsverband van private en publieke partijen, dat tijdens een grootschalige ICT-crisis of dreiging waarbij de nationale veiligheid in het geding is, een analyse maakt van de crisis, op basis van effectieve informatie-uitwisseling. Indien nodig brengt de IRB een advies uit over te nemen maatregelen aan beslissers binnen de Nationale Crisisstructuur en aan de vitale sectoren. Het project is in februari van dit jaar met een trainingsdag afgerond en de IRB is als functie ondergebracht bij het NCSC. De IRB is tevens ingebed in het Nationaal Crisisplan ICT van de Rijksoverheid, dat in de loop van 2012 wordt geactualiseerd.

Opstellen van dreigings- en risicoanalyses

Vanuit het NCSC wordt actief bijgedragen aan de bewustwording van publiek, overheid en het bedrijfsleven via publicaties, de website en het delen van concrete expertise met belanghebbende partijen. Het NCSC

publiceert kennisdocumenten die informatie en inzicht bieden over cyber aanval-technieken, preventie, kwetsbaarheden en dreigingen en daarnaast ook specifieke tools voor het bieden van concrete handelingsperspectieven. Zo zijn de afgelopen periode de «ICT-beveiligingsrichtlijnen voor webapplicaties» en factsheets rond de beveiliging van SCADA-systemen uitgebracht. Daarnaast wordt de website van het NCSC dagelijks aangevuld met technische beveiligingsadviezen voor ICT professionals. Tevens wordt jaarlijks het Cyber Security Beeld Nederland uitgebracht, een geïntegreerde dreigingsanalyse met inbreng van overheidspartijen, wetenschap en bedrijfsleven. Het Cyber Security Beeld Nederland beoogt een geïntegreerd en objectief beeld van dreigingstypen en impactfactoren te schetsen, dat als basis kan dienen voor beleids- en besluitvorming binnen de Rijksoverheid en binnen de private sectoren. Het volgende Cyber Security Beeld Nederland wordt voor de zomer aan uw Kamer toegezonden.

Vergroten weerbaarheid tegen ICT verstoringen en cyberaanvallen

Het goed functioneren van vitale sectoren is van essentieel belang voor onze samenleving. Met het Informatieknooppunt Cybercrime (IKC)[1] is afgelopen jaren veel ervaring opgedaan met informatie-uitwisseling over cybercrime en cyber security tussen overheidspartijen enerzijds en organisaties uit vitale sectoren anderzijds. Met de komst van het NCSC en in lijn met de NCSS zet de overheid in op centrale coördinatie via één loket ten aanzien van de uitwisseling van cyber security informatie. Hiertoe is een traject gestart waarbij uiterlijk eind 2012 het IKC (en zijn Information Sharing Analyses Centers (ISAC's)) functioneel onderdeel worden van het NCSC. Daarbij is in het bijzonder aandacht voor de eigen identiteit en werkwijze van het IKC en de vertrouwelijke omgang met informatie.

Eind 2011 is het Nationaal Crisisplan ICT opgeleverd dat in de loop van 2012 wordt geactualiseerd. Het crisisplan beoogt steun te bieden aan de crisisbeleidsadviseurs in de voorbereiding op en tijdens de situatie waarbij een maatschappelijke ontwrichting dreigt of plaatsvindt als gevolg van een ICT-verstoring of -uitval. Het crisisplan draagt bij aan een verkorting van de reactietijd van de nationale crisisorganisatie en aan een effectieve crisisbestrijding. Om bij de overheid de weerbaarheid tegen uitval van elektriciteit en ICT te versterken hebben alle ministeries in 2011 onder andere het continuïteitsmanagement verbeterd na een herijking van de kritieke processen. In 2011 is tevens ingezet op het vergroten van de weerbaarheid tegen grootschalige uitval van elektriciteit en ICT bij vitale maatschappelijke functies van de medeoverheden. Om gemeenten, provincies, veiligheidsregio's, politieregio's en waterschappen te ondersteunen bij het ontwikkelen van continuïteitsplannen is voor elke doelgroep een modelplan ontwikkeld. De ondersteuning bij het opstellen van continuïteitsplannen wordt voortgezet. Ook is cyberspionage als scenario voor het dreigingstype digitale veiligheid, toegevoegd aan de Nationale Risicobeoordeling, waarover in de voortgangsbrief Nationale Veiligheid van 5 juni 2012 is gerapporteerd aan uw Kamer.

Ten aanzien van de beveiligingsnormen voor de Rijksdienst geldt dat er een set rijksbrede beveiligingsnormen is opgesteld die in de plaats zal treden van bestaande interdepartementale normenkaders en een groot aantal bestaande normenkaders bij ministeries en uitvoeringsorganisaties. Deze set normen wordt de Baseline Informatiebeveiliging Rijksdienst genoemd (BIR). De invoering van de BIR bij de ministeries wordt afgesloten met een audit. Voorts wordt in de loop van dit jaar het geactualiseerde Voorschrift Informatiebeveiliging Rijksdienst – Bijzondere

[1] Het Informatieknooppunt Cybercrime biedt een platform waar vitale sectoren en overheidspartijen in een vertrouwde omgeving informatie uitwisselen over incidenten, dreigingen, kwetsbaarheden en good practices op het gebied van cybercrime en cyber security. Doel is de weerbaarheid van deze partijen tegen verstoringen te verhogen.

Informatie (VIR-BI) van kracht. Dit voorschrift is in lijn gebracht met het Voorschrift Informatiebeveiliging Rijksdienst 2007 (VIR2007). Zoals eerder aan de Tweede Kamer gemeld, worden diverse onderzoeken afgerond naar het toevoegen van elektronische functionaliteiten aan de bestaande Nederlandse Identiteitskaart; toevoeging van een eID (elektronische Identiteit) betekent dat het betrouwbaarheids- en veiligheidsniveau van authenticatie voor burgers wordt verhoogd en voldoet aan het hoogste niveau dat de Europese Unie hanteert.

Over de veiligheid van hard- en software zijn gesprekken gevoerd met ICT-office, Netelcom en het CIO-Platform. Doel van de gesprekken is het opstellen van een agenda gericht op bewustwording, op veilig gebruik en veilige implementatie van hardware en software alsook op de verbetering van de intrinsieke veiligheid ervan. Deze agenda wordt nu uitgewerkt met publieke en private partijen in het dit jaar gestarte programma Digiveilig (ECP-EPN). Onderdeel hiervan is ondermeer de wachtwoorden-campagne die dit jaar van start gaat. Verder is op de Safer Internet Day op 7 februari de website Meldknop.nl gelanceerd. Op deze website, gericht op jongeren, kunnen meldingen gedaan worden van bijvoorbeeld hacking of schendingen van privacy. De website www.mijndigitalewereld.nl biedt tips en feiten omtrent het veilig gebruik van internet en mobiele toepassingen.

Het Alerteringssysteem Terrorismebestrijding (ATb) informeert de vitale sectoren over dreigingen die de continuïteit in gevaar kunnen brengen. Met de inbedding van cyber security in het Alerteringssysteem Terrorismebestrijding (ATb) wordt cyber security-gerelateerde informatie ook in het informatieproces van het ATb meegenomen. Tevens worden cyber security-gerelateerde maatregelen opgenomen in het systeem en worden er relevante basisafspraken met de betreffende sectoren gemaakt. Ten behoeve van de inbedding van cyber security in het ATb is een *pilot* van start gegaan voor de ATb-sector Financieel. De uitkomsten van deze pilot zullen dienen als input voor de aansluiting van de overige ATb-sectoren. De planning is om eind 2013 gereed te zijn met het aansluiten van cyber security in alle ATb-sectoren.

Wijziging Telecomwet

Op 8 mei jl. heeft de Eerste Kamer ingestemd met de nieuwe Telecomwet. Deze is op 5 juni van kracht geworden. In deze gewijzigde wet is ondermeer geregeld dat aanbieders van open elektronische communicatienetwerken en diensten storingen en datalekken moeten melden. Voorts zijn bepalingen opgenomen die de aanbieders verplichten om passende technische en organisatorische maatregelen te treffen ter borging van de continuïteit.

Versterken van internationale samenwerking

Nederland blijft ook in internationaal verband streven naar goede samenwerking ter bevordering van de digitale veiligheid. Allereerst door het versterken van bilaterale samenwerking met onder meer de VS, het VK, Zweden, Australië en de Benelux-landen. Het kabinet verwelkomt het voorstel van de Europese Commissie om het Europese Cyber Crime Centre in Den Haag te vestigen bij Europol. Dit Centrum zal in 2013 zijn beslag krijgen en zich richten op de ondersteuning van lidstaten in de strijd tegen cybercrime. De EU zal naar verwachting nog dit jaar een integrale EU-cyberstrategie presenteren, die de interne en externe aspecten van digitale veiligheid in samenhang zal bezien.
Tijdens de NAVO-Top in Chicago onderstreepten de regeringsleiders het belang van het verder versterken van *cyber defense* capaciteiten van het bondgenootschap. Dit is opgenomen in de *Deterrence and Defence*

Posture Review, die een evaluatie bevat van de benodigde mix van militaire capaciteiten van het Bondgenootschap in de komende jaren. De NAVO zal hiertoe onder meer samenwerking zoeken met partnerlanden en internationale organisaties zoals de VN en EU. Dit wordt door Nederland sterk ondersteund. In OVSE-verband draagt Nederland bij aan het ontwikkelen van zgn. *confidence building measures* op het gebied van cyber security. Deze maatregelen moeten de transparantie over het cyberbeleid van landen vergroten en de escalatie van conflicten als gevolg van cyberincidenten voorkomen.
Om goed voorbereid te zijn op crises zijn oefeningen van belang. Cyber security is niet louter een nationale aangelegenheid en (mogelijke) crises kennen vaak een internationaal karakter. Daarom is in 2011 de stap gezet om ook in internationaal verband de samenwerking te versterken op het terrein van oefeningen en crisismanagement. Enkele voorbeelden: zo worden in Beneluxverband good practices uitgewisseld en is in EU-VS verband een cyber security werkgroep gestart die onder andere ziet op responsmogelijkheden. Eind 2011 heeft Nederland deelgenomen aan de oefening Cyberatlantic. Onder de vlag van Critical Information Infrastructure Protection (CIIP) van de Europese Commissie wordt gewerkt aan een 2^{e} pan-Europese oefening onder de naam Cyber Europe 2012. Er wordt gewerkt aan de opzet voor een oefenbeleid voor de komende jaren en Nederland neemt deel aan het opstellen van een European Cyber Crisis Coordination Framework (EC3F). Daarnaast neemt Nederland deel aan de NAVO-oefening Cyber Coalition 2012, die dit jaar (deels) wordt geïntegreerd met de politiek-strategische crisis management oefening van de NAVO (CMX 2012).

Intensivering digitale weerbaarheid krijgmacht en cyber operations

In 2012 is Defensie gestart met de in de NCSS aangekondigde intensivering op het terrein van digitale weerbaarheid en *cyber operations*. Er is een programmamanager Cyber aangetreden en de Taskforce Cyber is opgericht. Op 27 juni heeft de minister van Defensie de Defensie Cyber Strategie voor het opereren in het digitale domein gepresenteerd en aan de Tweede Kamer aangeboden. De programmamanager is verantwoordelijk voor de coördinatie van alle cybergerelateerde activiteiten binnen Defensie. Op grond van de Defensie Cyber Strategie wordt een Defensie cyber doctrine opgesteld. De oprichting van een Defensie Cyber Commando (DCC) is voorzien voor eind 2014. Het DCC wordt verantwoordelijk voor de coördinatie van alle cyber gerelateerde activiteiten binnen Defensie. Op dit niveau vindt ook de verbinding tussen de verschillende cybervermogens en de betrokken defensieonderdelen plaats. Het DCC draagt zo bij aan de betrouwbaarheid en beschikbaarheid van defensienetwerken en -systemen, uitvoering van militaire (cyber)operaties en het verzekeren van de vrijheid van handelen in cyberspace voor Nederland en zijn bondgenoten.
Eind 2013 wordt een Defensie Cyber Expertise Centrum (DCEC) opgericht dat binnen Defensie de kennisontwikkeling en -borging vorm zal gegeven. Het DCEC is een *shared service center* dat het strategische, operationele en tactische kennis- en vaardighedenpeil van Defensie voor militaire *cyber operations* op het gewenste niveau moet brengen. Dit gebeurt enerzijds door het ontwikkelen en samenbrengen van kennis en anderzijds door opleiding, training en oefening.

Het Defensie *Computer Emergency Response Team* (DefCERT) is mede verantwoordelijk voor de beveiliging van defensienetwerken en -systemen en zal medio 2013 volledig operationeel zijn om 24 uur per dag, zeven dagen per week de meest kritieke defensienetwerken te beschermen. Daarnaast werkt DefCERT nauw samen met het NCSC in het versterken van de weerbaarheid tegen cyberdreigingen. De MIVD versterkt in de

periode 2012–2015 de *cyber* inlichtingencapaciteit. Verder intensiveren de MIVD en de AIVD de samenwerking op het gebied van *cyber* en *signals intelligence* (SIGINT) wat moet leiden tot een gezamenlijke eenheid voor de verwerving van SIGINT en cyberinlichtingen. Deze intensivering zorgt voor een versterking van zowel civiele als militaire capaciteiten

Intensivering opsporing en vervolging van cybercrime

Voor de versterking van de opsporing en vervolging van cybercrime is een aantal concrete zaken gerealiseerd die in lijn liggen met de gestelde doelstellingen. Het Team High Tech Crime (THTC) van het KLPD wordt verdubbeld door dertig nieuwe digitaal rechercheurs aan te trekken. Het THTC heeft in 2011 acht grote onderzoeken gedraaid waarmee zij op koers liggen om de afgesproken twintig zaken per jaar in 2015 te halen. Binnen het Nationaal Cyber Security Centrum deelt het KLPD kennis en expertise met andere diensten en partijen. Waar het gaat om toezicht en monitoring geldt dat cybercrime een vast onderdeel geworden van de Integrale Veiligheidsmonitor en er komt binnenkort een onderzoek uit naar het slachtofferschap van cybercrime. De Inspectie Veiligheid en Justitie heeft in haar onderzoek naar de intake bij de politie cybercrime als onderdeel meegenomen. Dit onderzoek zal naar verwachting binnenkort gereed zijn.

Stimuleren onderzoek en onderwijs

Tijdens haar eerste vergadering heeft de Cyber Security Raad de Nationale Cyber Security Research Agenda (NCSRA) vastgesteld. Voor de eerste tender, die in 2012 in het kader van de NCSRA wordt gepubliceerd, is € 6.3 miljoen gereserveerd. Deze onderzoeksagenda sluit aan op de NCSS door invulling te geven aan actielijn 6 van de strategie, het stimuleren van onderzoek en onderwijs en prioriteit 5 van de CSR. De onderzoeksagenda stelt vijf hoofddoelen centraal:

1. Verbeteren van veiligheid van en vertrouwen in ICT-infrastructuur en diensten
2. Nederland voorbereiden op veiligheidsuitdagingen in de komende 6 tot 12 jaar
3. Stimuleren van de Nederlandse cyber security economie
4. Versterken en verbreden van kennis en innovatie tav cyber security
5. Onderzoekprogramma's cyber security bij de overheid verbinden

Momenteel wordt, onder regie van het ministerie van EL&I, met publieke en private partijen gewerkt aan de implementatie van deze agenda. In de tweede helft van 2012 zal een eerste, interdepartementaal gefinancierde, onderzoekstender voor cyber security worden uitgeschreven. Deze tender sluit tevens aan bij het topsectorenbeleid. Deze onderzoeken dragen niet alleen bij aan de opbouw van kennis en kunde op het gebied van cyber security maar leveren ook concrete tools op en meer Nederlandse experts op het gebied van cyber security. Inhoudelijk draagt het onderzoek dat hieruit voortkomt tevens bij aan de realisatie van alle andere actielijnen met kennis, kunde en concrete producten. Naast het stimuleren van onderzoek wordt momenteel ook verkend hoe het aandeel van ICT-veiligheid in de daarvoor geschikte opleidingen kan worden uitgebreid. Hoogwaardig opgeleid personeel op het gebied van cyber security is een schaars goed. Via overheidsinterne opleidingstrajecten, zoals binnen het NCSC reeds wordt toegepast (samenwerking TNO en HEC) wordt getracht cyber specialisten te trainen en te werven. Daarnaast kunnen samenwerkingsverbanden met private partijen worden opgezet om cyber specialisten uit te wisselen.

Naar aanleiding van vragen van leden van uw Kamer in het Algemeen Overleg van 11 april 2012, heb ik aangegeven initiatieven van de

beroepsgroep om te komen tot een eenduidig kader voor certificering en kwalificatie van informatiebeveiligingsprofessionals toe te juichen. Inmiddels heeft overleg plaatsgevonden met vertegenwoordigers van deze beroepsgroep. In de werkgroep European Competence Framework binnen het programma Digivaardig en Digiveilig (ECP-EPN) wordt nu gewerkt aan de eerste Nederlandse versie van het Europese e-Competence Framework. Dit raamwerk, dat in samenwerking met NEN en de beroepsgroep informatiebeveiligers wordt opgesteld, kan als basis dienen voor een uniform kwalificatie- en certificatiestelsel binnen de beroepsgroep informatiebeveiligers.

Tot slot

Het Kabinet constateert dat de urgentie van de uitdagingen waar wij ons in het kader van cyber security voor gesteld zien, door alle betrokken partijen gedeeld wordt. De actielijnen uit de strategie worden voortvarend aangepakt. In de afgelopen periode is hiermee het fundament gelegd voor een integrale Nederlandse cyber security aanpak. Nu is het zaak voort te bouwen op dit fundament, om in publiek-private, civiel-militaire en (inter)nationale samenwerking te komen tot integraal cyber security management, waarin verantwoordelijkheden helder zijn benoemd en intensievere samenwerking leidt tot synergie. Een belangrijke stap hiertoe is de intensivering van mogelijkheden om digitale aanvallen te detecteren die gericht zijn op de Rijksoverheid en vitale infrastructuren. Ook het vergroten van de weerbaarheid en het versterken van het herstelvermogen zal hier onderdeel uit van moeten maken. Het Kabinet zal zich blijven inspannen voor de implementatie van de Nationale Cyber Security Strategie en het versterken van de publiek-private en internationale samenwerking voor een veilige en vitale digitale samenleving.

De minister van Veiligheid en Justitie,
I. W. Opstelten