Eerste Kamer der Staten-Generaal

1

Vergaderjaar 2012–2013

33 602 EU-voorstel: Netwerk- en informatiebeveiliging in de Unie COM(2013)48[1]

A

VERSLAG VAN EEN SCHRIFTELIJK OVERLEG

Vastgesteld 5 juli 2013

De vaste commissie voor Immigratie & Asiel / JBZ-raad[2] heeft onlangs twee EU-dossiers in behandeling genomen die betrekking hebben op het onderwerp cyberbeveiliging. Het betreft een gezamenlijke mededeling van de Europese Commissie en de Hoge Vertegenwoordiger met de Strategie inzake cyberbeveiliging van de Europese Unie en een voorstel voor een richtlijn houdende maatregelen om een hoog gemeenschappelijk niveau van netwerk- en informatiebeveiliging in de Unie te waarborgen.[3]
Naar aanleiding hiervan heeft zij de minister van Veiligheid en Justitie op 5 juni 2013 een brief gestuurd.

De minister heeft op 4 juli 2013 gereageerd.

De commissie brengt bijgaand verslag uit van het gevoerde schriftelijk overleg.

De griffier van de vaste commissie voor Immigratie en Asiel / JBZ-Raad,
K. van Dooren

[1] Zie E130011.op www.europapoort.nl

[2] Samenstelling: Holdijk (SGP), Broekers-Knol (VVD), Slagter-Roukema (SP), Franken (CDA), Nagel (50PLUS), Ruers (SP), Van Bijsterveld (CDA), Duthler (VVD), Koffeman (PvdD), Kuiper (CU), Strik (GL), De Vries (PvdA), Lokin-Sassen (CDA), Scholten (D66), Th. de Graaf (D66), De Boer (GL), De Lange (OSF), Ter Horst (PvdA) *(voorzitter),* Beuving (PvdA), Schrijver (PvdA), M. de Graaff (PVV) *(vicevoorzitter),* Reynaers (PVV), Popken (PVV), Huijbregt-Schiedon (VVD), Schouwenaar (VVD), Swagerman (VVD), Gerkens (SP)

[3] JOIN(2013)1 en COM(2013)48. Zie ook de dossiers **E130010** en **E130011** op www.europapoort.nl; het JOIN-document en het COM-document zijn als bijlagen bij dit verslag opgenomen.

kst-33602-A
ISSN 0921 - 7371
's-Gravenhage 2013

BRIEF AAN DE MINISTER VAN VEILIGHEID EN JUSTITIE

Den Haag, 5 juni 2013

Onlangs heeft de commissie voor Immigratie & Asiel / JBZ-raad twee EU-dossiers in behandeling genomen die betrekking hebben op het onderwerp cyberbeveiliging. Het betreft een gezamenlijke mededeling van de Europese Commissie en de Hoge Vertegenwoordiger met de Strategie inzake cyberbeveiliging van de Europese Unie en een voorstel voor een richtlijn houdende maatregelen om een hoog gemeenschappelijk niveau van netwerk- en informatiebeveiliging in de Unie te waarborgen.[4] De mededeling en het richtlijnvoorstel geven de leden van de diverse fracties aanleiding tot het stellen van vragen en het maken van opmerkingen over beide dossiers.

Algemeen

De leden van de **VVD**-fractie en de leden van de **CDA**-fractie hebben met belangstelling kennisgenomen van het voorstel voor een richtlijn inzake netwerk- en informatiebeveiliging en van de gezamenlijke mededeling inzake de strategie van cyberbeveiliging van de Europese Unie. Zij achten de ambitie van een hoog niveau van beveiliging van netwerken en informatiesystemen in de EU van belang voor een sterke interne markt. Zij hebben nog een paar vragen over het gewenste niveau van beveiliging, de in te stellen beveiligingsautoriteit, de samenhang met de voorgestelde Europese privacyverordening met betrekking tot de voorgestelde meldingsplicht en de visie op de realisatie van de uitgangspunten zoals die in genoemde mededeling staan verwoord.

De leden van de **PvdA**-fractie hebben met belangstelling kennisgenomen van het voorstel voor een richtlijn. Zij hebben wel enige vragen over de prioriteiten en het tempo van de aanpak van cyberbeveiliging.

De leden van de **SP**-fractie hebben kennisgenomen van de mededeling en het richtlijnvoorstel. Zij hebben nog een paar vragen. Overigens zijn zij tevreden met de inzet om de cybersecurity te verstevigen. Het uitbreiden van de meldplicht voor incidenten en de plicht voor bedrijven om zich beter te beveiligen kan op de instemming van deze leden rekenen.

De leden van de fractie van **D66** hebben met belangstelling kennisgenomen van de strategie van de Europese Commissie inzake de cyberbeveiliging van de Europese Unie. De huidige digitale tijd vraagt om passende maatregelen en beleid om burgers een veilig en open internet te kunnen bieden. Cybercrime vraagt daarom om een Europese strategie. De leden van de D66-fractie onderstrepen het belang van een Europese strategie voor cyberbeveiliging en zij zijn positief op zowel subsidiariteit als proportionaliteit. Deze strategie schetst een visie van de Europese Commissie om de digitale omgeving in de Europese Unie de veiligste te maken. De leden van de D66-fractie zijn enthousiast over de ambitieuze inzet van de Europese Commissie, maar plaatsen hun vraagtekens bij de omvang en veelvoud van aandachtsgebieden. De digitale wereld beslaat uiteraard alle beleidsterreinen die ook in de fysieke wereld bestaan. De leden zijn wel bedachtzaam over de breedte van onderwerpen die deze strategie beslaat, omdat het aantal onderwerpen veelomvattend is. Zij hebben enkele vragen aan de regering over de positie die Nederland zal innemen tijdens besprekingen in de Raad.

---

[4] JOIN(2013)1 en COM(2013)48. Zie ook de dossiers **E130010** en **E130011** op www.europa-poort.nl

Vragen over de mededeling Strategie inzake cyberbeveiliging JOIN(2013)1

Coherente strategie

De Nederlandse regering onderstreept in het BNC-fiche het belang dat verschillende onderdelen binnen de Europese Commissie die zich met cyberbeveiliging en cyberspace bezig houden in samenhang optrekken. Echter, deze strategie haakt aan op tal van beleidsterreinen zoals seksuele uitbuiting van kinderen, cybercriminaliteit die is gericht op economisch gebied, belastingfraude en botnets. Tegelijkertijd streeft de strategie naar een waarborging van de grondrechten van de EU-burgers in de digitale wereld. Wat is de samenhang van deze aanpak, zo vragen de leden van de fractie van **D66** de regering. En hoe beoordeelt de regering de uitvoerbaarheid van deze veelvoud van beleidsterreinen onder één strategie?

Gegevensuitwisseling

Het dagelijks beheer van het internet ligt bij vele commerciële en non-gouvernementele partijen. De private sector dient volgens de strategie een vooraanstaande rol te blijven spelen bij de constructie en beheer van het internet. Zo wil de Europese Commissie dat de betrokkenheid van de private sector wordt bevorderd, omdat het overgrote deel van de netwerk- en informatiesystemen eigendom is van de private sector en door deze sector geëxploiteerd wordt. Tegelijkertijd roept de strategie op tot meer samenwerking van de verschillende bevoegde instanties voor de opsporing van cybercrime. Data- en gegevensuitwisseling is hierbij onvermijdelijk. Waarborging van de privacy is van groot belang om ook misbruik van gegevens tegen te kunnen gaan. De leden van de fractie van **D66** achten het van belang dat de Europese voorstellen bescherming persoonsgegevens (die in behandeling zijn) erbij betrokken worden. Kan de regering dat standpunt onderschrijven? En hoe beoordeelt de regering de wijze waarop in deze strategie de privacy is gewaarborgd?

Bij ernstige cyberaanvallen of incidenten dienen Europol/EC3 tenminste te worden ingelicht. Wanneer bij een incident persoonsgegevens in gevaar zijn gebracht, dient de nationale gegevensbeschermingsautoriteit of de nationale toezichthoudende instantie ingelicht te worden. De regering zet in het BNC-fiche in op het afzwakken van deze meldplicht. De leden van de fractie van D66 zijn van mening dat deze meldplicht noodzakelijk is om bescherming van gegevens te kunnen borgen. Deelt de regering die opvatting en hoe verhoudt zich die opvatting dan tot afzwakking van de meldplicht?

Het EC3 is onlangs opgericht (sinds 1 januari) en dient als spil voor de bestrijding van cybercriminaliteit. In dit voorstel vraagt de Europese Commissie het EC3 onder meer analyses en inlichtingen te verstrekken, onderzoek te verrichten, kanalen te scheppen voor informatiedeling tussen autoriteiten, de private sector en andere belanghebbende partijen. Graag vernemen deze leden wat de tot nu toe de ervaring is met de werkzaamheden en resultaten van het EC3.

Positie CEO's en raden van bestuur

In de gezamenlijke mededeling cyberbeveiligingsstrategie verzoekt de Europese Commissie de private sector te overwegen op welke manier CEO's en raden van bestuur meer verantwoording kunnen afleggen voor het waarborgen van cyberbeveiliging. Is de regering het met de leden van de **VVD**-fractie en de leden van de **CDA**-fractie eens dat een dergelijke afweging niet ook gemaakt zou moeten worden voor CEO's en raden van

bestuur van publieke en semi-publieke organisaties? Graag ontvangen deze leden een nadere toelichting.

Infrastructuur

Nederland stelt in het BNC-fiche geen nieuwe structuren te ontwikkelen die bestaande structuren binnen lidstaten vervangen of dupliceren. De leden van de **D66**-fractie sluiten zich aan bij deze opmerking, maar willen de regering erop wijzen dat de kwantiteit en kwaliteit van de infrastructuur niet in alle EU-lidstaten van gelijkwaardige aard is en optimaal functioneert. De regering bevestigt ook dat met name op het gebied van nationale capaciteit voor cyberbeveiliging en bij de coördinatie van grensoverschrijdende incidenten en binnen de EU nog steeds lacunes zijn. Is de regering het met deze leden eens dat voor een coherente Europese beveiligingsstrategie vervanging van structuren derhalve soms noodzakelijk kan zijn?

Effectiviteit van de strategie

In het algemeen zet deze strategie in op het drastisch terugdringen van cybercriminaliteit en de verhoging van cyberbeveiliging. De leden van de fractie van **D66** menen dat preventie aan de voorkant minstens zo effectief is als, zo niet effectiever is dan *damage control* achteraf. Deelt de regering deze visie? In dat geval vernemen deze leden graag haar inzet op dit punt.

Over 12 maanden wordt er beoordeeld of er vooruitgang is geboekt. Welke indicatoren wil de regering meten om te kunnen oordelen over het al dan niet slagen van beleid? Tot slot, kan de regering een indicatie geven van het tijdpad en de planning naar een wetgevingsvoorstel (anders dan het reeds gepubliceerde richtlijnvoorstel) toe?

Vragen over de richtlijn netwerk- en informatiebeveiliging COM(2013)48

Uitwerking kader richtlijn naar een hoog beveiligingsniveau

De leden van de **VVD**-fractie en de leden van de **CDA**-fractie vragen zich af hoe het doel van de richtlijn, namelijk om een «hoog gemeenschappelijk niveau van netwerk- en informatiebeveiliging in de Unie te waarborgen» zich verhoudt met artikel 14 van de voorgestelde richtlijn. In dat laatste artikel worden lidstaten verplicht er voor te zorgen dat overheden en marktdeelnemers passende technische en organisatorische maatregelen treffen ter beheersing van de risico's voor de beveiliging van netwerken en informatiesystemen. Ook artikel 13 van de Wet bescherming persoonsgegevens (Wbp) kent de verplichting tot het treffen van passende technische en organisatorische maatregelen. Nu wordt met de betreffende bepaling uit de Wbp geen hoog niveau van beveiliging beoogd, maar een passend beveiligingsniveau. Hoe moet het doel van een hoog beveiligingsniveau van de richtlijn uitgelegd worden tegen deze achtergrond? Is het doel van deze richtlijn inderdaad ambitieuzer dan die van de huidige Wet bescherming persoonsgegevens en de nog geldende Europese privacyrichtlijn?

De leden van de **PvdA**-fractie kunnen zich vinden in de gekozen aanpak, maar constateren dat het kader vooralsnog onuitgewerkt is omdat eigenlijk alles van belang wordt overgelaten aan de lidstaten. Daarbij missen zij in hoofdstuk II van het richtlijnvoorstel dat de strategie en het samenwerkingsplan een indicatie betreffen van de termijn waarop deze plannen tot stand moeten komen en de prioriteiten die hierbij moeten

worden gesteld. Hoofdstuk III over de samenwerking tussen bevoegde autoriteiten geeft evenmin aan hoe de Europese Commissie de snelheid van deze zeer wenselijke samenwerking meent te kunnen en te mogen bevorderen. Het belangrijke hoofdstuk IV over de beveiliging van netwerken, overheden en marktdeelnemers laat in het midden aan wat voor Europese randvoorwaarden de door de lidstaten te ontwikkelen passende technische en organisatorische maatregelen (artikel 14, eerste lid) dienen te voldoen. De leden van de PvdA-fractie willen weten of de indruk klopt dat het hele proces van cyberbeveiliging slechts zeer traag op gang komt.

Beveiligingsautoriteit

Elke lidstaat is volgens artikel 6 van de voorgestelde richtlijn verplicht een nationale autoriteit aan te wijzen voor de beveiliging van netwerk- en informatiesystemen. De leden van de **VVD**-fractie en de leden van de **CDA**-fractie vragen zich af of het nodig is om een aparte nieuwe autoriteit aan te wijzen. Deze autoriteit wordt (vanzelfsprekend) verplicht samen te werken met het College bescherming persoonsgegevens (CBP). Zou deze richtlijn voor de regering geen aanleiding kunnen vormen om een informatieautoriteit, zoals voorgesteld in het rapport van de WRR *iOverheid* uit 2011 in het leven te roepen, waarvan dan zo'n beveiligingsautoriteit als voorgesteld in deze richtlijn deel uit kan maken, alsook mogelijk het reeds bestaande CBP? Het bevordert de transparantie richting burgers en bedrijven en voorkomt dat burgers en bedrijven met verschillende toezichthouders te maken krijgen. Hoe denkt de regering hierover?

Meldplicht incidenten

Hoe verhoudt zich de meldplicht van de voorgestelde Europese privacyverordening met de meldplicht van incidenten met een aanzienlijke impact op de beveiliging aan de bevoegde autoriteiten? De Europese Commissie is straks krachtens de richtlijn bevoegd gedelegeerde handelingen vast te stellen met betrekking tot de omschrijving van de omstandigheden waarin overheden en marktdeelnemers incidenten moeten melden. De omstandigheden waaronder verantwoordelijken verplicht zijn incidenten die verband houden met persoonsgegevens te melden zijn in de Europese privacyverordening zelf omschreven. De leden van de **VVD**-fractie en de leden van de **CDA**-fractie zouden het een goede zaak vinden als dergelijke omstandigheden ook in de richtlijn zelf worden opgenomen. Is de regering bereid zich hiervoor sterk te maken? Wat is verder de status van richtsnoeren zoals die in artikel 14 lid 6 staan genoemd en die de bevoegde autoriteiten kunnen vaststellen met betrekking tot de omstandigheden waarin overheden en marktdeelnemers incidenten moeten melden?

De meldplicht voor incidenten richt zich op alle bedrijven waarvan de disruptie van belang kan zijn voor de samenleving. Onduidelijk voor de leden van de **SP**-fractie is wat precies nu een beveiligingsincident is. Welk standpunt neemt de Nederlandse regering hier in?

De omschrijving van het incident roept meer vragen op. De huidige omschrijving zou mislukte aanvallen buiten beschouwing laten, terwijl deze wel degelijk van belang kunnen zijn bij de bestrijding van cybercrime. Is de regering het met de leden van de SP-fractie eens dat de omschrijving te breed is geformuleerd en daardoor mogelijk haar doel voorbij schiet?

De meldplicht wordt niet Europees geregeld. De lidstaten zijn vrij dit te regelen. Onduidelijk is daardoor waar en bij wie gemeld dient te worden. Hierdoor kunnen grensoverschrijdende bedrijven als Google, Facebook e.d. onder verschillende meldplichten vallen. Wat is het standpunt van de Nederlandse regering hierin?

Het kleinbedrijf is uitgesloten van de meldplicht. Toch kan ook zeker het kleinbedrijf gevoelige informatie hebben, denk bijvoorbeeld aan kleine hosters of dataverrijkingsbedrijven. Hoe denkt de regering hier over?

Uitvoering richtlijn

Ook de uitvoering van de richtlijn roept bij de leden van de **SP**-fractie vragen op. Welke informatie moet gedeeld worden? Op welke wijze wordt de privacy van burgers gewaarborgd? Wordt er niet om onnodige informatie gevraagd?

De autoriteiten mogen voor de toetsing van cyberveiligheid informatie opvragen bij marktpartijen. De richtlijn geeft hier geen beperking aan. Dat betekent dat alle informatie nu opgevraagd kan worden. Op welke wijze gaat Nederland hier vorm aan geven?

Verantwoordelijkheid producenten

Als laatste missen de leden van de **SP**-fractie de verantwoordelijkheid van software- en hardwareproducenten, maar ook hosters kunnen meer doen. Zo worden er nog steeds modems afgegeven met een standaardtoegangscode, en kunnen hosters hun klanten beter informeren over nut en noodzaak van een up to date CMS. Op welke wijze gaat Nederland zich inzetten om dit te bewerkstelligen?

Tot slot

Graag ontvangen de leden van de **D66**-fractie een periodieke update over de ontwikkelingen van deze dossiers.

De commissie voor Immigratie & Asiel / JBZ-raad ziet met belangstelling uit naar uw reactie en ontvangt deze graag binnen **vier weken** na dagtekening van deze brief.

Voorzitter van de commissie voor Immigratie & Asiel / JBZ-raad,
G. ter Horst

BRIEF VAN DE MINISTER VAN ECONOMISCHE ZAKEN

Aan de Voorzitter van de Eerste Kamer der Staten-Generaal

Den Haag, 4 juli 2013

Hierbij bied ik u de antwoorden aan op de vragen die zijn gesteld en opmerkingen die zijn gemaakt door de leden van de commissie voor Immigratie & Asiel / JBZ-raad, d.d. 5 juni 2013, met kenmerk 153016u, inzake de gezamenlijke mededeling van de Europese Commissie en de Hoge Vertegenwoordiger met de Strategie inzake cyberbeveiliging van de Europese Unie en het voorstel voor een richtlijn houdende maatregelen om een hoog gemeenschappelijk niveau van netwerk- en informatiebeveiliging in de Unie te waarborgen.

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

Vragen over de mededeling Strategie inzake cyberbeveiliging JOIN(2013)1

Coherente strategie

De leden van de fractie van D66 zijn benieuwd naar de samenhang van de verschillende beleidsterreinen die de EU cyber security strategie aanhaalt en de uitvoerbaarheid van deze strategie.

Het terrein van cyber security heeft de laatste jaren een grote ontwikkeling doorgemaakt. Van een onderwerp over (de techniek van) informatiebeveiliging naar een breed beleidsterrein dat onder andere cyber crime, cyber spionage en cyber defence omvat en belangrijke politieke thema's raakt als privacy en een open en vrij internet.

Daarbij is het internet inmiddels verweven en onlosmakelijk verbonden met alle aspecten van de samenleving en is cyber security een terrein dat zowel overheid, bedrijfsleven als burgers raakt. De noodzaak om cyber security integraal op te pakken wordt daarmee steeds groter.

Een instrument om deze integraliteit vorm te geven is een cyber security strategie. Dit is ook de reden dat in Nederland in 2011 een nationale cyber security strategie is ontwikkeld. Een strategie als een paraplu die de verschillende deelgebieden op het terrein van cyber security omvat.

De EU cyber security strategie sluit dan ook aan bij de ontwikkeling van de diverse nationale cyber security strategieën van afgelopen jaren en is daarmee (inhoudelijk) in lijn. De bestaande verantwoordelijkheden op de deelterreinen van de EU cyber security strategie, zoals op cybercrime of cyber defence, blijven onveranderd. Doel van de EU cyber security strategie is om de samenwerking en afstemming tussen deze deelgebieden te verbeteren. Dit is belangrijk, omdat door verschillende partijen vaak gebruik wordt gemaakt van dezelfde capaciteiten en technieken.

De verantwoordelijkheid van de uitvoering van de verschillende maatregelen die in de EU cyber security strategie zijn opgenomen ligt bij verschillende partijen. Het is van belang dat deze maatregelen worden omgezet in een concreet actieplan waarbij duidelijk is wie voor welk resultaat verantwoordelijk is. Daarnaast is transparantie ten aanzien van de voortgang op de uitvoering van de maatregelen van belang.

Gegevensuitwisseling

De leden van de D66 fractie benoemen het belang van de waarborging van privacy om misbruik van gegevens tegen te kunnen gaan en achten het van belang dat de Europese voorstellen bescherming persoonsgegevens erbij betrokken worden. De leden vragen de regering om het standpunt in deze en vragen naar een beoordeling van de wijze waarop in de EU cyber security strategie de privacy is gewaarborgd. Deze vragen zijn meegenomen in het antwoord op de vragen van de leden van de SP-fractie die verderop in deze brief onder het kopje «Uitvoering strategie» worden beantwoord.

Vervolgens wijzen de leden van de D66-fractie op het belang van de meldplicht indien bij een incident persoonsgegevens in gevaar zijn gebracht. Zij vragen de regering naar haar opvatting en hoe zich dit verhoudt tot het afzwakken van de meldplicht. Deze vragen worden verder toegelicht onder het kopje «Meldplicht incidenten».

De leden van de fractie van de D66 wijzen op de centrale rol van het European Cybercrime Centre (EC3) bij Europol. Zij merken op dat het voorstel voor de netwerk- en informatiebeveiliging richtlijn (NIB-richtlijn) verschillende taken voor dit centrum aanwijst. In dit verband vragen zij naar ervaringen tot nu toe met het centrum.

Versterking van een Europees gezamenlijk antwoord op, de lidstaten individueel overstijgende, bedreigingen van de cybersecurity en toenemende cybercriminaliteit is een onderdeel van de acties op middellange termijn waartoe de EU ministers van Justitie en Binnenlandse Zaken in de raadsconclusies van 7 en 8 juni 2012 hebben besloten.

In een relatief kort tijdsbestek is door Europol vorm gegeven aan het EC3, dat op 11 januari 2013 van start is gegaan. In eerste instantie heeft Europol in het EC3 de al daarvoor binnen Europol bestaande units voor de aanpak van seksueel misbruik van kinderen, fraude via internet en cybercrime bij elkaar gebracht onder één paraplu. Aan dit verband is ook extra analyse en beleid ontwikkelende capaciteit toegevoegd. In de eerste helft van dit jaar is EC3 vooral doende met het bepalen van een eigen plaats en aanpak. Concrete ervaringen bestaan dan ook vooral uit de informatie-uitwisseling op het gebied van kinderporno en van cybercrime. Dit heeft verschillende keren tot een succesvolle aanpak tussen verschillende landen waaronder Nederland geleid.

Positie CEO's en raden van bestuur

De leden van de VVD-fractie en de leden van de CDA-fractie benoemen het belang van het afleggen van verantwoording door CEO's en raden van bestuur van publieke en semi-publieke organisaties. Hierbij kan worden aangegeven dat de lessen die getrokken kunnen worden uit incidenten uit het verleden, zoals DigiNotar, laten zien dat het beveiligen van informatie en de beschikbaarheid van de digitale dienstverlening urgent en blijvend op de agenda moeten staan.

Ook bestuurders en topmanagers in het openbaar bestuur moeten zich hiervan bewust zijn. Om dit bewustzijn en de kennis over informatieveiligheid bij deze groep te verbeteren en te borgen, is door de minister van Binnenlandse Zaken de taskforce Bestuur en informatieveiligheid dienstverlening ingericht (vergaderjaar 2012 – 2013, Kamerstuk 26 643 nr. 280).

Voor de komende twee jaar gaat deze taskforce de ministeries, uitvoeringsorganisaties, gemeenten, provincies en waterschappen bijstaan bij het verbeteren van hun bewustzijn van informatieveiligheid. De wijze waarop dit bereikt wordt, is door het maken van afspraken met de verschillende overheidslagen, in het kader van een verplichtende zelfregulering voor informatieveiligheid. Een stelsel van auditverplichtingen is daar onderdeel van. Er is specifieke aandacht voorzien voor de afzonderlijke ketens waarbinnen informatie-uitwisseling plaatsvindt (vergaderjaar 2012 – 2013, Kamerstuk 26 643, nr. 269).

Behalve bewustwording en borging bij afzonderlijke organisaties is het van belang dat het samenspel van organisaties in het openbaar bestuur op het terrein van informatieveiligheid leidt tot een efficiënte en effectieve manier van de aanpak bij incidenten en crisis. Samen met het NCSC en schakelorganisaties van de medeoverheden wordt gewerkt aan een netwerk waarin kennis, melding van incidenten en *lessons learned* worden gedeeld en incidenten en crises worden opgepakt.

Infrastructuur

In het BNC-fiche betreffende de EU cyber security strategie wordt aangegeven dat zoveel mogelijk dient te worden aangesloten bij bestaande structuren. De leden van de D66-fractie vragen of het desondanks niet nodig zal kunnen zijn om bestaande structuren te vervangen om zo tot een coherente de EU cyber security strategie te komen.

Gelijkwaardigheid tussen lidstaten realiseren op het terrein van cyberbeveiliging is van cruciaal belang. In cyberspace gaat het immers om de zwakste schakel. Momenteel heeft elke lidstaat de vrijheid om te besluiten hoe en in welke mate de cyberbeveiliging wordt ingericht. Hierdoor bestaan er grote verschillen tussen de lidstaten. Kleinere verschillen tussen lidstaten zijn van belang bij de aanpak van bijvoorbeeld grensoverschrijdende cyberincidenten.

Gelijkwaardigheid is ook van belang om betrouwbaar, effectief en tijdig informatie uit te wisselen over incidenten. De EU cyber security strategie sluit aan bij de nationale inspanningen op het gebied van cyberbeveiliging. Door goede internationale afspraken tussen CERTs (Computer Emergency Response Team) en crisisautoriteiten kunnen adequate maatregelen genomen worden om een crisis vroegtijdig te beheersen. De EU cyber security strategie onderschrijft een integrale aanpak, niet alleen van de Europese instellingen maar ook van de lidstaten, en onderstreept het belang dat de EU hecht aan een open en vrij internet. De regering verwelkomt de voorgestelde maatregelen om vanuit de EU de lidstaten te ondersteunen bij het opbouwen van cybercapaciteiten en het versterken van samenwerkingsverbanden.

De regering is hierbij van mening dat zoveel mogelijk gebruik moet worden gemaakt van bestaande nationale en internationale structuren. Dus geen nieuwe structuren die bestaande en goed functionerende structuren binnen lidstaten vervangen of dupliceren op Europees niveau. Het kan echter niet worden uitgesloten dat nieuwe structuren noodzakelijk zullen blijken en daarom dienen te worden ingericht.

Effectiviteit van de strategie

De leden van de fractie van D66 menen dat preventie aan de voorkant minstens zo effectief is, zo niet effectiever is dan *damage control* achteraf. Deze leden vernemen graag de inzet van de regering op dit punt.

In reactie hierop onderstreept de regering ook de door deze leden gemaakte opmerking. Om te komen tot optimale cyber security en cybercriminaliteit drastisch tegen te kunnen gaan, dient te worden geïnvesteerd in de gehele cyberveiligheidsketen: awareness, weerbaarheid, detectie, notificatie, response, crisismanagement, opsporing, vervolging en evaluatie.

De keten begint bij het verhogen van awareness en de weerbaarheid om alle betrokken partijen bewuster te laten omgaan met hun cyber security. Awareness en weerbaarheid zijn dan ook zeer belangrijke onderdelen binnen de Nederlandse cyber strategie. Voorbeelden zijn: de jaarlijkse Alert Online campagne, het dreigingsbeeld van het NCSC (CSBN) en de inzet op onderzoek en innovatie. Onderzoek betreft bijvoorbeeld het komen tot veiligere ICT.

Naast het verhogen van awareness en de weerbaarheid is het ook zaak de detectie, notificatie en response goed in te richten. Het is belangrijk een incident zo snel mogelijk te kunnen detecteren, zodat er voldoende tijd is

om de notificatie en response in te richten en indien noodzakelijk crisis management te starten. Hierdoor kan de impact van een incident worden beperkt. Daarna is bij criminaliteit opsporing en vervolging van belang, zodat daders niet nogmaals kunnen zorgen voor een incident. Een goede evaluatie kan er tot slot toe dienen om lessen te trekken en hiermee de cyberveiligheidsketen te verbeteren en versterken.

Bovenstaande geeft aan dat een integrale aanpak essentieel is. Cyber security wordt bevorderd door een brede inzet op te nemen maatregelen, waarbij samenwerking een cruciale voorwaarde is.

Ook willen de leden van de D66-fractie graag weten hoe de EU cyber security strategie zal worden geëvalueerd en geïmplementeerd. De regering ziet deze strategie niet als een opmaat naar een breed wetgevingsvoorstel, maar als een overzicht met maatregelen die relevant zijn op het brede terrein van cyber security.

De maatregelen zoals die in de EU cyber security strategie zijn opgenomen, moeten volgens de regering worden omgezet naar een actieprogramma dat SMART geformuleerd is. Dus waarbij duidelijk is wie, wanneer, wat moet doen.

Voor de uitvoering van de maatregelen die in de EU cyber security strategie zijn opgenomen, zijn verschillende partijen betrokken. Onder andere de Europese Commissie, de lidstaten, ENISA, maar ook private partijen. Het is daarom van belang dat niet alleen de Europese Commissie, maar ook bijvoorbeeld de lidstaten bij de beoordeling van de voortgang van de maatregelen worden betrokken.

Vragen over de richtlijn netwerk- en informatiebeveiliging COM(2013)48

Uitwerking kader richtlijn naar een hoog beveiligingsniveau

De leden van de PvdA-fractie uiten hun zorgen over het tempo waarop het proces van cyberbeveiliging op gang komt.

Het terrein van cyberbeveiliging is een complex en dynamisch terrein met veel nieuwe ontwikkelingen. In een aantal EU-landen, zoals het Verenigd Koninkrijk, Frankrijk, Duitsland, Nederland en Zweden heeft cyberbeveiliging prioriteit en worden in snel tempo capaciteiten opgebouwd. In Nederland is bijvoorbeeld een Nationaal Cyber Security Centrum (NCSC) opgericht en een Cyber Security Raad. Samenwerkingsverbanden (publiek en privaat) worden sindsdien snel opgebouwd.

Ook op internationaal niveau, vindt steeds meer en intensiever samenwerking plaats. Van het delen van *best-practices*, operationele samenwerking tot het doen van gezamenlijk onderzoek. Met de komst van de EU cyber security strategie en het voorstel voor de NIB-richtlijn gaat een extra prikkel uit naar alle landen binnen de EU om cyberbeveiliging tot prioriteit te maken. Ondanks dat er grote stappen worden gemaakt op het terrein van cyber security, is het zo dat wet- en regelgeving vaak tijd kost, vooral op Europees niveau.

De leden van de VVD-fractie en de leden van de CDA-fractie vragen zich af hoe het doel van de NIB-richtlijn zich verhoudt met artikel 14 van deze voorgestelde richtlijn. Daarnaast wordt door deze leden de vraag gesteld of de NIB-richtlijn wellicht een ambitieuzer doelstelling heeft dan de Wet bescherming persoonsgegevens (Wbp) en de nog geldende Europese privacyrichtlijn.

De NIB-richtlijn heeft inderdaad als doelstelling dat er binnen de EU een hoog gemeenschappelijk beveiligingsniveau van netwerk- en informatiesystemen wordt bereikt en gehandhaafd. Daartoe regelt de NIB-richtlijn de verplichtingen voor lidstaten om een nationale NIB-strategie vast te stellen, een voor netwerk- en informatiebeveiliging bevoegde nationale autoriteit aan te wijzen en een computercrisisteam op te zetten. Daarnaast dienen lidstaten ervoor te zorgen dat overheden en specifieke marktdeelnemers passende technische en organisatorische maatregelen nemen. Dit om met name incidenten met betrekking tot de voor hun kerndiensten in gebruik zijnde netwerk- en informatiesystemen te voorkomen en te minimaliseren en aldus te zorgen voor de continuïteit van die diensten.

Bepaald is voorts dat het te waarborgen beveiligingsniveau moet zijn afgestemd op de risico's die zich voordoen en dat bij het treffen van die maatregelen rekening dient te worden gehouden met de meest recente technische mogelijkheden. Hiermee verschilt de NIB-richtlijn niet zozeer in ambitieniveau van de huidige Europese privacyrichtlijn en de Wet bescherming persoonsgegevens. Ook voor laatstgenoemde richtlijn geldt dat in de overwegingen is opgenomen dat de daarmee beoogde onderlinge aanpassing van de nationale wetgevingen betreffende de verwerking van persoonsgegevens erop is gericht een hoog beschermingsniveau binnen de EU te waarborgen. Vervolgens wordt in de artikelen onder meer bepaald dat de lidstaten dienen te bepalen dat de voor verwerking van persoonsgegevens verantwoordelijken ter beveiliging van die gegevens passende technische en organisatorische maatregelen moeten treffen. Bovendien volgt uit het op dat laatste betrekking hebbende artikel in de Wet bescherming persoonsgegevens eveneens dat bij het treffen van beveiligingsmaatregelen rekening moet worden gehouden met onder meer de stand van de techniek. Daarnaast dat het beveiligingsniveau moet zijn afgestemd op de risico's met betrekking tot de te beveiligen gegevens.

Beveiligingsautoriteit

In de NIB-richtlijn is bepaald dat elke lidstaat een bevoegde autoriteit aanwijst. De leden van VVD-fractie en de leden van de CDA-fractie vragen de regering hoe deze bevoegde autoriteit dient worden ingericht.
De bevoegde autoriteit zoals in de NIB-richtlijn beschreven, omvat meerdere functies: operationeel, beleidsmatig en toezichthoudend. De regering is van mening dat zo'n grote hoeveelheid van verschillende functies binnen een autoriteit niet wenselijk is en dat zoveel mogelijk moet worden aangesloten bij bestaande structuren.

Zo is de operationele rol bij het NCSC (Nederlandse CERT) belegd. Incidentafhandeling moet door en tussen CERTs worden afgehandeld. Daarnaast hebben we in Nederland toezicht op sectoraal niveau georganiseerd en niet bij één organisatie. De bevoegde autoriteit waar de NIB-richtlijn naar verwijst zal zich vooral moeten richten op het organiseren van het crisisoverleg (gezamenlijke communicatie op politiek-bestuurlijk niveau).

Meldplicht incidenten

De leden van de fracties D66, CDA, VVD en SP stellen verschillende vragen rondom de meldplicht bij incidenten en de meldplicht bij datalekken.

Er dient een scheiding te worden gemaakt tussen het melden van cyber security incidenten in het algemeen en het melden van security breaches en het melden van datalekken in het bijzonder.

In geval van cyber security breaches, waar zowel de NIB-richtlijn over spreekt alsmede waarover gesproken wordt in de uitwerking van de Nederlandse security breach notification n.a.v. de motie Hennis-Plasschaert c.s. (Kamerstukken II 2011/2012, 26 643, nr. 202), betreft het inbreuken op de veiligheid en of integriteit van informatiesystemen die de continuïteit van de eigen of andermans dienstverlening in belangrijke mate kunnen verstoren en die potentieel leiden tot maatschappelijke ontwrichting. In geval van datalekken gaat het om inbreuken op beveiligingsmaatregelen voor persoonsgegevens.

De leden van de D66-fractie vragen of de meldplicht in het huidige voorstel niet wordt afgezwakt en of een meldplicht niet noodzakelijk is voor het beschermen van persoonsgegevens. Zoals reeds is aangegeven, dient er een onderscheid te worden gemaakt tussen de meldplicht rondom cyber security incidenten en het melden van datalekken.

De bereidheid onder organisaties tot het vrijwillig melden van cyber security incidenten neemt toe. Het aantal gemelde cyber security breaches is echter nog relatief gering. Om deze reden wordt naar aanleiding van de motie Hennis-Plasschaert c.s. (Kamerstukken II 2011/2012, 26 643, nr. 202) door de minister van VenJ ontwerpwetgeving voorbereid, die strekt tot de regeling van een meldplicht voor de overheid en private bedrijven in randvoorwaardelijke sectoren van cyberincidenten met een potentieel maatschappelijk ontwrichtende werking. Dit is ook de lijn die de regering binnen de EU zal hanteren.

Ook voor datalekken geldt dat de bereidheid tot het vrijwillig melden ervan aan de toezichthouder of aan de betrokkenen, wier persoonsgegevens het betreft, gering is. De verwachting is gerechtvaardigd dat een wettelijke verplichting het aantal meldingen zal doen toenemen. De overheid verstrekt daarmee juridische duidelijkheid wanneer het doen van een melding verplicht is. Op grond hiervan zullen de geadresseerden van de meldplicht hun verantwoordelijkheid moeten nemen. Een wetsvoorstel tot aanvulling van de Wet bescherming persoonsgegevens met een meldplicht voor datalekken is onlangs bij de Tweede Kamer ingediend. Bij de uitwerking van de EU cyber security strategie zal Nederland pleiten voor het behoud van de reeds bestaande nationale structuren.

De leden van de VVD-fractie en de leden van de CDA-fractie willen daarnaast helderheid over de verhouding tussen de meldplicht in de voorgestelde Europese privacyverordening en de meldplicht zoals beschreven in de NIB-richtlijn. Hierbij worden vragen gesteld over de gedelegeerde handelingen in artikel 14(5) met betrekking tot de omstandigheden waarin overheden en marktdeelnemers incidenten moeten melden.

Wederom is het belangrijk om aan te geven dat de Europese verordening gegevensbescherming en de NIB-richtlijn twee gescheiden trajecten zijn. De NIB-richtlijn richt zich op incidenten met een aanzienlijke impact op de veiligheid. De verordening gegevensbescherming ziet toe op de bescherming van privacy-gevoelige informatie en mogelijke inbreuken daarop. Het is van belang deze te scheiden aangezien er ook incidenten zijn waarbij de privacy niet direct wordt aangetast, maar waarbij wel een aanzienlijk veiligheidsrisico wordt gelopen. Denk daarbij bijvoorbeeld aan aansturingssystemen in de vitale sectoren.

Nederland is kritisch ten aanzien van de gedelegeerde handelingen omtrent de omschrijving van de omstandigheden waarin overheden en markdeelnemers incidenten moeten melden (artikel 14(5)). Nederland is voorstander van een meldplicht die is ingericht volgens de Nederlandse

criteria waarbij het belangrijk is dat alleen incidenten met een mogelijk ontwrichtende werking voor de nationale veiligheid worden gemeld. De richtsnoeren, zoals beschreven in artikel 14(6) die kunnen worden vastgesteld op grond van artikel 14(5), dienen hiermee in lijn te zijn en zullen een aanvullend karakter moeten hebben. Deze lijn zal tijdens de onderhandelingen worden uitgedragen.

De leden van de SP-fractie stellen vragen bij de huidige omschrijving van een incident in de NIB-richtlijn en menen dat hierdoor mislukte aanvallen buiten beschouwing worden gelaten terwijl deze van belang kunnen zijn bij de bestrijding van cybercrime.

De regering is van mening dat er bij het melden van incidenten en breaches gezocht dient te worden naar een balans tussen administratieve lasten en het doel van de voorgestelde security breach notification zijnde het verhogen van de digitale veiligheid. Bij de uitwerking van de meldplicht is het realiseren van digitaal veiligheidsmanagement daarbij het streven. Dit houdt in dat organisaties kennis delen om risico's en breaches beter in te kunnen schatten, binnen de sector luchtvaart staat dit bekend als «*just culture*».

Inderdaad komen pogingen tot aanvallen op zeer geregelde basis voor. Niet al deze aanvallen zijn detecteerbaar. Daarmee zou het melden van alle pogingen een onevenredige verbreding van de scope zijn. De NIB-richtlijn heeft betrekking op incidenten met een daadwerkelijk schadelijk effect op de beveiliging. Het staat partijen uiteraard vrij om relevante pogingen alsnog kenbaar te maken bij het NCSC.
Daarnaast vragen de leden van de SP-fractie zich af of grensoverschrijdende bedrijven onder verschillende meldplichten kunnen vallen. Vervolgens vragen de leden van de SP-fractie of kleinbedrijven inderdaad zijn uitgesloten van de meldplicht.

Met het oog op de nationale veiligheid is het belangrijk dat incidenten met een mogelijk ontwrichtende werking gemeld worden. Het uitgangspunt hierbij is dat een bedrijf dat valt onder de werking van de NIB-richtlijn meldt aan de nationale autoriteit. Als er sprake is van grensoverschrijdende incidenten zou de melding daardoor in meerdere landen kunnen plaatsvinden. Uiteraard zal Nederland bij de onderhandelingen over de NIB-richtlijn aandacht hebben voor de administratieve lasten voor bedrijven. In de implementatie van de NIB-richtlijn zullen deze punten nader worden uitgewerkt.

Zoals eerder reeds is aangegeven, dient er een onderscheid gemaakt te worden tussen de diverse meldplichten en de bijbehorende doelen daarvan. De in de NIB-richtlijn voorgestelde meldplicht alsmede de Nederlandse security breach notification ziet op het melden door partijen binnen de vitale sectoren. Daarbij gaat het niet om de grootte van deze partijen, maar om het vitale product en/of de dienst die zij leveren.

Uitvoering richtlijn

De leden van de SP-fractie en de leden van de D66-fractie benoemen het belang van de borging van privacy van burgers bij het uitwisselen van gegevens en vragen welke informatie gedeeld mag worden. Daarnaast vragen de leden van de D66-fractie de regering hoe binnen de EU cyber security strategie de privacy is gewaarborgd.

De EU cyber security strategie roept op tot meer samenwerking op het terrein van cyber security (zowel binnen als buiten de EU). Internationale

samenwerking is belangrijk omdat cyber security veelal grensoverschrijdend is.

Wanneer samenwerking plaatsvindt, is het kunnen uitwisselen van informatie cruciaal. Ook op nationaal niveau wordt onder andere binnen het NCSC samengewerkt met een groot aantal publieke en private organisaties. Daarbij is het belangrijk om goede afspraken te maken over welke informatie wel of niet kan worden gedeeld, met welke personen, onder welke omstandigheden, op welke manier en met welk doel. Ook geldt het uitgangspunt van proportionaliteit. Transparantie hierover is van groot belang. Daarnaast dient de informatie-uitwisseling binnen de kaders van bestaande wetgeving te gebeuren. Ditzelfde dient ook te gelden voor informatie-uitwisseling op Europees niveau.

In de huidige EU cyber security strategie worden wel maatregelen benoemd, ook voor het uitwisselen van informatie, maar is niet uitgewerkt op welke wijze en onder welke randvoorwaarden informatie wordt gedeeld. De verdere invulling zal middels de onderhandelingen over de NIB-richtlijn verder worden vormgegeven.

Bij de uitwerking van de EU cyber security strategie zal het standpunt van de regering zijn dat binnen de huidige Nederlandse kaders ten aanzien van de bescherming persoonsgegevens zal worden gehandeld.

Verantwoordelijkheid producenten

De leden van de SP-fractie vragen de regering welke verantwoordelijkheden gelden voor software- en hardwareproducenten en hosters.

Om tot een hoog niveau van netwerk- en informatiebeveiliging te komen is het belangrijk dat er veilige ICT-producten worden ontwikkeld. De leveranciers van deze producten dragen hiervoor een eigen verantwoordelijkheid in de vorm van een zorgplicht. Daar staat goed opdrachtgeverschap (zakelijke mark) en veilig gebruik tegenover. Gegeven deze gedeelde en gezamenlijke verantwoordelijkheid, is het wel van belang dat veilige producten en verdere standaardisering door middel van publiek private samenwerking worden ontwikkeld. Deze gesprekken tussen overheid en bedrijven worden reeds gevoerd en komen in brede zin in de herijking van de Nederlandse strategie (NCSS 2) nadrukkelijk aan de orde.

De EU cyber security strategie sluit hierop aan en vraagt ook expliciet aandacht voor deze benadering. Zo is aangegeven dat er een nieuw publiek privaat samenwerkingsforum zal komen, het NIS-platform, op Europees niveau. Dit platform moet de juiste incentives ontwikkelen voor veilige ICT producten en dient verdere standaardisering en normering te stimuleren. Nederland zal binnen dit platform een actieve rol innemen.

Tot slot

De leden van de D66-fractie vragen om een periodieke update over de ontwikkelingen van deze dossiers.

De Eerste Kamer zal schriftelijk worden geïnformeerd over de onderhandelingen van de NIB-richtlijn. Omdat de voortgang van de onderhandeling over de NIB-richtlijn in de EU Telecomraad wordt besproken, zal er twee maal per jaar, nadat de Telecomraad heeft plaatsgevonden, worden geïnformeerd. Indien er tussentijds belangrijke ontwikkelingen zijn rondom de NIB-richtlijn zal de Eerste Kamer ook dan schriftelijk worden geïnformeerd.