Eerste Kamer der Staten-Generaal

Binnenhof 22
postbus 20017
2500 EA Den Haag

telefoon 070-312 92 00
fax 070-312 93 90

e-mail postbus@eerstekamer.nl
Internet www.eerstekamer.nl

Minister van Veiligheid en Justitie
De heer mr. I.W. Opstelten
Postbus 20301
2500 EH Den Haag

datum 5 juni 2013
betreft Cyberbeveiliging
ons kenmerk 153016u

Geachte heer Opstelten,

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.[1] 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

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

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.

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.

Hoogachtend,

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