Ministerie van Veiligheid en Justitie

> Retouradres Postbus 20011 2500 EA Den Haag

Aan de Voorzitter van de Eerste Kamer
der Staten-Generaal
Postbus 20018
2500 EA DEN HAAG

Nationaal Coördinator Terrorismebestrijding en Veiligheid
Directie Cyber Security
DCS

Turfmarkt 147
2511 DP Den Haag
Postbus 20011
2500 EA Den Haag
www.nctv.nl

Uw kenmerk
153016.02U

Ons kenmerk
448463

Bij beantwoording de datum en ons kenmerk vermelden. Wilt u slechts één zaak in uw brief behandelen.

Datum 26 november 2013
Onderwerp Beantwoording Eerste Kamervragen betreffende cyberbeveiliging

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. 11 oktober 2013, met kenmerk 153016.02U, 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 ontwerprichtlijn netwerk - en informatiebeveiliging [COM (2013)48]

Directie Cyber Security

Datum
26 november 2013

Ons kenmerk
448463

De leden van de commissie voor Immigratie & Asiel / JBZ-Raad uiten hun zorg over de voortgang van de ontwerprichtlijn voor Netwerk- en Informatiebeveiliging.

Het kabinet onderschrijft de noodzaak dat er stappen gemaakt moeten worden op het terrein van cybersecurity en verwelkomt daarom ook deze ontwerprichtlijn. Nederland is het eens met de Commissie dat veel bereikt is op basis van vrijwillige regulering, maar dat er in de EU nog steeds lacunes zijn in nationale capaciteiten, bij de coördinatie in geval van grensoverschrijdende incidenten en met betrekking tot de betrokkenheid en paraatheid van de private sector. Terwijl tegelijkertijd gewerkt wordt aan de implementatie van de bredere Mededeling met de Strategie inzake cyberbeveiliging van de Europese Unie, vergt het traject voor de ontwerp-richtlijn tijd. De Raad heeft in de Raadswerkgroep Telecom & Informatiemaatschappij inmiddels 7 maal over de richtlijn gesproken, waarbij de Raad artikelsgewijs door de richtlijn is gelopen. De verwachting is dat gedurende het Litouws voorzitterschap de eerste behandeling van het voorstel kan plaatsvinden. Tegelijk werkt het Europees Parlement in de Commissies voor Interne Markt en Consumentenbescherming (IMCO), voor Industrie, Onderzoek en Energie (ITRE) en voor Burgerlijke vrijheden, justitie en binnenlandse zaken (LIBE) aan zijn inbreng voor deze richtlijn. Het Europees Parlement zal naar verwachting zijn positie eind januari 2014 bepalen.

Hoofdstuk II - Nationale kaders voor netwerk - en informatiebeveiliging

De commissie vraagt naar een indicatie van de termijn waarbinnen de plannen met betrekking tot de nationale Netwerk en Informatie beveiliging-strategieën van Lidstaten en de nationale samenwerkingsplannen tot stand dienen te komen. Conform het huidige voorstel dienen de Lidstaten binnen anderhalf jaar na totstandkoming van de richtlijn de maatregelen te implementeren, waaronder de totstandkoming van een nationale cybersecurity strategie en een samenwerkingsplan. Momenteel zijn al vele Lidstaten bezig met het ontwikkelen van een nationale strategie op het gebied van netwerk- en informatiebeveiliging. Nederland moedigt dit ook aan. Zo wordt bijvoorbeeld in de Friends of the Presidency (FoP) Group on Cyber Issues en ook in bilaterale contacten de tweede Nederlandse Nationale Cybersecuritystrategie van 28 oktober jl. (Kamerstukken II, 2013-2014, 26643, nr. 291) en de totstandkoming daarvan besproken.

De leden van de commissie vragen voorts ook naar de voortgang van een actieprogramma op basis van de EU Cybersecurity Strategie. Hieraan wordt gezamenlijk met het Voorzitterschap, de Commissie, de Europese Dienst voor Extern Optreden (EDEO) en de Lidstaten zelf in de FoP Group on Cyber Issues gewerkt. Nederland heeft daartoe met enkele andere Lidstaten, te weten het Verenigd Koninkrijk, Frankrijk en Duitsland, ook een non-paper opgesteld om nader richting aan een dergelijk actieprogramma of een zogenaamde 'roadmap' te geven. Het Voorzitterschap werkt aan een concept roadmap. De roadmap zal dienen als implementatie-instrument voor de FoP Group om de acties zoals die in de Strategie al verwoord zijn (in de tekstkaders) nader richting te geven. De FoP Group bewaakt de horizontale samenhang van implementatie over de verschillende Raadswerkgroepen en gremia heen.

Hoofdstuk III - Samenwerking tussen bevoegde autoriteiten

Vervolgens vraagt de commissie naar de mogelijkheden om de samenwerking tussen bevoegde autoriteiten te versterken. In het BNC-fiche is verwoord dat Nederland tegen opgelegde verplichtingen vanuit de EU is, die raken aan de nationale veiligheid en dus aan nationale bevoegdheden. Lidstaten moeten zelf kunnen bepalen hoe op nationaal niveau wordt samengewerkt tussen betrokken partijen. Nederland is voorstander van een beleidsmatige, sturende, randvoorwaardelijke rol voor de Competent Authorities, en een operationele rol die belegd wordt bij de Computer Emergency Respons Teams (CERTs). Bovendien vind ik dat de Competent Authority geen te operationele rol dient te hebben bij incidenten en early warnings. Uiteraard dient de nationale CERT de eigen Competent Authority steeds goed te informeren. Het valt nog te bezien hoe andere landen hun Competente Autoriteit of Autoriteiten in zullen vullen. Het netwerk van Competent Authorities kan daarom vooral een actieve rol spelen in crisissamenwerking bij een Europese crisis, zorgen voor de beleidsmatige en politiek-bestuurlijke afstemming waar nodig, en heeft een rol bij bewustwordingscampagnes voor het grote publiek.
Het kabinet acht het bovendien wenselijk om samenwerking op het gebied van netwerk- en informatiebeveiliging op basis van bestaande structuren en samenwerkingsvormen te versterken in plaats van het op korte termijn af te dwingen. In Nederland is de implementatie van de eerste Nationale Cybersecurity Strategie zo voorspoedig gelopen dat vorige week een nieuwe strategie kon worden uitgebracht. De samenwerking binnen structuren als het Nationale Cyber Security Centrum, de Cyber Security Raad, de ICT Response Board, de Information Sharing and Analysis Centres en andere samenwerkingsverbanden is in die periode sterk gegroeid zodat we daar nu de vruchten van kunnen plukken. Het kabinet acht het wenselijk als dit proces in Europa bij voorkeur ook op een dergelijke wijze plaatsvindt.

De commissie vraagt ook naar het geval van een aanval op Nederlandse doelen. Wanneer sprake is van (potentieel) maatschappelijke ontwrichting in Nederland, kan de nationale crisisstructuur in werking treden. Deze structuur is regelmatig beoefend en is bijvoorbeeld in werking getreden tijdens de DigiNotar crisis. De ervaringen zoals de DigiNotar-casus laten zien dat er op basis van bestaande structuren slagvaardig gehandeld kan worden. Het rapport van de Inspectie VenJ n.a.v. het DigiNotar incident onderschrijft dit.

Bij een ICT-crisis met (potentieel) maatschappelijke ontwrichting heeft het NCSC op operationeel niveau een coördinerende taak, waaronder het bijeenbrengen en duiden van de juiste operationele informatie en het adviseren van de nationale crisisstructuur over te nemen maatregelen. De publiek-private ICT response board is hierbij een belangrijk adviesinstrument.

Hoofdstuk IV - Beveiliging van de netwerken en overheden en marktdeelnemers

De leden van de commissie vragen naar de Europese randvoorwaarden waaraan risico-beheersende maatregelen van Lidstaten moeten voldoen. Op dit moment is nog onvoldoende duidelijk welke maatregelen de Commissie en de Lidstaten in dit verband specifiek voor ogen hebben. Om echter een publiek-privaat gedragen beeld te realiseren met betrekking tot standaarden en risicobeheersings-maatregelen, heeft de Europese Commissie al wel onder andere het publiek-private Netwerk en Informatie Beveiligings Platform (NIS Platform) ingericht. Het

NIS platform stemt in drie verschillende werkgroepen af over risicomanagement, informatiedeling, en onderzoek en innovatie.

De commissie vraagt ook naar de verantwoording van marktdeelnemers en overheden ter zake. Daar waar naar aanleiding van de onderhandelingen zal worden overgegaan tot implementatie van artikel 14(1) van de ontwerprichtlijn, zal worden aangesloten, conform het BNC-fiche, bij bestaande structuren, dat wil zeggen door middel van implementatie in sectorale wet- en regelgeving. Dit artikel is inmiddels ook in de Raadswerkgroep behandeld. Vooralsnog zie ik geen aanleiding te veronderstellen dat een impasse dreigt. Ik zal de voortgang nauwgezet volgen.

Vragen over Awareness

Met de Commissie deel ik de mening dat er nog een behoorlijke stap kan en moet worden gemaakt om awareness te verhogen. De menselijke component is en blijft juist bij cyber security de kritieke factor. Nederland heeft in 2013 besloten om de tweede Alert Online campagne aaneensluitend aan de European Cyber Security Month te organiseren. Deze campagne heb ik op maandag 28 oktober afgetrapt. Met het thema smart security wil ik met de campagne een verdieping aanbrengen in de richting van bedrijven en ondernemers. Daarnaast stimuleert het Nationaal Platform Criminaliteitsbeheersing bewustwording bij het midden en klein-bedrijf (MKB) met de campagne StopCybercrime.nu. Bij onder andere ondernemersdagen van MKB-Nederland wordt dit thema onder de aandacht gebracht van ondernemers. Bovendien zal het kabinet, met de tweede Nationale Cybersecurity Strategie het cyber bouwwerk verder versterken, waarbij het streven is om van bewustzijn naar bekwaamheid te komen.

Daarnaast vraagt de commissie naar het instellen van een meldplicht voor het MKB. Ik acht het niet wenselijk om een meldplicht als bewustzijns-vergrotende maatregel voor het MKB in te richten. Ook de lijst van sectoren die in de bijlage van het ontwerpvoorstel voor de Netwerk- en Informatie Beveiligings-richtlijn staat, is niet in algemene zin van toepassing op het MKB.

Het wetsvoorstel Melding inbreuken elektronische informatiesystemen, introduceert een meldplicht voor ICT-inbreuken, te melden bij het NCSC. Inmiddels is de consultatie voor dit wetsvoorstel gesloten en worden de bijdragen verwerkt. Doelstelling van het wetsvoorstel betreft het kunnen voorkomen of beperken van maatschappelijke ontwrichting. De melding stelt het NCSC in staat om hulp te verlenen aan de getroffen aanbieder en om andere vitale aanbieders te waarschuwen, met als uiteindelijke doel om het risico van maatschappelijke ontwrichting in te schatten en die ontwrichting te voorkomen of in elk geval zo veel mogelijk te beperken. Teneinde een balans tussen de administratieve lasten en het doel van het wetsvoorstel te realiseren, is bewust gekozen om de meldplicht alleen van toepassing te laten zijn op aanbieders van producten of diensten waarvan de beschikbaarheid of betrouwbaarheid van vitaal belang is voor de Nederlandse samenleving, en alleen als de inbreuk tot gevolg heeft of kan hebben dat de beschikbaarheid of betrouwbaarheid in belangrijke mate wordt onderbroken. In algemene zin is deze meldplicht dus ook niet van toepassing op MKB.

Vragen over Meldplicht van databreaches

De commissie stelt enkele vragen over de meldplicht 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 het wetsvoorstel 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.

Wat de meldplicht datalekken ter beveiliging van persoonsgegevens betreft, is er op 21 juni 2013 bij de Tweede Kamer een voorstel van wet ingediend tot wijziging van de Wet bescherming persoonsgegevens (Kamerstukken II 2012/13, 33662, nrs. 1-3) waarin een meldplicht voor datalekken wordt geregeld, specifiek voor gevallen waarin een doorbreking van de beveiligingsmaatregelen zou leiden tot een aanmerkelijk risico op verlies of onrechtmatige verwerking van gegevens.

Laatstbedoeld wetsvoorstel voorziet niet in een algemene uitzondering op de meldplicht voor het MKB. Wel wordt voorgesteld om de nadelen die evident verbonden zijn aan een meldplicht die zonder enig onderscheid zou gelden voor alle verantwoordelijken te ondervangen. Een effectieve meldplicht kan alleen worden bereikt wanneer toezichthouder en publiek niet overvoerd worden door een al te routineuze melding van elk denkbaar datalek. Er wordt gekozen voor een model waarin de betrokkene een aantal afwegingen moet verrichten die refereren aan het risico dat met de verwerking wordt doorlopen. Van deze regeling zal het MKB naar verwachting wat meer kunnen profiteren dan grotere bedrijven. Met het voorgaande wordt overigens niet gezegd dat verhoging van het bewustzijn van burgers, bedrijven en overheidsinstellingen bij een goede beveiliging van persoonsgegevens en ICT-systemen niet voortdurend aandacht verdient. Zoals reeds vermeld, organiseert het kabinet daarom op meerdere thema's bewustwordingscampagnes.

Tot slot

Met de beantwoording in deze brief ga ik ervan uit u voldoende te hebben geïnformeerd. Zoals eerder toegezegd, zal ik Uw Kamer in elk geval na de Telecomraad in december wederom informeren over de stand van zaken met betrekking tot de richtlijn voor netwerk- en informatiebeveiliging.