Eerste Kamer der Staten-Generaal

1

Vergaderjaar 2017–2018

34 883 Regels ter implementatie van richtlijn (EU) 2016/1148 (Wet beveiliging netwerk- en informatiesystemen)

B

VOORLOPIG VERSLAG VAN DE VASTE COMMISSIE VOOR JUSTITIE EN VEILIGHEID[1]

Vastgesteld 16 juli 2018

Het voorbereidend onderzoek heeft de commissie aanleiding gegeven tot het maken van de volgende opmerkingen en het stellen van de volgende vragen.

Inleiding

De leden van de **VVD**-fractie hebben met belangstelling kennis genomen van het wetsvoorstel beveillging netwerk- en informatiesystemen. Zij onderschrijven het belang van dit wetsvoorstel en zijn verheugd dat deze ter behandeling voorligt in de Eerste Kamer. De (Nederlandse) samenleving is immers in toenemende mate afhankelijk van het naar behoren en veilig functioneren van netwerk- en informatiesystemen. De leden van de VVD-fractie hebben nog wel enkele vragen die zij graag spoedig beantwoord zien. De implementatietermijn is op 9 mei jl. immers reeds verstreken en het zou goed zou zijn als het wetsvoorstel zo snel mogelijk in werking kan treden.

De leden van de fractie van de **PvdA** hebben met belangstelling kennisgenomen van de Wet beveiliging netwerk- en informatiesystemen. Graag maken zij gebruik van de gelegenheid de regering hierover enkele vragen te stellen. De fractie van de **SP** sluit zich bij een van de vragen aan.

Taken van de Minister van Justitie en Veiligheid

De Minister van J&V heeft ex artikel 3 lid 1 sub c van het wetsvoorstel onder meer als taak het bijstaan van vitale aanbieders en van andere

[1] Samenstelling:
Engels (D66), Kox (SP), Van Bijsterveld (CDA) (*vicevoorzitter*), Duthler (VVD) *(voorzitter),* Ten Hoeve (OSF), Koffeman (PvdD), Strik (GL), Knip (VVD), Backer (D66), Schouwenaar (VVD), Van Strien (PVV), Kok (PVV), Gerkens (SP), Vlietstra (PvdA), Lokin-Sassen (CDA), Bredenoord (D66), Dercksen (PVV), D.J.H. van Dijk (SGP), Van Rij (CDA), Rombouts (CDA), Van de Ven (VVD), Wezel (SP), Bikker (CU), Baay-Timmerman (50PLUS) Van Zandbrink (PvdA), vac. (PVV), Fiers (PvdA)

kst-34883-B
ISSN 0921 - 7371
's-Gravenhage 2018

aanbieders die onderdeel zijn van de rijksoverheid bij het treffen van maatregelen om de continuïteit van hun diensten te waarborgen of te herstellen. De leden van de **VVD**-fractie vragen de regering wat het bijstaan precies inhoudt? Tot hoever reikt deze taak? Beperkt de Minister zich tot het geven van algemene adviezen en best practices? Of gaat de Minister ook individuele aanbieders bijstaan en van adviezen voorzien? Zal de Minister bijvoorbeeld ook ten behoeve van het uitbrengen van adviezen zogenaamde nulmetingen en andere assessments uitvoeren?

In artikel 3, tweede lid sub b en c wordt een onderscheid gemaakt tussen CSIRT's en andere computercrisisteams, die worden aangewezen bij ministeriële regeling. Wat is het onderscheid tussen een CSIRT en een computercrisisteam? En wat zijn de criteria om op de lijst van de ministeriële regeling te komen, zo vragen de leden van de VVD-fractie? Hoe wordt voorkomen dat een organisatie die niet op de lijst staat, maar wel voor een bepaalde sector of beroepsgroep vergelijkbare diensten verleent als die van een computercrisisteam ook geïnformeerd wordt over dreigingen en incidenten?

Meldplicht voor incidenten

Bijzonder is dat zorgaanbieders nu ook gekwalificeerd gaan worden als aanbieders van essentiële diensten. In de voorganger van deze wet – de Wet gegevensverwerking en meldplicht cybersecurity –, waren zij namelijk uitgesloten van deze categorie.
Verder worden er drie Ministers en DNB aangewezen als bevoegde autoriteit waaraan gemeld moet worden, naast de Minister van Justitie en Veiligheid. Mocht een incident betrekking hebben op persoonsgegevens, dan moet datzelfde incident ook gemeld worden bij de Autoriteit Persoonsgegevens. Dit betekent dat een aanbieder mogelijk bij drie instanties moet melden. Hoe wordt voorkomen dat aanbieders die bij verschillende instanties dezelfde meldingen moeten doen op verschillende wijzen worden behandeld, zo vragen de leden van de **VVD**-fractie? En hoe wordt onnodige administratieve rompslomp voor deze aanbieders voorkomen?

In de wet zijn vier categorieën «bevoegde autoriteit» opgenomen. Niet (alle incidenten van) alle aanbieders zullen in een specifieke categorie vallen. Hoe en bij wie moeten deze «overige categorie» aanbieders hun incidenten melden, zo vragen de leden van de VVD-fractie?

De leden van de **PvdA**-fractie menen dat de aard van een aanval of inbreuk minder een criterium van invloed zou moeten zijn, en de nadruk zou moeten liggen op de gevolgen van de ICT-inbreuk. Is de regering dit met hen eens? Zo nee, waarom niet? Graag vragen zij specifieke aandacht voor DDoS-aanvallen. Deze kunnen de beschikbaarheid van diensten van aanbieders in vitale sectoren ernstig inperken. Is de regering bereid om dergelijke DDoS-aanvallen op te nemen in de meldplicht? Zo nee, waarom niet?

De gevolgen voor wat betreft eventuele aansprakelijkheid zouden een grote drempel kunnen zijn om ICT-inbreuken te melden. Echter, dat is nu precies wat de richtlijn probeert te vermijden. De leden van de PvdA-fractie menen niet dat aansprakelijkheid voor eventuele fouten moet worden weggenomen wanneer deze gemeld worden. Zij menen wel dat de aansprakelijkheid door het doen van de melding niet mag toenemen. Is de regering dit met hen eens?

Als gevolg van het voorliggende wetsvoorstel dienen ernstige ICT-incidenten dubbel gemeld te worden: zowel bij het CSIRT als bij de

bevoegde autoriteit. De leden van de fractie van de PvdA merken op dat ernaar gestreefd wordt deze dubbele meldplicht technisch zó in te richten dat het verspreiden van de benodigde informatie maar één handeling vergt. Zij vernemen graag van de regering welke rol zij voor zichzelf ziet in het bevorderen van de samenwerking tussen de betrokken autoriteiten.

Verwerking van gegevens

De leden van de **PvdA**-fractie constateren dat het NCSC de bevoegdheid krijgt om eenieder te verzoeken om gegevens te verstrekken. Zij merken op dat ontvangers van het verzoek weliswaar niet verplicht zijn mee te werken, maar daar mogelijk niet van op de hoogte zijn en zich toch verplicht voelen om mee te werken. Acht de regering dit wenselijk? Zo nee, hoe meent de regering dit op te lossen?

Openbaarmaking van incidenten

De bevoegde autoriteit kan ex artikel 23 incidenten openbaar maken als publieke bewustwording nodig is om incidenten te voorkomen of het publiek te informeren over een gemeld incident. De vitale aanbieder wordt weliswaar geraadpleegd, maar heeft uiteindelijk geen doorslaggevende stem. Welke rechtsbescherming heeft deze vitale aanbieder, zo vragen de leden van de **VVD**-fractie? De vitale aanbieder zal mogelijk bezwaar en beroep kunnen instellen, maar deze hebben geen schorsende werking. (Ten onrechte) openbaarmaking kan voor deze aanbieders echter wel schadelijke gevolgen hebben. Denk alleen al aan de mogelijke reputatie-schade. Welke instrumenten hebben deze aanbieders op het moment dat ze het niet eens zijn met het besluit van een bevoegde autoriteit om een melding openbaar te maken?
En zal de mogelijke openbaarmaking niet drempelverhogend werken voor aanbieders om meldingen bij de bevoegde autoriteiten te doen? Hoe denkt de regering hierover? Welke maatregelen treft zij om het mogelijke negatieve effect van de mogelijke openbaarmaking van een melding op de meldingsbereidheid te mitigeren?

Een actieve openbaarmaking kan een effectieve bijdrage leveren aan bewustwording en verbetering van de bescherming van ICT-systemen. De leden van de **PvdA**-fractie vernemen graag of de regering bereid is om transparantie te bieden over het aantal meldingen, type incidenten, de impact daarvan en de opvolging naar aanleiding van deze meldingen? Zo nee, waarom niet?

Overlap tussen de beveiligingseisen en meldplichten van de AVG en het voorliggende wetsvoorstel

Graag vragen de leden van de fractie van de **PvdA** in het bijzonder aandacht voor de overlap tussen de beveiligingseisen en meldplichten van de AVG en het voorliggende wetsvoorstel. Vanwege de verschillende grondslag (bescherming van persoonsgegevens en bescherming van vitale infrastructuur) is dit niet eenvoudig te voorkomen. Welke rol ziet de regering voor zichzelf in het bevorderen van de samenwerking tussen het CSIRT en Autoriteit Persoonsgegevens in het bijzonder?

Onbekende kwetsbaarheden

Het Nationaal Cyber Security Centrum voorziet de AIVD (en MIVD) in sommige gevallen van informatie over onbekende kwetsbaarheden die door ethische hackers zijn gemeld. De diensten kunnen deze informatie gebruiken om te hacken. Een dergelijke praktijk kan in de weg staan van een veiliger internet en daarmee de positie van het NCSC bemoeilijken. Is

de regering bereid, zo vragen de leden van de **PvdA**-fractie mede namens de leden van de fractie van de **SP**, te bewerkstelligen dat informatie over onbekende kwetsbaarheden die door onderzoekers, ethische hackers of anderen aan het NCSC wordt gemeld, altijd wordt doorgegeven aan de maker van de software waarin de onbekende kwetsbaarheid is gevonden, met uitzondering van die situaties waarin er naar het oordeel van het NCSC sprake is van een belang van nationale veiligheid?

Tot slot

De richtlijn moest uiterlijk op 9 mei 2018 geïmplementeerd zijn. Waarom is die datum niet gehaald, zo vragen de leden van de **PvdA**-fractie. Baart het de regering zorgen dat de Nederlandse invulling van de verplichtingen van netwerk- en informatiebeveiliging, en daarmee de harmonisatie op Unieniveau, langer op zich zal laten wachten dan gewenst is? Zo nee, waarom niet?

Het voorliggende wetsvoorstel is een stap in de richting van het verbeteren van cybersecurity. De leden van de PvdA-fractie vernemen graag van de regering welke additionele stappen zij mogen verwachten. Voorts merken zij op dat het dossier een internationaal karakter heeft. Derhalve lezen zij graag wat de inzet van Nederland is om cybersecurity verder op Europees niveau aan te pakken. Tenslotte constateren zij dat veel digitale dreigingen afkomstig zijn van statelijke actoren buiten Europa of van cybercriminelen die in landen buiten Europa actief zijn. Welke ruimte ziet en benut de regering voor mondiale afspraken ter verbetering van cybersecurity?

De leden van de vaste commissie voor Justitie en Veiligheid zien de reactie van de regering met belangstelling en bij voorkeur voor 7 september 2018 tegemoet.

De voorzitter van de vaste commissie voor Justitie en Veiligheid,
Duthler

De griffier van de vaste commissie voor Justitie en Veiligheid,
Van Dooren