Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2012–2013

Aanhangsel van de Handelingen

Vragen gesteld door de leden der Kamer, met de daarop door de regering gegeven antwoorden

2092

Vragen van de leden **Dijkhoff** en **De Liefde** (beiden VVD) aan de ministers van Veiligheid en Justitie en van Economische Zaken over *het bericht dat de Verenigde Staten kiezen voor het vrijwillig melden van cybersecurity-incidenten* (ingezonden 7 maart 2013).

Antwoord van minister **Opstelten** (Veiligheid en Justitie) mede namens de Minister van Economische Zaken (ontvangen 26 april 2013) Zie ook Aanhangsel Handelingen, vergaderjaar 2012–2013, nr. 1780

Vraag 1
Bent u bekend met het bericht «EU, US go separate ways on cybersecurity»?[1]

Antwoord 1
Ja.

Vraag 2
Hoeveel schade wordt er jaarlijks geleden als gevolg van cybersecurity-incidenten?

Antwoord 2
De schade die jaarlijks in landen wordt geleden als gevolg van cybersecurity incidenten is niet goed vast te stellen omdat de schade bij veel verschillende partijen wordt geleden, niet eenduidig en volledig wordt gemeld, en naast economische schade ook imagoschade behelst.

Vraag 3
Is het waar dat de Verenigde Staten overwegen een regeling te introduceren, of deze al geïntroduceerd hebben, waarin de keuze cybersecurity-incidenten te melden, zoals bijvoorbeeld een lek in de beveiliging van data, aan bedrijven en instellingen wordt overgelaten op vrijwillige basis?

[1] http://www.euractiv.com/specialreport-cybersecurity/eu-us-set-different-approach-cyb-news-518252?utm_source=EurActiv%20Newsletter&utm_campaign=9089d867b1-newsletter_daily_update&utm_medium=email

ah-tk-20122013-2092
ISSN 0921 - 7398
's-Gravenhage 2013

Antwoord 3
Op 12 februari 2013 stelde president Barack Obama een «executive order» vast waarin federale autoriteiten verplicht worden de informatiedeling over cybersecurity dreigingen met private bedrijven die kritieke infrastructuur ondersteunen te verbeteren. Vitale organisaties worden opgeroepen om op vrijwillige basis informatie over incidenten te delen. De uitwerking van de verschillende onderdelen van de «executive order» vindt in de komende maanden plaats.

Vraag 4
Is het waar dat de door de Europese Commissie voorgestelde richtlijn voorziet in een meldplicht van dit soort incidenten? Wat is uw oordeel over dit onderdeel van deze richtlijn?

Antwoord 4
Ja. Voor het standpunt van de regering over dit voorstel verwijs ik u naar het BNC-fiche dat op 15 maart 2013 naar uw Kamer is gezonden (Kamerstukken II 2012/2013, 22 112, nr. 1587).

Vraag 5
Hoe groot is de bereidwilligheid onder bedrijven tot het op vrijwillige basis melden van cybersecurity-incidenten, zoals bijvoorbeeld datalekken? Hoeveel meer incidenten zouden worden gemeld indien er sprake zou zijn van een verplichting?

Antwoord 5
De bereidheid onder organisaties tot het vrijwillig melden van cybersecurity incidenten neemt toe. In 2012 zijn er 364 incidenten gemeld bij het Nationaal Cyber Security Centrum. In 2011 waren dit er nog 236. Het aantal gemelde cybersecurity breaches is echter nog relatief beperkt. Het betreft hier inbreuken op de veiligheid en of integriteit van informatiesystemen die potentieel kunnen leiden tot maatschappelijke ontwrichting. 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 ontwerp-wetgeving 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. In geval van datalekken gaat het om een inbreuk op beveiligingsmaatregelen voor persoonsgegevens, die leidt tot het verlies van persoonsgegevens. Ook voor datalekken geldt dat de bereidheid tot het vrijwillig melden ervan aan de toezichthouder of aan de betrokkene wiens persoonsgegevens het betreft, gering is. Bij het College bescherming persoonsgegevens zijn de afgelopen twee jaar drie datalekken door verantwoordelijken gemeld. De verwachting is dat een wettelijke verplichting het aantal meldingen zal doen toenemen.

Vraag 6
Wat is de invloed van de voorgestelde Amerikaanse regelgeving op de internetveiligheid van Nederlandse burgers, bedrijven en overheid? Leidt dit per saldo ertoe dat hun persoonlijke gegevens minder goed kunnen worden beschermd?

Antwoord 6
Elke maatregel die er op is gericht de bereidheid van organisaties tot het melden van cybersecurity incidenten te vergroten zal in principe bij kunnen dragen aan het verbeteren van de internetveiligheid. Het valt echter niet op voorhand te zeggen wat de gevolgen van de door de Verenigde Staten gemaakte keuzes zullen zijn.

Vraag 7
Deelt u de mening dat het uiteenlopen van deze regelgeving er niet toe zou moeten leiden dat de gegevens van Nederlandse burgers, bedrijven of zelfs staatsgevoelige informatie op straat komt te liggen? Hoe kan dat worden voorkomen?

Antwoord 7
Ik deel uw mening dat het onwenselijk is als gevoelige informatie op straat komt te liggen. In de «executive order» wordt ook specifiek gesteld dat de grondrechten (*privacy en civil liberties*) geborgd moeten worden bij het uitwerken van de maatregelen.

Vraag 8
Wat is de invloed van de voorgestelde regelgeving voor het handelsverkeer tussen de Verenigde Staten en Nederland? Leidt dit ertoe dat er handelsrestricties, al dan niet feitelijk, ontstaan waardoor het intercontinentale handelsverkeer wordt belemmerd?

Antwoord 8
De zowel in de VS als in de EU aangekondigde maatregelen met betrekking tot het melden van cybersecurity-incidenten hebben geen directe betrekking op het intercontinentale handelsverkeer. Het gaat om het al dan niet vrijwillig melden van incidenten vanuit de door de VS en de EU gedeelde noodzaak om tot een hoger niveau van netwerk- en informatiebeveiliging te komen. De meeste bedrijven nemen vanuit oogpunt van bedrijfszekerheid ook zelf al de nodige maatregelen. De eigen verantwoordelijkheid wordt door de in de VS en de EU aangekondigde maatregelen expliciet gemaakt.

Vraag 9
In hoeverre schaadt het uiteenlopen van de regelgeving de belangen van Nederlandse bedrijven? Bestaat hier verschil tussen bedrijven die wel en bedrijven die niet in de Verenigde Staten zijn gevestigd?

Antwoord 9
De manier waarop de maatregelen zijn opgesteld verschilt maar lijkt vanwege het beoogde materiële effect geen wezenlijk verschil te maken voor de positie van in de VS gevestigde Nederlandse bedrijven ten opzichte van de in de EU actief zijnde Nederlandse bedrijven. Niettemin zal het kabinet dit punt meenemen in de komende besprekingen van de ontwerprichtlijn van de EU.

Vraag 10
Welke risico's ziet u voor de Europese ambitie cloud computing te stimuleren nu de regeling van de Verenigde Staten en de Europese Unie zo van elkaar verschillen?

Antwoord 10
Net als de VS heeft ook Europa ambities om *cloud computing* te stimuleren. *Cloud computing* is een relatief nieuwe ontwikkeling die kansen biedt voor efficienter en flexibeler werken. De globalisering van de opslag en het beheer van data, de juridische kaders die gelden en de wijze waarop eigenaar en beheerder van persoonsgegevens hun verantwoordelijkheden kunnen nemen, vraagt ook om om een goede borging van de privacy.
In de op 27 september 2012 gepubliceerde EU Cloud Strategie benoemt de Commissie de economische kansen maar ook de acties die nodig zijn in het kader van dataprotectie en de standaardisatie van privacy-aspecten in internationaal verband. De internationale dialoog over deze aspecten is van belang om zo ook buiten de EU de privacy te beschermen.

Vraag 11
Welke acties gaat u ondernemen naar aanleiding van deze informatie?

Antwoord 11
Het standpunt van de regering over voorstel voor richtlijn COM(2013)48 van de Europese Commissie is in een BNC-fiche naar uw Kamer gezonden op 15 maart 2013 (Kamerstukken II 2012/2013, 22 112, nr. 1587). Tevens bereidt het Ministerie van VenJ ontwerp-wetgeving voor, die zoals eerder gemeld strekt tot de regeling van een meldplicht voor de overheid en private bedrijven in randvoorwaardelijke sectoren van cyberincidenten met een potentieel maatschappelijk ontwrichtende werking. Op grond van de definitieve tekst van de EU richtlijn zal moeten worden bezien of en in welke mate deze nationale (ontwerp) wetgeving hiermee in overeenstemming is.

Hiernaast zal de staatssecretaris van VenJ, samen met de ministers van BZK en EZ, binnenkort een wetsvoorstel tot wijziging van de Wet bescherming persoonsgegevens indienen dat strekt tot invoering van een wettelijke meldplicht voor datalekken. Daarnaast streeft het kabinet nationaal en internationaal naar een adequate balans tussen veiligheid, vrijheid en (economische) groei. In de nieuwe nationale cybersecuritystrategie en in de internationale arena is er aandacht voor deze balans en de genoemde risico's.