Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2009–2010

26 485 Maatschappelijk verantwoord ondernemen

Nr. 72 **BRIEF VAN DE STAATSSECRETARIS VAN ECONOMISCHE ZAKEN**

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 5 oktober 2009

Hierbij stuur ik u het antwoord op de vraag van het lid Van der Vlies (SGP) gesteld tijdens het AO Maatschappelijk Verantwoord Ondernemen van 4 maart jl. (Kamerstuk 26 485, nr. 66) De heer Van der Vlies heeft naar analogie van de wereldwijde ervaringen bij het toezicht op de financiële sector rond de kredietcrisis, de parallel getrokken met de ICT-sector en gevraagd hoe dat toezicht in de internationale dimensie is ontwikkeld en hoe daadkrachtig en effectief dit is ingericht.

De heer Van der Vlies stelt hier een belangrijke alsook een ingewikkelde kwestie aan de orde. De door hem getrokken parallel met de financiële sector herken ik op het punt van de internationale verwevenheid en complexiteit. Via ICT zijn we op mondiale schaal via allerlei systemen aan elkaar gekoppeld. Immers, de inzet van ICT leidt niet alleen tot meer gemak maar ook tot verhoging van de productiviteit en daarmee duurzame economische groei. ICT is vandaag de dag dan ook tot in de haarvaten van onze samenleving doorgedrongen. Dagelijks worden duizenden processen aangestuurd via ICT zonder dat we ons hier altijd goed van bewust zijn.

De kwetsbaarheid van deze processen is sterk toegenomen vanwege deze afhankelijkheid van ICT. Dit vraagt om inzicht in mogelijke risico's zoals uitval van ICT en het misbruik ervan in de vorm van cybercrime. Veiligheid en betrouwbaarheid van ICT, naast een economisch efficiënte markt, is één van de maatschappelijke belangen waaraan de ICT-infrastructuren en diensten voldoende tegemoet moeten komen. Als de veiligheid niet wordt gewaarborgd of we gaan er te lichtvoetig mee om, dan kan dit schade veroorzaken en daarmee een rem plaatsen op innovatie en het toekomstig gebruik van ICT. Ook hier gaat de vergelijking met de financiële sector op: vertrouwen is van groot belang, nationaal én internationaal.
De financiële crisis heeft bevestigd dat inzicht in de onderlinge afhankelijkheden en kwetsbaarheden aan de basis ligt van vertrouwen. Pas als dit helder is kunnen waar nodig maatregelen getroffen worden en is ook effectief toezicht aan de orde. Op dit moment wordt op vele plekken hard

KST135408
0910tkkst26485-72
ISSN 0921 - 7371
Sdu Uitgevers
's-Gravenhage 2009

gewerkt aan het vergroten van dit inzicht en vertrouwen. Ik zal dit in deze brief nader toelichten en dan in het bijzonder ingaan op de internationale dimensie.

Wie is verantwoordelijk/welke acties?

De ontwikkeling van toezicht op veiligheid en betrouwbaarheid van ICT kan niet los gezien worden van de rol van de gebruiker van de openbare diensten uit de ICT-sector. De eerste verantwoordelijkheid voor een veilig en betrouwbaar gebruik van de ICT-voorzieningen ligt immers bij de gebruikers en bedrijven zelf. Echter, niet iedereen is zich (voldoende) bewust is van deze verantwoordelijkheid.
Op dit moment werkt de overheid aan het vergroten van de bewustwording van gebruikers als het gaat om hun afhankelijkheid van ICT-infrastructuur. Op gebruikersniveau is recent het programma Digibewust en Digivaardig van start gegaan. Hier gaat het om het aanzetten van gebruikers, via kennisoverdracht, tot een bewuste manier van omgaan met computers en mobiele telefoons, en dergelijke en tot het daarbij nemen van eigen verantwoordelijkheid. Hierdoor worden gevaren en risico's beperkt en het vertrouwen in digitale middelen vergroot.
Daarnaast draagt de overheid bij aan het vergroten van het inzicht in hoe de afhankelijkheden in vitale infrastructuren liggen. Via programma's als Strategie Nationale Veiligheid en Bescherming Vitale Infrastructuren worden ondermeer de afhankelijkheden van ICT-systemen van de diverse vitale sectoren zoals bankwezen, energie en drinkwatervoorzieningen in kaart gebracht. Over de voortgang ervan bent u via de minister van BZK met o.a. de brieven TK 2008–2009, 29 668, nr. 26, en TK 2007–2008, 30 821, nr. 6 geïnformeerd.

In de benadering van het vraagstuk rond een veilig en vertrouwd ICT-gebruik nemen begrippen als eigen verantwoordelijkheid, publiek-private samenwerking en bewustwording een belangrijke plaats in. Gelet op de dynamiek van ICT-ontwikkelingen en de verwevenheid ervan in onze samenleving, ligt in deze fase regelgeving (nog) niet direct voor de hand. Het gaat nu vooral om samenwerking die kan uitmonden in vormen van zelfregulering.

Die samenwerking wordt ook internationaal gezocht. Voor Nederland met een grote open infrastructuur en een hoge gebruikersdichtheid is het belang van internationale samenwerking op het gebied van bijvoorbeeld internetveiligheid groot. Binnen de internationale gemeenschap wordt internetveiligheid meer en meer als prioriteit erkend en nader vorm gegeven. De uitwerking ervan zal vanwege de complexiteit en verwevenheid wel veel tijd vergen. De verschillen tussen landen in mate van gebruik en niveau van ICT zijn groot. Ook de wijze van benadering van het probleem c.q. de gevolgde aanpak om de betrouwbaarheid van en het vertrouwen in ICT te vergroten, varieert sterk. Juist daarom zet Nederland, wederom lerend van de financiële crisis, zich ook internationaal in op het vergroten van transparantie, inzicht in kwetsbaarheden en inter-afhankelijkheden en het helder maken van eigen verantwoordelijkheden bij gebruikers.

Nederland speelt hierin, ook internationaal, een actieve rol en plaatst onderwerpen als netwerk- en informatiebeveiliging regelmatig op de agenda. Hieronder vindt u een indruk van de mondiale en Europese ontwikkelingen.

Mondiale ontwikkelingen

Mondiaal gezien zijn o.a. de OECD en NAVO actief op het terrein van netwerk- en informatiebeveiliging. Zo heeft de OECD enige tijd terug handreikingen voor informatiebeveiliging en voor de beveiliging van kritische informatie-infrastructuur uitgebracht. Tevens zijn enkele overzichten opgesteld van de diverse nationale aanpakken van netwerk- en informatiebeveiliging en hun voor- en nadelen. De NAVO heeft onlangs het Cyber Defence Centre of Excellence opgericht en wordt het NAVO beleid voor cyber security aangescherpt. Zowel EU als NAVO werken aan een intensievere samenwerking op het gebied van cyber security.

Op mondiaal niveau kan verder worden gewezen op de activiteiten van de International Telecommunications Union (ITU). Op basis van afspraken gemaakt op de VN World Summit on the Information Society (WSIS) in 2005 is de ITU de mondiale organisatie die de coördinerende rol moet vervullen in het scheppen van vertrouwen en veiligheid in het gebruik van ICT. Dit beleid wordt vormgegeven in een zgn. Global Cybersecurity Agenda, dat een raamwerk biedt voor internationale samenwerking met betrekking tot Cybersecurity. Voorbeelden van activiteiten in het kader van de Global Security Agenda zijn het IMPACT (International Multilateral Partnership Against Cyber-Threats) initiatief en het COP (Child Online Protection) initiatief. Recent is door de ITU in samenwerking met de Portugese regering een World Telecommunications Policy Forum georganiseerd, waar door de internationale gemeenschap een zogenoemde Opinion is vastgesteld over gezamenlijke strategieën voor het scheppen van vertrouwen en veiligheid in het gebruik van ICT.

Het – op basis van afspraken voortvloeiende uit de WSIS opgerichte – Internet Governance Forum (IGF) heeft sinds 2006 Cybersecurity aangemerkt als een van de hoogste prioriteiten. Hoewel dit Forum geen bindende afspraken kan maken brengt het alle relevante partijen bijeen (overheden, bedrijven, civil society, academici, parlementariërs) en stimuleert het initiatieven zoals de stop spam alliance en de dynamic coalition met betrekking tot veiligheid voor kinderen.

Op meer operationeel niveau zijn of worden wereldwijd in veel landen de zogenaamde Computer Emergency Response Teams/ Computer Incident Response Teams (CERT's/CIRT's) opgericht om ingeval van opkomende problemen snel en adequaat te kunnen reageren met waarschuwen en waar nodig bijstaan in het treffen van maatregelen. Deze organisaties werken steeds meer op globale schaal samen. In ons land neemt GovCert.NL, de CERT voor de Nederlandse overheid, daar actief in deel.

Ontwikkelingen in de EU

De Europese Commissie heeft zeer recent een mededeling uitgegeven over de bescherming van vitale informatie-infrastructuur. Dat is het deel van de vitale infrastructuur dat ICT omvat. De mededeling bevat o.a. een actieplan om de beveiliging en veerkracht van de vitale informatie-infrastructuren te verbeteren. Voorbeelden van acties zijn het bevorderen van publiekprivate samenwerking op EU niveau, het maken van afspraken over basisvoorzieningen te leveren door nationale CERTs (Computer Emergency Response Teams) en over internationale samenwerking tussen CERTs en het organiseren van telecom/ICT gerelateerde oefeningen op pan-Europees niveau.

Naast bovengenoemde ontwikkelingen is op het terrein van kennis- en informatiedeling het Europees Agentschap voor Netwerk- en Informatiebeveiliging (ENISA) actief. Doel van dit agentschap is om vanuit samen-

werking de veiligheid waaronder de weerbaarheid en daarmee het vertrouwen in onze ICT-voorzieningen op een hoger niveau te krijgen.

De stap naar toezicht?

Bovenstaande ontwikkelingen geven een beeld van de internationale samenwerkingsverbanden die er zijn en die vooral inzetten op bewustwording, informatie-uitwisseling, best practices en soms richtlijnen. Dit vormt ook de basis voor een meer eenduidige en geaccepteerde aanpak om te komen tot een zekere vorm en mate van regulering op een aantal terreinen. Waar nodig kan dit leiden tot wettelijke verankering.

Binnen de Europese Unie is gewerkt aan de herziening van het regelgevend kader inzake elektronische communicatie. Hoewel het kader breder is, bestrijkt het een scala van onderwerpen gerelateerd aan de elektronische communicatiesector. Bedoeling is dat een nieuw onderdeel wordt toegevoegd over de veiligheid en integriteit van de openbare communicatienetwerken en -diensten, hetgeen ik van harte ondersteun. Zo zal, als het kader wordt goedgekeurd, een meldingsplicht voor aanbieders van elektronische communicatienetwerken en -diensten worden geïntroduceerd, volgens welke het verlies van privacygevoelige gegevens moet worden gemeld aan de overheid. Zowel de Europese Commissie als de lidstaten zullen van bevoegdheden worden voorzien om nadere eisen te stellen aan de wijze waarop en de omstandigheden waaronder deze meldingen moeten plaatsvinden. Tenslotte zullen de nationale toezichthouders worden voorzien in de mogelijkheid om audits uit te voeren op de maatregelen die de aanbieders hebben getroffen inzake deze veiligheid en integriteit.

Tot slot

Het vraagstuk met betrekking tot een veilig en betrouwbaar gebruik is complex, dynamisch en kent een sterke internationale dimensie. Daarbij bestaan er grote nationale verschillen in gebruik van ICT en de wijze waarop men het onderwerp benadert. Inzicht in de intersectorale afhankelijkheden en kwetsbaarheden is onontbeerlijk. Op dit punt liggen we in Nederland aardig op koers. Via de weg van bewustwording, kennis- en informatie-uitwisseling, zelfregulering en indien nodig regelgeving kunnen we een balans vinden tussen enerzijds de groeiambities die we met de inzet van ICT willen realiseren en anderzijds de afhankelijkheid en kwetsbaarheden beheersbaar maken. Deze aanpak en de daarbij opgedane ervaringen brengen wij actief in de internationale arena in. De internationale bereidheid tot samenwerking is toegenomen en ik heb er vertrouwen in dat hier indien nodig de basis wordt gelegd voor een passende vorm van toezicht.

De staatssecretaris van Economische Zaken,
F. Heemskerk