Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2007–2008

26 643 Informatie- en communicatietechnologie (ICT)

Nr. 103

BRIEF VAN DE MINISTERS VAN JUSTITIE EN VAN BINNENLANDSE ZAKEN EN KONINKRIJKSRELATIES EN DE STAATSSECRETARIS VAN ECONOMISCHE ZAKEN

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 17 december 2007

Op 16 juli jongstleden zijn u de rapporten Herijking Veiligheidsbeleid ICT aangeboden (Tweede Kamer, vergaderjaar 2006–2007, 26 643, nr. 96). Daarbij is u een nadere agenda toegezegd. Met deze brief wordt u deze agenda aangeboden.
Voorts heeft de Tweede Kamer met de motie Gerkens en Wagner (Tweede Kamer, vergaderjaar 2006–2007, 28 684, nr. 94) gevraagd om versterking van de coördinatie en aansturing: de in deze brief beschreven aanpak kan als een reactie op deze motie worden gezien.

Achtereenvolgens zullen in deze brief aan de orde komen: Aanleiding en reikwijdte, de belangrijkste bevindingen uit het rapport, de inzet van het kabinet en de agenda.

1. Aanleiding en reikwijdte

ICT Veiligheid is een beleidsterrein, waarvoor meerdere departementen een verantwoordelijkheid kennen. Onder ICT veiligheid wordt hier verstaan zowel de continuïteit van de ICT/telecom dienstverlening, de borging van de mogelijkheid om daar veilig gebruik van te maken, als de opsporing en vervolging ingeval deze veiligheid op strafbare wijze is aangetast. Het inzetten van elektronische middelen ten behoeve van veiligheidsmaatregelen wordt *niet* tot de reikwijdte van deze brief gerekend.

Coördinatie vanuit de betrokken departementen richting uitvoerende organisaties en samenleving is belangrijk om samenhang en richting in de aanpak van ICT veiligheid te bevorderen.

De rapporten van het project Herijking ICT Veiligheidsbeleid zijn opgesteld om intern richting te geven aan het verbeteren van de interdepartementale samenwerking tussen Justitie, BZK en EZ op het terrein van het ICT

KST113870
0708tkkst26643-103
ISSN 0921 - 7371
Sdu Uitgevers
's-Gravenhage 2007

veiligheidsbeleid. De departementen hadden behoefte aan meer gezamenlijk inzicht, waar de coördinatie en samenhang in alle activiteiten op dit terrein noodzakelijk en mogelijk is. Deze rapporten zijn niet opgesteld met het oogmerk van externe verspreiding. De status van de rapporten moet in dat licht worden bezien. Inmiddels hebben de drie departementen goede stappen gezet op weg naar structurele borging van de coördinatie en samenhang in al deze activiteiten.

2. Bevindingen van het rapport

In algemene zin heeft het rapport het beeld opgeleverd dat weliswaar alle bekende bedreigingen actief worden bestreden, maar dat daarbij de beschikbare mix aan (beleids)instrumenten niet ten volle wordt benut. Daarnaast bleek een grote behoefte aan meer regie en minder versnippering op dit terrein.

De belangrijkste aanbevelingen uit het rapport zijn:
- groepering van gerelateerde beleidsonderwerpen in arena's en een gezamenlijke agenda op de punten waar de arena's elkaar raken; in de uitwerking van de gezamenlijke agenda zal worden gezorgd voor een betere sturing en een betere samenwerking.
- verbetering van de governance; professionalisering door bewuster andere beleidsinstrumenten mee te wegen en aandacht voor internationale samenwerking.
- zoeken naar en borgen van een goede samenwerking met het bedrijfsleven: effectiviteit van het beleid wordt alleen bereikt als overheid en bedrijfsleven in deze agenda gezamenlijk optrekken.

Het rapport constateert een verdeling in de volgende drie arena's:
- maatschappij ontwrichtende gebeurtenissen,
- niet-maatschappij ontwrichtende gebeurtenissen,
- opsporing en vervolging.

– *Voorkomen van maatschappij ontwrichtende gebeurtenissen*: hier worden vraagstukken omtrent maatschappijontwrichtende risico's en nationale veiligheid behandeld.
  Het betreft gebeurtenissen die ten koste van bijna alles moeten worden voorkomen. Daar treedt de overheid sturend op, opdat de overheid de zekerheid heeft dat partijen doen wat vanuit publiek belang noodzakelijk is. BZK is in deze arena de belangrijkste portefeuillehouder; EZ is op grond van hoofdstuk 14 Telecommunicatiewet (buitengewone omstandigheden) betrokken.
– *Beperken van niet maatschappij ontwrichtende gebeurtenissen*: vraagstukken omtrent risico's waar de maatschappij last van heeft, maar die niet maatschappijontwrichtend zijn. De overheid tracht hier d.m.v. interventies organisaties te beïnvloeden het gewenste gedrag te vertonen. Vanuit haar rol op gebied van duurzaam ondernemen is EZ hier een belangrijke portefeuillehouder. Waar het goed huisvaderschap van de eigen overheidssystemen betreft, is dit BZK als beleidscoördinator binnen de overheid.
– *Opsporen en vervolgen cybercriminelen*: vraagstukken die te maken hebben met opsporing en vervolging van cybercriminelen. Het betreft hier reguliere overheidstaken van het OM, politie en opsporingsdiensten; Justitie is in deze arena de belangrijkste portefeuillehouder.

De drie voorgestelde arena's overlappen elkaar op sommige onderwerpen, daarnaast zijn veel dreigingsbeelden of kwetsbaarheidrisico's niet eenduidig aan één bepaalde arena gebonden. Soms kunnen dreigingen door toename of verandering van kenmerken verschuiven naar een andere arena.

De aanbevelingen uit de rapporten «Herijking ICT Veiligheidsbeleid» zijn als volgt opgepakt:

- interdepartementale afstemming en coördinatie, waartoe ook een geregeld overleg tussen de drie meest betrokken directeuren-generaal wordt gerekend.
- de gezamenlijke agenda, die u in de bijlage aantreft en die gerelateerd is aan de twee grotere beleidsprogramma's: Nationale Veiligheid en Veiligheid begint bij voorkomen.
- het streven naar een goede samenwerking met bedrijfsleven en betrokken sectoren, zoals uit de agenda naar voren komt.

Zo werken de departementen in samenhang aan reeds eerder ingezette maatregelen zoals de diverse pilots binnen de ontwikkelomgeving van de Nationale Infrastructuur Cybercrime (NICC) en de ondersteuning van de vitale sectoren door het Nationaal Adviescentrum Vitale Infrastructuur (NAVI).

3. Inzet van het kabinet

ICT levert een belangrijke bijdrage aan het innovatieve vermogen van de samenleving. Borging van een veilig en vertrouwd gebruik van ICT is derhalve van groot belang.
Kijkend naar de toekomst is het kabinet dan ook van mening dat onze samenleving weerbaar dient te zijn tegen dreigingen: tegen fysieke maar ook tegen digitale dreigingen, zoals ICT-verstoring of cybercrime.
Deze weerbaarheid geldt niet alleen voor burgers en bedrijven maar ook voor de overheid. Daarnaast dient de veiligheidsketen optimaal te functioneren indien een dreiging toch tot een gebeurtenis heeft geleid.

Het kabinetsbeleid krijgt vorm in twee grote beleidsvelden waarbinnen de borging van de veiligheid van ICT en veiligheid een belangrijke rol vervult:

- De strategie Nationale Veiligheid, die zich richt op de bescherming van de samenleving en bevolking op eigen grondgebied tegen interne en externe dreigingen en het project Bescherming Vitale Infrastructuur, gericht op continuïteit van de voor onze samenleving vitale sectoren, inclusief ICT.
- Binnen het project «Veiligheid begint bij Voorkomen» (VbbV, zie Tweede Kamer, vergaderjaar 2007–2008, 28 684, nr. 119) neemt cybercrime een belangrijke plaats in: naast de aangekondigde intensivering van de opsporing en vervolging van cybercrime zijn preventie en onderzoek belangrijk. Het op cybercrime gerichte beleid in deze pijler is met name gericht op het bevorderen van de werkende veiligheidsketen.

Bij beide beleidsvelden speelt de inbreng van bedrijfsleven en consumenten in het kader van preventie, handhaving en toezicht een belangrijke rol.

Het kabinet is van mening dat, gezien het bovenstaande, verder voortgebouwd moet en kan worden op de bevindingen uit het rapport «Herijking ICT en Veiligheid» en dat de beoogde versterking van de samenhang in de inzet van de departementen het beste bereikt wordt door waar mogelijk op deze twee beleidsvelden gezamenlijk op te trekken. Dit wordt mogelijk gemaakt door de gezamenlijke agenda, die in deze brief wordt gepresenteerd.

4. Agenda

Deze agenda zal onlosmakelijk deel uitmaken van deze beleidsvelden, waarover u via de periodieke rapportages geïnformeerd wordt:

- de rapportages in het kader van Nationale Veiligheid en Bescherming Vitale Infrastructuur (over de voortgang van dit laatste onderwerp

wordt u parallel aan deze brief geïnformeerd door de minister van BZK)
- en de rapportage in het kader van het programma «Veiligheid begint bij Voorkomen».

Gelet op deze borging zal *niet* in een zelfstandige rapportagecyclus over deze bijgevoegde agenda worden voorzien.

Voor zover het de continuïteit van de ICT betreft en de weerbaarheid van de sector tegen diverse dreigingen zal de aanpak passen binnen het bredere kader van Nationale Veiligheid en Bescherming Vitale Infrastructuur. Eén van de rode draden in dit verband betreft «ICT als doorsnijdend thema», omdat vrijwel alle (al dan niet vitale) sectoren in belangrijke mate van eigen ICT én openbare netwerken afhankelijk zijn.
Binnen dit kader wordt nauw samengewerkt met het bedrijfsleven, vanwege het feit dat het merendeel van de vitale infrastructuur in beheer is bij private bedrijven. In diverse PPS gelijkende samenwerkingsvormen is het bedrijfsleven betrokken bij de uitwerking en implementatie van de diverse beleidvelden rond ICT veiligheid. Waar nodig zal de samenwerking verder verdiept worden. In de agenda in de bijlage bij deze brief wordt dit nader aangegeven.

Preventie en bestrijding van cybercrime is een belangrijk thema in het programma Veiligheid begint bij Voorkomen, dat de invulling geeft aan de vijfde pijler van het kabinetsbeleid. Cybercrime is een breed begrip en omvat diverse vormen van criminaliteit: diverse vormen van fraude, verspreiding van illegale content, terrorisme, bedreiging, oplichting tot phishing. Elke vorm heeft zijn eigen bijzonderheden en aandachtspunten, dus een effectieve bestrijding van cybercrime vergt een gedifferentieerde aanpak.
Evenals bij andere vormen van criminaliteit begint een effectieve aanpak van cybercrime bij preventie. Hiertoe dienen kennis, kunde en middelen op orde te zijn. Daarnaast is vooral ook een goede samenwerking tussen burger, bedrijfsleven en opsporingsinstanties gewenst. In de voortgangsrapportages over Pijler V zal worden ingegaan op de voortgang van de preventie en bestrijding van cybercrime. Daarnaast zal de opsporing en vervolging van cybercrime geïntensiveerd worden door een betere toerusting van de opsporingsen vervolgingsinstanties.
Het verstevigen van de aanpak en het gezamenlijk optrekken leidt intrinsiek tot een professionaliseringsslag op de diverse onderwerpen en in de benodigde middelen. Er wordt niet ingezet op een apart traject hiervoor, de aandacht voor governance zal onderdeel zijn van de aanpak van de diverse onderwerpen op de agenda en daardoor effectiever zijn.

De gezamenlijke agenda voor ICT veiligheid volgt op de gebieden nationale veiligheid en bescherming vitale infrastructuur de elementen, die in de General Assembly van de Verenigde Naties (30-01-2004: A/RES/58/199) genoemd zijn voor de bescherming van vitale informatie-infrastructuren. Ook voor de opsporing en vervolging kunnen deze elementen tot voorbeeld dienen voor een soortgelijke aanpak (voor zover relevant). In de bijlage[1] wordt ingegaan op lopende en nieuwe activiteiten, die voor de komende periode onderdeel uitmaken van deze agenda.

De minister van Justitie,
E. M. H. Hirsch Ballin

De minister van Binnenlandse Zaken en Koninkrijkrelaties,
G. ter Horst

De staatssecretaris van Economische Zaken,
F. Heemskerk

[1] Ter inzage gelegd bij het Centraal Informatiepunt Tweede Kamer.