Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2010–2011

26 643 Informatie- en communicatietechnologie (ICT)

Nr. 185

BRIEF VAN DE STAATSSECRETARIS VAN VEILIGHEID EN JUSTITIE

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 20 juni 2011

Onze samenleving wordt steeds vaker geconfronteerd met crises die hun oorsprong vinden in dreigingen vanuit de Informatie- en computertechnologie (ICT). In toenemende mate doen zich op dit terrein incidenten voor die de voorbode kunnen zijn van majeure problemen met grote maatschappelijke effecten. In de Nationale Risicobeoordeling is dit type dreiging geïdentificeerd als één met een hoge impact en grote waarschijnlijkheid. Daarom zijn er de afgelopen periode ook verschillende maatregelen genomen om de weerbaarheid op het gebied van ICT-dreiging te versterken zoals de Nationale Cyber Security Strategie en het bijbehorende actieplan[1] en de oefening Cyberstorm III. Deze oefening vond plaats op 29 en 30 september 2010. Hierbij zend ik het evaluatierapport van deze oefening[2] en informeer ik u over de leerpunten en de hieraan gekoppelde acties.

Oefening Cyberstorm III

De oefening is onderdeel van de jaarlijkse oefencyclus van het Nationaal Crisiscentrum waarbij ook interdepartementaal op hoog politiek-bestuurlijk niveau wordt geoefend. Er is aangesloten bij de door de Verenigde Staten georganiseerde oefening Cyberstorm III. ICT is immers mondiaal en houdt zich niet aan landsgrenzen. Dertien van de vijftien landen van het International Watch and Warning Network (IWWN), een gremium op het gebied van ICT-dreigingen, hebben meegedaan.

Deelnemers en scenario

In Nederland oefenden, naast het ministerie van Veiligheid en Justitie, ook de ministeries van Algemene Zaken, Economische Zaken, Landbouw en Innovatie, Binnenlandse Zaken en Koninkrijksrelaties, Buitenlandse Zaken, Defensie, Infrastructuur en Milieu en Sociale Zaken en Werkgelegenheid. Het Nationaal Crisiscentrum, GOVCERT.NL, het Landelijk Operationeel Coördinatiecentrum/Landelijke Operationele Staf, de Nationaal Coördi-

[1] Brief aan Tweede Kamer, Nationale Cybersecuritystrategie, 22 februari 2011, Kamerstuk 26 643, nr. 174.
[2] Ter inzage gelegd bij het Centraal Informatiepunt Tweede Kamer.

kst-26643-185
ISSN 0921 - 7371
's-Gravenhage 2011

nator Terrorismebestrijding en het Team High Tech Crime van het Korps Landelijke Politiediensten waren ook partners in de oefening.

De basis van het scenario was de infectie van miljoenen computers wereldwijd door een geavanceerd computervirus, een zgn. «cyberworm». Hierdoor ontstond de dreiging dat diverse websites van de rijksoverheid massaal werden overvraagd, overheidsgegevens werden vernietigd, vertrouwelijke informatie openbaar werd en ICT-systemen in vitale sectoren uitvielen of dreigden uit te vallen. De gevolgen voor burgers, bedrijfsleven en overheid konden immens zijn.

Oefendoelen van Cyberstorm III

Vooraf werden de volgende oefendoelen geformuleerd:
1. het beoefenen van de nationale crisisbesluitvormingsstructuur met dilemma's behorende bij een grootschalige ICT-crisis;
2. de realisatie van snelle en kwalitatief hoogwaardige informatie-uitwisseling binnen de ICT Response Board (in oprichting);
3. het versterken van de internationale samenwerking (operationele afspraken) bij een ICT crisis.

Leerpunten van en acties volgend uit oefening Cyberstorm III

Oefeningen zijn er om van te leren en dat kan zeker ook naar aanleiding van deze oefening. De evaluatie kent een aantal leerpunten waarop inmiddels ook actie is ondernomen. Ik ga hierna in op de belangrijkste genomen maatregelen.

Crisisbesluitvorming

Uit de oefening is gebleken dat een non-conventionele ICT-crisis veel beleidssectoren raakt en dat er behoefte en noodzaak is aan nationale coördinatie zowel ten aanzien van de informatie-uitwisseling als ten aanzien van de advisering en besluitvorming over dilemma's.

a. In de oefening is een pilot gedraaid met de inzet van een ICT Response Board. Dit is een netwerkstructuur van publieke en private partijen waarin expertise wordt samengebracht over ICT-crises. In tijden van een grootschalige ICT-verstoring zal deze board bijeenkomen om een expert opinion te geven ten behoeve van de crisisbesluitvormings-structuur en aan de deelnemende private partijen. Aan de hand van enkele incidenten uit het scenario is gekeken wat de gewenste aanpak en de inhoudelijk toegevoegde waarde van de ICT Response Board is. De eerste operationalisatie van de ICT Response Board is per 1 juli 2011 gereed. De IRB zal vervolgens stapsgewijs doorontwikkeld worden en per 1 januari 2012 onderdeel uitmaken van het Nationaal Cyber Security Centrum.
b. Voor 1 juli wordt het Nationaal Crisisplan ICT opgeleverd waarin alle specifieke partijen en procedures worden opgenomen die nodig zijn waar het gaat om ICT-crisis. De aanbevelingen uit de deze oefening zijn daarin meegenomen.
c. Gebleken is dat nieuwe dreigingen zoals ICT helemaal vragen om een sectoroverstijgende en bovenregionale of nationale aanpak. Een adequaat instrumentarium met de mogelijkheden om daadwerkelijk regie te voeren bij de vraagstukken waarvoor we staan hoort daarbij. In de zomer zal ik helderheid geven over hoe ik de versterking van de regierol van de rijksoverheid bij (dreigende) crises zie, inclusief thema's zoals de crisiscommunicatie, het optreden van landelijke operationele diensten en de wijze van opschaling. Hierover heb ik u eerder geïnformeerd via de voortgangsbrief Nationale Veiligheid[1].

[1] Brief aan Tweede Kamer, vergaderjaar 2010–2011, 30 821, nr. 12.

d. Het Nationaal Crisis Plan beschrijft de generieke crisisbesluitvormingsstructuur op rijksniveau en wordt deze zomer gepubliceerd. Hierin worden de ervaringen van de oefening meegenomen.
e. De afgelopen periode is er intensief geoefend waaronder drie kleinere oefeningen voor het adviesteam, een dilemmatraining voor de MCCB (Ministeriële Commissie Crisisbeheersing) en op 28 april jl. een extra oefening voor de deelnemers van de MCCB en de ICCB (Interdepartementale Commissie Crisisbeheersing/ DG niveau) en het adviesteam. Ook de komende periode staat er een aantal kleinere en grote oefeningen gepland voor de nationale crisisstructuur.

Informatie-uitwisseling

Bij elke oefening blijkt dat een snelle en adequate informatie-uitwisseling telkens weer als een leerpunt in de samenwerking tussen organisaties en mensen wordt gekenschetst. Zodra er meer sectoren en instanties betrokken zijn kan het belang van het bijeenbrengen en verifiëren van informatie voor het verkrijgen van een juist beeld van de dilemma's die spelen en hoe de maatschappij daarmee omgaat ten behoeve van de besluitvorming niet genoeg benadrukt worden. Ook bij deze oefening blijkt dat hierin nog stappen te zetten zijn. Ik heb er vertrouwen in dat het ingezette traject met het interdepartementale project van netcentrisch werken hierin belangrijke voortgang zal betekenen.

Internationale samenwerking

Ook oefenen met internationale partners is nuttig gebleken. Het is dan ook de inzet van Nederland om de samenwerking binnen het IWWN te intensiveren. Deze inzet is vooral gericht op het verder verbeteren van de processen en procedures voor een snelle informatie-uitwisseling. Bij de uitwisseling van gegevens moet overigens rekening worden gehouden met beveiligingsaspecten dat invloed heeft op de mogelijkheid van snelle uitwisseling van gegevens. Naast de samenwerking binnen de IWWN neemt Nederland ook actief deel aan de oefencyclus van de Europese Unie onder de naam Cyberseurope. Een eerste pan-Europese oefencyclus heeft in november 2010 plaatsgevonden en in 2012 vindt er een tweede plaats.

Tot slot

Zoals in de conclusie van het rapport is verwoord, heeft de oefening Cyberstorm III maar ook de voorbereiding daarop een belangrijke bijdrage geleverd aan de bewustwording van de complexiteit en de veelvormigheid van ICT-crises. Het is een ander soort crisis dan een klassieke ramp zoals het neerstorten van een vliegtuig, een grote brand of een overstroming. In de voortgangsbrief Nationale Veiligheid[1] en in deze Nationale Cyber Security Strategie[2] die u recent van mij heeft ontvangen, wordt eveneens nadrukkelijk gewezen op de ICT-afhankelijkheid van onze samenleving, de kwetsbaarheid die we daarbij hebben en de gevolgen die dit kan hebben voor onze vitale sectoren, maar ook voor het vertrouwen van burgers in de overheid in het algemeen. Het kabinet is van mening dat er regelmatig moet worden getraind en geoefend om vaardigheden te onderhouden en ontwikkeld beleid te toetsen. Het kabinet heeft zelf de daad bij het woord gevoegd en is op 28 april jl. beoefend tijdens de oefening Copy...*paste*. Deze oefening had wederom een ICT-dreiging als scenario en was een vervolg op de oefening Cyberstorm III. Een veilig Nederland begint bij onszelf, goed voorbereid zijn ook.

De staatssecretaris van Veiligheid en Justitie,
F. Teeven

[1] Brief aan Tweede Kamer, vergaderjaar 2010–2011, 30 821, nr. 12.
[2] Brief aan Tweede Kamer, Nationale Cybersecuritystrategie, 15 februari 2011, kenmerk 2011-20000129681.