2070811180

Vragen van de leden Heerts, Heijnen en Smeets (allen PvdA) aan de ministers van Justitie, van Binnenlandse Zaken en Koninkrijksrelaties en van Economische Zaken met betrekking tot cybercrime. (Ingezonden 11 februari 2008)

Vraag 1
Kent u het bericht “Nederland niet bestand tegen cybercrime”? [1)]

Antwoord 1
Ja.

Vraag 2
Is het waar dat driekwart van alle overheidsinstellingen geen enkel noodplan heeft om zich tegen cybercrime te weren? Zo ja, acht u dit wel wenselijk en hoe gaat u dit dan verbeteren? Zo neen, waarom niet?

Antwoord 2
Wij achten het wenselijk dat overheidsinstellingen weerbaar zijn en de eigen continuïteit kunnen waarborgen. Zie verder het antwoord op vraag 1 van de vragen van uw collega Gerkens (SP) aan de ministers van Binnenlandse Zaken en Koninkrijksrelaties over de voorbereiding van de overheid op een cybercrime aanval. (Ingezonden 11 februari 2008).

Vraag 3
Is het waar dat de overheid slechter op cybercrime is voorbereid dan het bedrijfsleven? Zo ja, wat gaat u hieraan doen? Zo neen, waarom niet?

Antwoord 3
Nee, dit is niet het geval. Zie verder het antwoord op vraag 6 van de vragen van uw collega Gerkens (SP) aan de ministers van Binnenlandse Zaken en Koninkrijksrelaties over de voorbereiding van de overheid op digitale aanvallen (Ingezonden 11 februari 2008) en zie het antwoord op uw vraag 4 omtrent de bijdrage van het NICC aan de beveiliging van de overheidsinfrastructuur.

Vraag 4
Draagt het programma Nationale infrastructuur Cybercrime (NICC) ook bij aan de beveiliging van de infrastructuur van de overheid zelf? Zo ja, op welke wijze? Zo neen, waarom niet?

Antwoord 4
Het programma NICC (Nationale Infrastructuur Cybercrime) is een tijdelijk programma, dat tot doel heeft om de aanpak van de preventie en de bestrijding van cybercrime te verbeteren. Het NICC werkt – binnen strikte randvoorwaarden van vertrouwelijkheid - oplossings- en resultaatgericht aan vraagstellingen, die door de partners in de veiligheidsketen (private partijen, waaronder ISP’s e.d.,

OM, politie, OPTA, GOVCERT.NL, Consumentenautoriteit, CBP) worden aangedragen. Deze verzoeken zijn zowel van overheids- als van private zijde afkomstig. Zo is er in overleg met enkele gemeenten een zgn. 'ethische hack' in voorbereiding, waarbij getest wordt hoe het met de veiligheid van gemeentelijke digitale diensten is gesteld. Deze hack zal worden uitgevoerd conform de hierover gemaakte afspraken met de desbetreffende gemeenten, in een veilige en vertrouwde omgeving.

Vraag 5
Hoe verhoudt zich uw conclusie dat het Actieplan Veilig Ondernemen "goed op schema ligt" [2)] en het feit dat in dat kader het project cybercrime reeds is afgerond tot het in bovengenoemd bericht gestelde dat minder dan de helft van de bedrijven noodmaatregelen heeft klaarliggen?

Antwoord 5
Afgerond is het projectdeel cybercrime binnen het Actieplan Veilig Ondernemen. Dit kabinet heeft in zijn Regeerakkoord en beleidsprogramma aan de preventie van cybercrime een vervolg en intensivering gegeven, die onder andere middels het programma NICC tot uitvoering wordt gebracht.
Het NICC maakt momenteel geen deel meer uit van het Actieplan Veilig Ondernemen, maar is onder de gezamenlijke aansturing van EZ, Justitie en BZK gebracht. Dit in het verlengde van de conclusies, die zijn getrokken in het kader van het traject 'Herijking ICT veiligheidsbeleid' (zie Tweede Kamer, vergaderjaar 2007-2008, 26 643, nr. 103), waarin het belang van coördinatie en samenhang werd benadrukt in het tegengaan van cybercrime. Deze aanpak van 'werkende weg ontwikkelen van oplossingen' wordt door de deelnemers als bijzonder effectief ervaren. Partijen in de veiligheidsketen kunnen de samenwerking rond concrete vraagstellingen oppakken en weten zich daarbij ondersteund door het NICC.

Vraag 6
Hoe oordeelt u over gestelde in bovengenoemd onderzoek dat slechts een kleine groep van de bedrijven die een cybercrime aanval te verduren heeft gehad hiervan aangifte doet bij politie of Justitie?

Antwoord 6
Zie mijn antwoord op vraag 3 van uw collega Gerkens (SP) over de aangiftebereidheid van ondervraagden en over hun vertrouwen in de bestrijding van cybercrime door de politie.

Vraag 7
Hoe oordeelt u over het gestelde dat 83 procent van de respondenten in dit verband zegt weinig of geen vertrouwen te hebben in politie en Justitie? Past dit beeld bij uw stelling dat de bestrijding van cybercrime een "normaal onderdeel" van de dagelijkse werkzaamheden van het Openbaar Ministerie en de politie moet worden? [3)]

Antwoord 7
Zie mijn antwoord op vraag 3 van uw collega Gerkens (SP) over de aangiftebereidheid van ondervraagden en over hun vertrouwen in de bestrijding van cybercrime door de politie.

Vraag 8
Hoe en op welke termijn zullen de maatregelen tegen cybercrime, die in het plan "Veiligheid begint bij Voorkomen" aangekondigd zijn, bijdragen aan de verbetering van de bescherming tegen cybercrime?

Antwoord 8
De maatregelen die in het kader van het "Veiligheid begint bij voorkomen" genomen worden aangaande de opsporing en vervolging maken deel uit van een meerjarig programma dat loopt van 2008 tot en met 2012. De Nota "Rechtshandhaving op internet" waarin dit programma is vervat, zal nog dit voorjaar naar de Tweede Kamer worden gezonden. De komende jaren zullen er naar verwachting stap voor stap concrete verbeteringen zichtbaar worden, zoals het verbeteren van de aangiftemogelijkheden van cybercrime en ook het aantal cybercrime zaken dat in behandeling wordt genomen en dat tot vervolging en veroordeling komt.

Toelichting:
Deze vragen dienen ter aanvulling op eerdere vragen ter zake van het lid Gerkens (SP), ingezonden 11 februari 2008, vraagnummer 2070811120.

1) http://www.ey.nl/?pag=788&nieuws_id=3175
2) "Veiligheid begin bij Voorkomen, 28684, nr. 119, p.)
3) "Veiligheid begin bij Voorkomen, 28684, nr. 119, p. 19