**2070811120**

Vragen van het lid Gerkens (SP) aan de ministers van Binnenlandse Zaken en Koninkrijksrelaties en van Justitie over de voorbereiding van de overheid op een cybercrime aanval. (Ingezonden 11 februari 2008)

**Vraag 1**
Wat is uw mening over de uitkomsten van de ICT barometer, waaruit blijkt dat driekwart van de overheid geen maatregelen heeft getroffen om cybercrime te verminderen en de helft geen noodplan heeft? [1)]

**Antwoord 1**
Het probleem van cybercrime wordt naar onze zin nog te weinig onderkend.
Het kabinet is van mening dat de overheid een voorbeeldfunctie heeft als het gaat om veilig en betrouwbaar omgaan met informatie. Het kan hier gaan om een verantwoordelijkheid van het Rijk, van specifieke diensten of van mede-overheden.
Op grond van het Voorschrift Informatiebeveiliging Rijksdienst (VIR 2007) zijn overheidsorganisaties binnen de rijksdienst verplicht tot een risicoafweging.
Op basis van deze afweging nemen organisaties onder eigen verantwoordelijkheid voor hun systemen passende maatregelen. Een noodplan kan, maar hoeft hier geen onderdeel van uit te maken. Jaarlijks worden de departementen en de uitvoerende diensten geaudit naar opzet, bestaan en werking van de maatregelen. Daarnaast maken beveiligingsafspraken en incidentrespons onderdeel uit van de overeenkomsten met ICT-dienstverleners.
Het Rijk kan niet in de bevoegdheden van mede-overheden treden, maar bevordert het risicobewustzijn via GOVCERT.NL[1] en het programma Nationale Infrastructuur Cybercrime (NICC).

**Vraag 2**
Hoe oordeelt u over de uitspraak van de onderzoeker dat de noodklok geluid wordt, omdat Nederland kwetsbaar zou zijn voor een digitale terroristische aanslag? Hoe rijmt u deze uitspraak met uw antwoorden op eerdere Kamervragen over de bestrijding van cybercriminaliteit en een mogelijke digitale aanslag in Almere? [2)]

**Antwoord 2**
Wij zien geen reden tot het luiden van de noodklok. Cyberaanvallen door terroristen tegen het internet en via het internet tegen andere doelwitten, zoals vitale sectoren, zijn weliswaar voorstelbaar, maar niet erg waarschijnlijk, zoals ik u indertijd reeds heb gemeld. De argumentatie hiervoor, zoals vermeld in het begin 2007 uitgebrachte rapport van de NCTb met als titel ‘Jihadisten en het internet’[2], blijft van kracht.
De kans op grootschalige verstoring van netwerken is overigens minimaal, door technische redundantie, diversiteit en overcapaciteit. In Nederland zijn een vijftiental grotere Internet Service Providers actief en daarnaast enkele honderden meer gespecialiseerde kleinere. Deze providers hebben allen maatregelen genomen om de integriteit van hun netwerk in stand te houden en denial-of-service attacks tegen te gaan.

---

1 het Computer Emergency Response Team van en voor de Nederlandse overheid
2 TK 2006-2007, 29 754 nr. 95

Dit laat onverlet, dat de afhankelijkheid van onze samenleving van ICT toeneemt. Ook het bedrijfsleven in de vitale infrastructuur erkent deze afhankelijkheid en heeft ICT benoemd als het belangrijkste thema voor 2008, waarbij ook gekeken wordt naar onderlinge afhankelijkheden. Binnen het programma Nationale Veiligheid en het project Bescherming Vitale Infrastructuur wordt dit thema in publiek-private samenwerking opgepakt en volgt er in 2008 een integrale analyse en risico-beoordeling, zoals toegezegd in het AO Nationale Veiligheid van 31 oktober 2007.

**Vraag 3**
Wat is uw oordeel over het feit dat maar 6% van de ondervraagden aangifte heeft gedaan van cybercrime bij de politie, 11% wegens te weinig vertrouwen en 9% wegens onduidelijkheid over de plaats waar aangifte kan worden gedaan? Wat is uw oordeel over het feit dat 71% van de ondervraagden geen vertrouwen heeft in de bestrijding van cybercrime door de politie? Kunt u uw antwoord toelichten?

**Antwoord 3**
Het feit dat slechts 6% van de ondervraagden aangifte heeft gedaan bij de politie, is betreurenswaardig. Indien 11% van de respondenten te weinig vertrouwen heeft en 9% geen aangifte doet vanwege de onduidelijkheid over de plaats van aangifte betekent dit dat de meeste respondenten een andere reden hebben om geen aangifte te doen. Het is mij bekend dat het bedrijfsleven terughoudend is met het doen van aangifte van cybercrime uit angst voor reputatieschade.
Ik betreur het dat 71% van de respondenten geen vertrouwen heeft in de bestrijding van cybercrime door de politie. Dit was dan ook één van de redenen om in deze kabinetsperiode binnen het programma “Veiligheid begint bij voorkomen” meer aandacht te besteden aan de bestrijding van minder zichtbare vormen van criminaliteit, zoals cybercrime. In dit kader zijn aan zowel de politie als het OM extra middelen toegewezen ter verbetering van de aanpak van cybercrime.
Tot de voorgenomen verbeteringen bij zowel de politie als het OM behoort onder andere het aanstellen van extra personeel, alsmede het vergroten van kennis en deskundigheid bij zowel het bestaande als het nieuw aan te stellen personeel. De concrete invulling hiervan wordt thans vormgegeven. Daarnaast zal door de politie worden onderzocht in hoeverre het mogelijk is om het doen van aangifte via internet van internetgerelateerde criminaliteit te realiseren.

**Vraag 4**
Hoe staat het met het Landelijk Project Digitaal Opsporen, dat in 2005 is gestart? [3)]
Hoeveel van de 2000 rechercheurs, die getraind zouden worden in vier jaar tijd, zijn er inmiddels opgeleid? Acht u dit aantal voldoende? Zo ja, waarom? Zo neen, wat gaat u doen om meer rechercheurs op te leiden?

**Antwoord 4**
Het project Digitaal Opsporen is beëindigd. Inmiddels hebben zo’n 1050 rechercheurs deelgenomen aan de opleiding digitaal opsporen. In 2008 zullen er nog eens circa 500 worden opgeleid. Een van de onderdelen uit het programma “Veiligheid begint bij voorkomen” is de intensivering van de aanpak van cybercrime. In het kader van deze intensivering zal de opleidingsinspanning worden gecontinueerd en zullen nog meer rechercheurs een training digitale opsporing gaan volgen.

**Vraag 5**

Deelt u de mening dat sinds het High Tech Crime Centre is opgedoekt de bestrijding van cybercrime niet meer van de grond is gekomen? Zo ja, welke maatregelen gaat u treffen om cybercrime te bestrijden en voorkomen? Zo neen, waarom niet?

**Antwoord 5**
Ik deel deze mening niet. Het NHTCC was een project, dat is voortgezet in de vorm van een unit High Tech Crime bij het KLPD. De capaciteit van het NHTCC bedroeg destijds 11 fte en is waar mogelijk overgegaan. Inmiddels zijn er 28 fte actief bij deze unit. Deze unit richt zich op vormen van cybercrime die niet door de regio of Bovenregionale Recherche opgepakt kunnen worden. Dit kan zijn doordat de opsporingsonderzoeken bijzondere ICT-kennis vergen of internationale componenten bevatten.
Overigens verwijs ik u naar de kabinetsbrief over Veiligheid begint bij voorkomen voor de maatregelen die het kabinet treft voor de bestrijding van cybercrime.

**Vraag 6**
Wat gaat u doen om ervoor te zorgen dat overheden maatregelen treffen tegen (het voorkomen van) digitale aanvallen?

**Antwoord 6**
De overheid treft al maatregelen ter voorkoming van digitale aanvallen.
(zie ook de beantwoording op vraag 1). Alle kerndepartementen en daarnaast nog vele andere – aan de overheid gelieerde – organisaties zijn aangesloten bij GOVCERT.NL, het Computer Emergency Response Team van en voor de Nederlandse overheid. GOVCERT.NL biedt overheidsorganisaties ondersteuning bij het voorkomen, detecteren, analyseren en oplossen van ICT incidenten.
Daarnaast heeft GOVCERT.NL een monitoringsysteem ontwikkeld, dat externe dreigingen voor netwerken van de overheid in kaart brengt en bijdraagt tot de bescherming van deze netwerken.
De overheid doet ook veel ter voorkoming van schade door digitale aanvallen.
Bij de omgang met persoonsgegevens wordt de Wet bescherming persoonsgegevens gevolgd, die normen stelt voor een behoorlijke en zorgvuldige verwerking.
Een belangrijk element daarbij is dat passende technische en organisatorische maatregelen worden getroffen om persoonsgegevens te beveiligen tegen verlies of enige vorm van onrechtmatige verwerking. Ervaringen worden verwerkt in een samenhangend pakket van beveiligingsmaatregelen die door de departementen en uitvoerende diensten zelf worden getroffen en onderhouden.

1) 6 februari 2008,
http://www.nu.nl/news/1424008/50/%27Driekwart_overheid_geen_plan_tegen_cybercriminaliteit%27.html
2) Aanhangsel Handelingen 2007-2008, nr. 895, zie antwoord op 2
3) Aanhangsel Handelingen 2007-2008, nr. 1501