Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2005–2006

26 671 Wijziging van het Wetboek van Strafrecht, het Wetboek van Strafvordering en enige andere wetten in verband met nieuwe ontwikkelingen in de informatietechnologie (computercriminaliteit II)

Nr. 24 **BRIEF VAN DE STAATSSECRETARIS VAN ECONOMISCHE ZAKEN**

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 18 mei 2006

Op 19 december 2005 is een brief gestuurd aan de Tweede Kamer over de aanpak van cybercrime. Op 20 december 2005 is de brief toegelicht in een Algemeen Overleg. In de brief en tijdens het AO is aangegeven u aan het eind van het eerste kwartaal van 2006 te informeren over het eindadvies van het *project National High Tech Crime Center (NHTCC)* en het *NPC-project Aanpak Cybercrime (NPAC)*.[1]

Met deze brief bied ik u het eindadvies aan.[2] De verantwoordingsrapportage van het project NHTCC is als bijlage bij het advies toegevoegd. Ik wil u met deze brief informeren over het standpunt dat ik mede namens de bewindslieden van Justitie, Binnenlandse Zaken en Koninkrijksrelaties en de Minister voor Bestuurlijke Vernieuwing en Koninkrijksrelaties over het advies inneem.

Aanleiding advies

In 2004 zijn twee projecten van start gegaan gericht op versterking van de aanpak van cybercrime.
- *Het project NHTCC.* Dit project concentreert zich primair op het vormgeven van de proactieve taak van de overheid en meer specifiek van de politie, op het gebied van de bestrijding van ICT-criminaliteit.
- *Het NPAC.* Dit project richt zich met name op de niet-strafrechtelijke bestrijding van cybercrime. Dit gebeurt door het versterken van de informatie-uitwisseling, samenwerking en coördinatie tussen publieke en private partijen.

Vanwege de samenhang tussen beide projecten, zijn vanaf het voorjaar van 2005 de projectactiviteiten op elkaar afgestemd wat heeft geresulteerd in een gezamenlijk eindadvies.

Samenvatting eindadvies

Kort samengevat wordt in het advies het volgende voorgesteld:
- Ontwikkel een Nationale Infrastructuur voor de bestrijding van cyber-

[1] Kamerstukken 26 671, nr. 21 en nr. 22.
[2] Ter inzage gelegd bij het Centraal Informatiepunt Tweede Kamer.

KST97660
0506tkkst26671-24
ISSN 0921 - 7371
Sdu Uitgevers
's-Gravenhage 2006

crime. Deze infrastructuur moet ervoor zorgen dat er meer samenhang komt in de bestrijding van cybercrime. Een professionele aanpak van publieke en private partijen en een gedegen kennisuitwisseling moet een effectievere aanpak en bestrijding realiseren.
– Richt in aanvulling op regionale en bovenregionale inzet ten aanzien van de opsporing van cybercrime ook op nationaal niveau een voorziening in. Deze nationale voorziening werkt samen met de ketenpartners op het gebied van bestrijding van cybercrime (zowel bij de overheid als in het bedrijfsleven).

Deze twee componenten zijn hieronder verder uitgewerkt. Eerst zal ik toelichten welke definitie van cybercrime is gehanteerd.

Wat is cybercrime?

In het advies is gekozen voor een indeling in vier verschijningsvormen van cybercrime die bij elkaar opgeteld het totale terrein bestrijken van wat men onder cybercrime kan verstaan.

1. Illegale communicatie. In deze variant bedienen criminelen zich van publieke netwerken voor onderlinge communicatie voor het uitwisselen van strafbare zaken, zoals bijvoorbeeld kinderporno. Het netwerk als infrastructuur op zich, leidt door deze vorm van communicatie geen schade.
2. Inbreuk op de integriteit van gegevensbeheer. Het netwerk wordt gebruikt om ergens binnen te komen voor het moedwillig beschadigen van gegevens of voor het stelen van gegevens. Het fysieke netwerk als zodanig wordt niet beschadigd en blijft intact.
3. Beschadiging van het netwerk. Niet gegevens op het netwerk zijn het eerste doelwit, maar het netwerk of aangesloten apparatuur zelf. Waardoor die apparatuur bijvoorbeeld niet meer werkt, of werkt volgens de specificaties van degene die inbreuk maakt, zoals in het geval van botnets[1].
4. Legale communicatie voor illegale doeleinden,
waarbij men zich net als in variant 1 als misdadigers bedient van publieke netwerken voor onderlinge communicatie maar het type van de communicatie verschilt. Bellen via internet, mailen en chatten maar ook het doen van financiële transacties valt onder regulier gebruik, of dat nu door een crimineel of een niet-crimineel plaatsvindt. Kenmerk van regulier gebruik is dat het gebruik van het netwerk op zich zichzelf genomen niet illegaal is.

De laatste variant raakt slechts zijdelings aan het onderwerp. De nadruk ligt op de bestrijding van cybercrime gericht op publieke elektronische netwerken en de daarop aangesloten apparatuur. Dit laat onverlet het belang van strafrechtelijke aanpak van incidenten met betrekking tot bedrijfsinterne netwerken die niet in verbinding staan met de buitenwereld. Dit vanwege het grote belang om vitale ICT-infrastructuren te beschermen tegen inbreuken van buiten, ongeacht of het om fysieke of virtuele inbreuken gaat en of het een openbare of een bedrijfsinterne netwerkinfrastructuur betreft.

Reactie op het eindadvies

Ik onderschrijf het centrale betoog dat een effectieve aanpak van cybercrime er op gericht moet zijn om de kwetsbaarheid van overheid en bedrijfsleven voor cybercrime te verminderen door publieke en private partijen gezamenlijk te laten werken aan het voorkomen, stoppen en zo mogelijk herstellen van schade als gevolg van cybercrime.

In lijn met het advies is door de betrokken bewindslieden gekozen voor:
1. Het ontwikkelen van een Nationale Infrastructuur voor de bestrijding van cybercrime.

[1] Het woord «bot» komt van robot. Een bot is een programma dat zelfstandig «geautomatiseerd werk» kan uitvoeren. Een bot kan heel onschuldig zijn, zoals zoekmachines bots gebruiken om websites in kaart te brengen. Maar een bot wordt echter ook gebruikt om andere, meer kwaadaardige handelingen te kunnen uitvoeren op computers. Zo kan een bot creditcard- of bankgegevens onderscheppen. Bij een botnet is sprake van een (vaak) grootschalig en wereldwijd botnetwerk van geïnfecteerde pc's. Een persoon kan een botnet vanuit een centraal punt op het internet besturen.

2. Het versterken van de samenhang tussen de lokale, regionale, bovenregionale en nationale aanpak van de opsporing en vervolging van cybercrime. Inzet is daarom de organisatie van de aanpak van cybercrime door de politie onderdeel te maken van de prestatieafspraken tussen de politie, Ministers en de politiekorpsen die de komende maanden gemaakt gaan worden voor de jaren 2007 en 2008. De inrichting bij het KLPD van een nationale voorziening voor de opsporing zal daarvan deel gaan uitmaken. Conform een eerdere toezegging aan uw Kamer zult u over die prestatieafspraken worden geïnformeerd.

In deze aanpak ligt de nadruk op het verder versterken van de onderlinge samenwerking tussen partijen betrokken bij de aanpak van cybercrime[1] om effectiever op te kunnen treden. Daarbij zal zoveel mogelijk gebruik wordt gemaakt van bestaande organisaties.

1 De Nationale Infrastructuur Bestrijding Cybercrime

Op verschillende plekken zowel bij de overheid als het bedrijfsleven wordt aan de aanpak van cybercrime gewerkt. Uit het advies blijkt dat op onderdelen nog witte vlekken worden ervaren.[2]
Bovendien wordt gewezen op de noodzaak van betere informatie-uitwisseling. Daarom is voorgesteld een Nationale Infrastructuur te ontwikkelen met het oog op het verbeteren van de (bestuurlijke) samenhang, het invullen van de witte vlekken en anderzijds het professionaliseren van de informatie-uitwisseling. Deze Nationale Infrastructuur laat zich het best omschrijven als een virtuele ringleiding tussen publieke en private organisaties die betrokken zijn bij de aanpak van cybercrime.

Het gaat bij de aanpak van cybercrime om een scala aan taken. Van voorlichting en *trendwatching* tot het daadwerkelijk opsporen en vervolgen. De uitvoering van die verschillende taken is op dit moment te gefragmenteerd. Er kan meer en beter worden samengewerkt. De Nationale Infrastructuur beoogt die samenwerking vorm te geven in nauw overleg met de organisaties die betrokken zijn bij de aanpak van cybercrime. Met behulp van o.m. een aantal experimenten, waarover in de volgende paragraaf meer, ontstaat inzicht in de manier waarop de Nationale Infrastructuur het beste kan functioneren. Ook zal worden bekeken in welke mate taken van bestaande organisaties moeten worden uitgebreid of overgeheveld.

Experimenten

Om beter zicht op de aard en omvang van cybercrime te krijgen wordt conform het eindadvies een aantal experimenten uitgevoerd als onderdeel van een breder implementatieprogramma. De kern wordt gevormd door een viertal experimenten gericht op respectievelijk de bancaire sector, het MKB, de decentrale overheid en de grote industrie. De resultaten van de experimenten vormen input voor de implementatie van de Nationale Infrastructuur.

Een eerste experiment is al gestart. GOVCERT heeft samen met de bancaire sector een experiment opgezet dat erop is gericht om via het internationale netwerk van GOVCERT meldingen door banken over phishing-sites, die vrijwel altijd niet in Nederland worden gehost, door te geven aan publieke en private counterparts van GOVCERT in het buitenland. Op basis van dit experiment dat eindigt in september 2006 zal in kaart worden gebracht of en in welke vorm een vergelijkbare voorziening gerealiseerd kan worden waarbij de focus verbreed wordt naar andere sectoren.

[1] Zoals GOVCERT.NL (het computer emergency response team van de overheid), de politie, het Nationaal Meldpunt Cybercriminaliteit, OPTA, Internet Service Providers.
[2] Dit speelt met name rond de pro-actie, de preparatie, de signalering (het melden en het doen van aangifte), de opsporing en vervolging (opvolging), en de terugkoppeling naar aangevers.

In de eerste twee maanden sinds de start van het experiment zijn door Nederlandse Banken zeven meldingen gedaan. Het betrof phishing-sites die in het buitenland gehost werden. In zes gevallen is het gelukt om de betreffende site uit de lucht te krijgen. Eén geval is een nog lopende actie. De doorlooptijd bij het uit de lucht halen van de sites varieerde van één tot veertien dagen.

Een tweede experiment rond het midden- en kleinbedrijf start in april 2006. In samenwerking met de MKB-Nederland, het regionaal platform criminaliteitsbeheersing Flevoland en KvK Flevoland zal bij een vijftigtal bedrijven een ICT-scan worden uitgevoerd en onderzoek worden gedaan naar aard en omvang van cybercrime bij het midden- en kleinbedrijf. Doel van het experiment is om beter inzicht te krijgen in de specifieke problematiek en vragen bij het middenen kleinbedrijf over cybercrime. De uitkomsten (oktober 2006) worden meegenomen in de implementatie van de Nationale Infrastructuur.

De voorbereidingen voor het derde en vierde experiment zullen voor de zomer zijn afgerond.

2 Organisatie van de opsporing en vervolging

Zoals hierboven is aangegeven is in het rapport voorgesteld de opsporing en vervolging wel onderdeel te maken van Nationale Infrastructuur, maar de opsporingscapaciteit apart vorm te geven.

Uit de ervaringen die door het project NHTCC zijn opgedaan, blijkt dat de relatief veelvoorkomende vormen van cybercrime, zoals oplichting via veilingsites, door de regiokorpsen opgepakt kunnen worden. Met name op nationaal niveau, kan de opsporing en vervolging nog een impuls gebruiken. Daarom wordt een nationale voorziening bij het KLPD gebouwd. Aangezien het precieze zicht op aard en omvang van cybercrime nog niet volledig is, wordt deze impuls voor drie jaar gegeven. Na drie jaar moet in het Nationaal Dreigingsbeeld ook voor cybercrime een goed beeld geschetst kunnen worden. Op basis van dat beeld en de dan opgedane ervaring kan definitieve besluitvorming plaatsvinden.

De nationale voorziening bij het KLPD zal zich richten op bijzondere vormen van cybercrime die kunnen worden gekwalificeerd als vormen van zware, georganiseerde misdaad. Ook kan het gaan om innovatieve vormen van cybercrime of incidenten met een belangrijke internationale component. Gekozen is om deze capaciteit bij de Dienst Nationale Recherche onder te brengen. Dit betekent dat de kennis en ervaring die is opgedaan door de medewerkers van het huidige project NHTCC zoveel mogelijk daarin instroomt. De nationale voorziening bij het KLPD zal de volgende taken gaan vervullen:

– Het verrichten van opsporingsonderzoeken naar cybercrime.
– Het ontwikkelen en uitvoeren van strategieën op het gebied van tegenhouden van cybercrime.
– Het benutten, opbouwen en uitdragen van expertise.
– Het vergaren en uitwisselen van informatie.

Momenteel wordt er door het KLPD en OM gewerkt aan voorstellen voor de inrichting.

Het Nationaal Meldpunt Cybercrime

Het Nationaal Meldpunt Cybercrime is per 1 maart operationeel voor meldingen betreffende haatzaaiende en terroristische uitingen op het internet. Sinds 31 maart kan de burger er ook terecht voor meldingen inzake kinderporno. Gelet op deze twee taken van het meldpunt is het tijdelijk bij het KLPD ondergebracht. Later worden de taken van het meldpunt uitgebreid met andere vormen van cybercrime. Zo is het onder meer nodig een meldpuntfunctie te ontwikkelen voor het bedrijfsleven. Later volgt een besluit waar het beheer van het meldpunt definitief wordt ondergebracht.

Besturing en planning

Het implementatieprogramma om de Nationale Infrastructuur valt onder de vlag van het Nationaal Platform Criminaliteitsbeheersing (NPC). De voorgestelde aanpak kan op een breed draagvlak rekenen van de Raad van Advies van het NPC. Naast o.m. de voorzitters van o.a. MKB-NL, VNO-NCW, de NVB en het Verbond van Verzekeraars zijn in het NPC de Ministers van Justitie, Binnenlandse Zaken en Koninkrijksrelaties en de Staatssecretaris van Economische Zaken vertegenwoordigd. De laatste zal als opdrachtgever voor het programma optreden in nauwe samenwerking met betrokken departementen.

Het programma zal naar verwachting twee jaar duren. Vanaf de start van het programma wordt gewerkt volgens een model waarbij ontwikkeling (bijv. de experimenten) en implementatie (inventariseren en borgen van structurele taken) parallel lopen. Na afloop van het programma is de Nationale Infrastructuur volledig operationeel. De Nationale Infrastructuur zal tijdens het programma geleidelijk vorm krijgen, hiermee wordt niet gewacht tot het einde van het programma. Het karakter van het programma laat zich kenschetsen als een proces van *trial-and-error*, waarbij met name aan de hand van de resultaten van experimenten zal worden beoordeeld welke consequenties die hebben voor de inrichting van de Nationale Infrastructuur.

Conclusie

Cybercrime is een fenomeen dat zich kenmerkt door snelle technologische veranderingen en een sterke internationale dimensie. De aanpak ervan is belangrijk want steeds meer burgers, bedrijven en overheden krijgen ermee te maken. Tegelijkertijd ontbreekt een precies inzicht in aard en omvang van het probleem. Toch is er geen sprake van een *greenfield-situatie*. De afgelopen jaren zijn op verschillende fronten belangrijke stappen gezet met de aanpak van cybercrime; onder andere via bewustwordingsactiviteiten, internationale samenwerking, en met wetgeving. De nu gekozen programmatische aanpak is een aanzienlijke extra investering in de bestrijding van cybercrime. Niet alleen door de overheid, maar ook door het bedrijfsleven. Het feit dat dit voorstel op breed draagvlak kan rekenen binnen het NPC effent de weg om gezamenlijk te gaan werken aan het aanbrengen van de gewenste samenhang tussen publieke en private organisaties die bij de bestijding van cybercrime zijn betrokken. Met de nationale voorziening bij het KLPD ontstaat bovendien een aanvullend instrument voor effectieve opsporing en vervolging.

Het bijgaande rapport gaat in meer detail in op de probleemstelling rond cybercrime, de varianten voor een effectieve aanpak en de activiteiten die in het programma zullen worden verricht.

Tot slot. Ik ben van mening dat met de geschetste activiteiten een aantal belangrijke randvoorwaarden is ingevuld en dat we daarmee goed zijn toegerust voor een succesvolle aanpak van cybercrime.

De Staatssecretaris van Economische Zaken,
C. E. G. van Gennip