EUROPESE COMMISSIE

Brussel, 30.9.2010
SEC(2010) 1123 definitief

WERKDOCUMENT VAN DE DIENSTEN VAN DE COMMISSIE

SAMENVATTING VAN DE EFFECTBEOORDELING

Begeleidend document bij het

voorstel voor een

RICHTLIJN VAN HET EUROPEES PARLEMENT EN DE RAAD

over aanvallen op informatiesystemen en tot intrekking van Kaderbesluit 2005/222/JBZ van de Raad

{COM(2010) 517 final}
{SEC(2010) 1122 final}

SAMENVATTING VAN DE EFFECTBEOORDELING

1. OMSCHRIJVING VAN HET PROBLEEM

Het aantal aanvallen op informatiesystemen is sinds de goedkeuring van het kaderbesluit over aanvallen op informatiesystemen (hierna "kaderbesluit aanvallen" genoemd) fors toegenomen. Volgens een toonaangevend bedrijf op het gebied van internetbeveiliging is het aantal bedreigingen van vertrouwelijke informatie (tegenover openbaar beschikbare informatie) in 2008 aanzienlijk toegenomen; het aantal nieuwe bedreigingen dat werd geregistreerd steeg dat jaar van 624 267 tot 1 656 227[1]. Bovendien is een aantal aanvallen van ongekend grote en gevaarlijke schaal waargenomen, zoals die in Estland (2007) en Litouwen (2008). In maart 2009 werden er in 103 landen computersystemen van overheids- en particuliere organisaties aangevallen door een netwerk van besmette computers, waarbij gevoelige en gerubriceerde documenten werden buitgemaakt[2]. Hiertoe werd gebruikgemaakt van "botnets"[3], netwerken van besmette computers, die op afstand bestuurbaar zijn. Ten slotte verspreidt zich momenteel een botnet genaamd "Conficker" (ook bekend als Downup, Downadup en Kido). De groei en activiteit van dit netwerk zijn qua schaal en omvang ongekend: sinds november 2008 zijn wereldwijd al miljoenen computers aangetast[4].

Ten tweede is het moeilijk om op gecoördineerde en doeltreffende wijze op deze aanvallen te reageren, doordat de lidstaten, en met name de rechtshandhavingsinstanties en justitiële autoriteiten binnen de EU, onvoldoende samenwerken. Hoewel uit het uitvoeringsverslag over het kaderbesluit aanvallen blijkt dat de meeste lidstaten overeenkomstig artikel 11 van het kaderbesluit aanvallen permanente meldpunten hebben ingesteld, zijn er nog steeds problemen wat betreft hun alertheid en vermogen om te reageren op dringende verzoeken om samenwerking[5].

Dat een meldpunt bestaat, wil niet zeggen dat het ook goed werkt. In hun kennisgevingen aan de Commissie verklaarde een aantal lidstaten dat hun respectieve meldpunten weliswaar waren ingesteld, maar – anders dan vereist in het kaderbesluit aanvallen – niet 24 uur per dag operationeel waren. Buiten kantooruren blijken zij geen gehoor te kunnen geven aan dringende verzoeken. Publiek-private samenwerking wordt vaak gehinderd doordat meldpunten weinig doeltreffendheid zijn of niet kunnen ingaan op samenwerkingsverzoeken uit de particuliere sector.

---

1 http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xiv_04-2009.en-us.pdf, blz.10.

2 ww.theglobeandmail.com/servlet/story/RTGAM.20090328.wspy0328/BNStory/International/home?cid=al_gam_mostemail

3 Onder de term botnet wordt een netwerk verstaan van computers die zijn besmet met kwaadaardige software (een computervirus). Een dergelijk netwerk van besmette computers ("zombies") kan worden ingezet voor specifieke acties, zoals aanvallen op informatiesystemen (cyberaanvallen). Deze zombies kunnen door een andere computer worden bestuurd – dikwijls zonder dat de gebruikers van de besmette computers hier erg in hebben. De besturingscomputer wordt ook wel aangeduid als het "command-and-control centre". De personen die dit centrum besturen behoren tot de daders, aangezien zij de besmette computers gebruiken voor aanvallen op informatiesystemen. Het is bijzonder moeilijk om de daders op te sporen, doordat de computers die deel uitmaken van het botnet en de aanval uitvoeren, zich ergens anders kunnen bevinden dan de dader zelf.

4 http://www.lemonde.fr/technologies/article/2009/03/31/virus-conficker-catastrophe-ou-poisson-d-avril_1174916_651865.html

5 Verslag van de Commissie aan de Raad op basis van artikel 12 van het kaderbesluit van de Raad van 24 februari 2005 over aanvallen op informatiesystemen, COM(2008)448 def.

Ten derde zijn er nog steeds weinig gegevens beschikbaar over cyberaanvallen en over de politiële en justitiële follow-up van dergelijke aanvallen. Niet alle lidstaten verzamelen gegevens over cyberaanvallen. Van de lidstaten die dit wel doen, zijn de gegevens niet onderling vergelijkbaar, doordat zij uiteenlopende statistische methoden gebruiken.

Tot de slachtoffers van grootschalige aanvallen op informatiesystemen behoren onder meer het algemene publiek dat gebruikmaakt van informatiesystemen, evenals centrale en lokale overheden, internationale organisaties en particuliere entiteiten.

Doelen binnen de EU kunnen worden aangevallen vanuit derde landen en omgekeerd.

2. SUBSIDIARITEIT

Cybercriminaliteit is een typisch internationaal probleem, waartegen optreden op nationaal niveau maar zelden volstaat. Algemeen wordt aangenomen dat er maatregelen op EU- en internationaal niveau nodig zijn om dit probleem op te lossen en te voorkomen. Bij de meeste aanvallen worden de grenzen van de EU overschreden. De aanvallen hebben hun weerslag op alle lidstaten en er zijn aanwijzingen dat het bij een aanzienlijk deel ervan gaat om activiteiten tussen lidstaten onderling. In technisch opzicht zijn informatiesystemen vaak over grenzen heen met elkaar verbonden en onderling afhankelijk. Onder deskundigen bestaat dan ook een consensus dat er op internationaal en EU-niveau maatregelen nodig zijn en dat de bestrijding van cybercriminaliteit een doelstelling is die de lidstaten alleen niet toereikend kunnen verwezenlijken.

Een nationale aanpak van cybercriminaliteit kan tot fragmentering en inefficiëntie binnen Europa leiden. Verschillen tussen de nationale werkwijzen en het ontbreken van stelselmatige grensoverschrijdende samenwerking beperken de doeltreffendheid van de nationale tegenmaatregelen aanzienlijk. Dit is ten dele te wijten aan de onderlinge verbondenheid van informatiesystemen, aangezien een zwakke beveiliging in één land de kwetsbaarheid in andere landen kan vergroten.

3. WAT ZIJN DE DOELSTELLINGEN?

3.1 Algemene, specifieke en operationele doelstellingen

Het algemene doel van het EU-optreden is het bestrijden en vervolgen van al dan niet georganiseerde criminaliteit, overeenkomstig artikel 67 van het Verdrag betreffende de werking van de Europese Unie, door grootschalige aanvallen op informatiesystemen tegen te gaan.

A Specifieke doelstelling: criminelen die verantwoordelijk zijn voor grootschalige aanvallen vervolgen en veroordelen door onderlinge aanpassing van het strafrecht op het gebied van aanvallen op informatiesystemen

B Specifieke doelstelling: grensoverschrijdende samenwerking tussen rechtshandhavingsinstanties verbeteren

C Specifieke doelstelling: doeltreffende systemen opzetten voor bewaking en gegevensverzameling

4. WAT ZIJN DE BELEIDSOPTIES?

4.1 Optie 1 – Status quo/geen nieuwe EU-maatregelen

Deze optie houdt in dat de EU geen verdere maatregelen treft om deze vorm van cybercriminaliteit te bestrijden. Lopende maatregelen, met name de programma's voor betere bescherming van de vitale informatiestructuur en betere publiek-private samenwerking bij de aanpak van cybercriminaliteit zouden worden voortgezet.

4.2 Optie 2 – Ontwikkeling van een programma om aanvallen op informatiesystemen krachtiger tegen te gaan met niet-wetgevende maatregelen

Naast het programma ter bescherming van de vitale informatie-infrastructuur zouden niet-wetgevende maatregelen met name grensoverschrijdende wetshandhaving en publiek-private samenwerking bevorderen; deze maatregelen zouden ook nader gecoördineerd optreden op EU-niveau mogelijk moeten maken. Een niet-wetgevend voorstel zou onder meer maatregelen kunnen omvatten gericht op de versterking van het bestaande 24/7-netwerk van meldpunten voor wetshandhavingsinstanties, de oprichting van een EU-netwerk van publiek-private meldpunten voor deskundigen op het gebied van cybercriminaliteit en rechtshandhaving, en de formulering van een EU-standaardovereenkomst inzake het dienstverleningsniveau voor samenwerking op het gebied van rechtshandhaving met particuliere partijen.

4.3 Optie 3 – Gerichte herziening van het kaderbesluit aanvallen om het specifieke gevaar van grootschalige aanvallen op informatiesystemen aan te pakken

Deze optie houdt de invoering in van specifieke gerichte (d.w.z. beperkte) wetgeving ter bestrijding van bijzonder gevaarlijke grootschalige aanvallen op informatiesystemen. Deze gerichte wetgeving zou gepaard gaan met maatregelen om de operationele grensoverschrijdende samenwerking ter bestrijding van aanvallen op informatiesystemen op te voeren en met een verhoging van de bestaande minimumstraffen. Deze optie zou een herziening van het bestaande kaderbesluit aanvallen inhouden, plus een aantal niet-wetgevende maatregelen voor meer alertheid, veiligheid en flexibiliteit bij de bescherming van de vitale informatie-infrastructuur en voor betere instrumenten en procedures voor grensoverschrijdende samenwerking inzake rechtshandhaving en uitwisseling van goede praktijken.

4.4 Optie 4 – Invoering van alomvattende EU-wetgeving tegen cybercriminaliteit

Door de toename van geavanceerde aanvallen op informatiesystemen zijn dringend maatregelen geboden. In dat licht rijst de vraag of er niet ook bredere EU-wetgeving inzake cybercriminaliteit in het algemeen moet worden ingevoerd. Een dergelijke wetgeving zou niet alleen betrekking hebben op aanvallen op informatiesystemen, maar ook op zaken als financiële cybercriminaliteit, illegale internetcontent, het verzamelen/bewaren/doorgeven van elektronisch bewijsmateriaal en meer gedetailleerde rechtsmachtsregels. Een dergelijke EU-wetgeving zou van kracht kunnen zijn naast het Verdrag inzake cybercriminaliteit van de Raad van Europa, dat met name zou worden aangevuld met nieuwe, binnen de EU noodzakelijk geachte voorschriften.

4.5 Optie 5 – Herziening van het Verdrag inzake cybercriminaliteit van de Raad van Europa

Deze optie houdt een grondige heronderhandeling van het huidige Verdrag in. Dit veronderstelt een langdurig proces en is niet te rijmen met de actietermijnen die in de

effectbeoordeling worden voorgesteld. Er lijkt geen internationale bereidheid te zijn om opnieuw te onderhandelen over het Verdrag. Gelet op de termijn waarop actie geboden is, kan herziening van het Verdrag niet als een haalbare optie worden aangemerkt.

5. EFFECTBEOORDELING

Opties	Economische gevolgen	Maatschappelijke gevolgen	Gevolgen voor de grondrechten	Gevolgen voor derde landen	Relevantie voor doelstellingen A, B en C	Consistentie met internationaal recht
Optie 1: Status quo/geen nieuwe EU-maatregelen	0	0	0	-	0	0
Optie 2: Ontwikkeling van een programma om aanvallen op informatiesystemen krachtiger tegen te gaan met niet-wetgevende maatregelen	-/+	++	-/+	++	A + B ++ C +	-/+
Optie 3: Gerichte herziening van het kaderbesluit aanvallen om het gevaar van grootschalige aanvallen op informatiesystemen aan te pakken	--/++	-/+++	-/++	+++	A +++ B +++ C +++	++
Optie 4: Invoering van alomvattende EU-wetgeving tegen cybercriminaliteit	---/+++	+++	--/++	++	A ++ B ++ C ++	-/++
Voorkeursoptie (opties 2 en 3): Combinatie van niet-wetgevende maatregelen en een gerichte herziening van het kaderbesluit aanvallen	--/+++	+++	-/++	+++	A +++ B +++ C +++	++

6. WELKE OPTIES BIEDEN DE MEESTE VOORDELEN?

6.1 Optie 1 – Status quo

Deze optie brengt de particuliere partijen, de lidstaten en de Unie als geheel onvermijdelijk in een kwetsbaarder positie wat betreft de aanpak van cybercriminaliteit, gelet op de aard en groei van het verschijnsel. Ook voortzetting van de bestaande maatregelen zou Europese coördinatie vergen.

6.2 Optie 2 – Ontwikkeling van een programma ter versterking van de inspanningen om aanvallen op informatiesystemen tegen te gaan met niet-wetgevende maatregelen

Deze optie biedt alle voor- en nadelen van een "soft law"-instrument. Positief is dat elke beleidsoptie zo kan worden beschreven dat deze overeenkomt met de beste nationale praktijken, zodat de efficiëntste maatregelen gemakkelijker kunnen worden vastgesteld.

Deze optie is wat betreft de verwezenlijking van doelstellingen echter minder doeltreffend.

6.3 Optie 3 – Gerichte herziening van het kaderbesluit aanvallen om het specifieke gevaar van grootschalige aanvallen op informatiesystemen aan te pakken

Deze optie voorziet in een tijdige en gerichte respons op de gesignaleerde problemen. Er wordt werk gemaakt van de strafrechtelijke kwesties die moeten worden geregeld om de daders van dit soort criminaliteit doeltreffend te vervolgen. Ook wordt de internationale samenwerking verbeterd door de invoering van een mechanisme voor onmiddellijke internationale bijstand bij dringende verzoeken om samenwerking en wordt de samenwerking met de particuliere sector bevorderd door begeleidende maatregelen, zoals bijeenkomsten van deskundigen. Bij deze optie wordt ook een aantal verzwarende omstandigheden ingevoerd, zoals grootschalige aanvallen en aanvallen waarbij de dader zijn ware identiteit verhult en de rechtmatige bezitter van een identiteit schade berokkent.

Ten slotte worden toezichtverplichtingen ingevoerd om de omvang van het probleem te kunnen vaststellen.

6.4 Optie 4 – Invoering van alomvattende EU-wetgeving tegen cybercriminaliteit

Deze optie heeft evenals optie 3 als voordeel dat er bindende voorschriften worden opgesteld en zal – volledig uitgevoerd – naar verwachting dan ook doeltreffender uitpakken. Verder zouden bij deze optie waarschijnlijk zowel de wetgevende als de niet-wetgevende instrumenten tot optimale effecten leiden, en ook voor andere vormen van cybercriminaliteit dan grootschalige aanvallen. Bovendien zou er werk worden gemaakt van het strafrechtelijk kader en zou de grensoverschrijdende samenwerking bij rechtshandhaving erop vooruitgaan. Over deze holistische aanpak bestaat onder de belanghebbenden vooralsnog echter geen consensus, hoewel uitvoering ervan de strijd tegen cybercriminaliteit op een hoger plan zou brengen.

7. DE VOORKEURSOPTIE

Op basis van de analyse van de economisch en maatschappelijke gevolgen en van de analyse van de impact op de grondrechten, vormen opties 2 en 3 de beste aanpak van het probleem; de doelstellingen zouden ermee kunnen worden verwezenlijkt.

Over het geheel genomen zou de voorkeursoptie een combinatie zijn van de beleidsopties 2 en 3, aangezien deze elkaar aanvullen en het beste aansluiten bij de doelstellingen, zowel inhoudelijk als qua timing.

8. TOEZICHT EN EVALUATIE

Uiterlijk twee jaar na de inwerkingtreding van de richtlijn dient een uitvoeringsverslag te worden gepubliceerd. Uit dit verslag moet blijken hoe de lidstaten de richtlijn precies ten uitvoer hebben gelegd.

Verder dient regelmatig te worden nagegaan hoe en in hoeverre de richtlijn heeft bijgedragen tot de verwezenlijking van zijn doelstellingen. De eerste evaluatie dient uiterlijk vijf jaar na de inwerkingtreding van de richtlijn te worden verricht. De Commissie zal nadien om de vijf jaar een evaluatieverslag uitbrengen met daarin informatie over de tenuitvoerlegging. Op grond van de conclusies en aanbevelingen van de evaluaties dient de Commissie zich te beraden op eventuele wijzigingen of andere ontwikkelingen van de richtlijn.