EUROPESE
COMMISSIE

Brussel, 7.2.2013
SWD(2013) 31 final

WERKDOCUMENT VAN DE DIENSTEN VAN DE COMMISSIE

SAMENVATTING VAN DE EFFECTBEOORDELING

Bij

Voorstel voor een richtlijn van het Europees Parlement en de Raad

houdende maatregelen om een hoog gemeenschappelijk niveau van netwerk- en informatiebeveiliging in de Unie te waarborgen

{COM(2013) 48 final}
{SWD(2013) 32 final}

WERKDOCUMENT VAN DE DIENSTEN VAN DE COMMISSIE

SAMENVATTING VAN DE EFFECTBEOORDELING

Bij

Voorstel voor een richtlijn van het Europees Parlement en de Raad

houdende maatregelen om een hoog gemeenschappelijk niveau van netwerk- en informatiebeveiliging in de Unie te waarborgen

1. TOEPASSINGSGEBIED

Deze effectbeoordeling heeft betrekking op beleidsopties voor een betere beveiliging van het internet en van andere netwerken en informatiesystemen voor diensten die de werking van onze samenleving ondersteunen (zoals overheden, de financiële wereld en het bankwezen, energie, vervoer, gezondheidszorg en bepaalde internetdiensten die essentiële economische en maatschappelijke processen faciliteren, zoals platforms voor elektronische handel en sociale netwerken). Instrumenten om deze soort beveiliging te verzekeren, vallen onder de algemene noemer "netwerk- en informatiebeveiliging" (NIB).

2. BELEIDSCONTEXT

In 2001 heeft de Commissie voor het eerst gewezen op het toenemende belang van NIB voor onze economie en onze samenleving. Om een hoog en doeltreffend NIB-niveau op de interne markt te waarborgen, heeft de Europese Gemeenschap in 2004 besloten het Europees Agentschap voor netwerk- en informatiebeveiliging (ENISA) op te richten. De benadering die de Europese Unie tot dusverre met betrekking tot NIB heeft gevolgd, komt erop neer dat zij een reeks actieplannen en strategieën heeft vastgesteld die de lidstaten ertoe moeten aanzetten hun NIB-capaciteit te vergroten en met elkaar samen te werken om grensoverschrijdende NIB-problemen te lijf te gaan.

Er is met de belanghebbende partijen overleg gepleegd over de verschillende aspecten van het initiatief (probleemomschrijving en opties om de bestaande tekortkomingen te verhelpen):

- een **openbare online-raadpleging** over de verbetering van NIB in de EU (van 23 juli tot 15 oktober 2012). De Commissie heeft in totaal 169 reacties via de online-toepassing ontvangen en nog eens 10 schriftelijk;
- besprekingen met **de lidstaten** in het kader van het Europees Forum voor de lidstaten, bilaterale contacten en de conferentie over cyberbeveiliging die de Europese Commissie en de Europese dienst voor extern optreden op 6 juli 2012 hebben gehouden;
- besprekingen met bedrijven en verenigingen uit de **particuliere sector** in het kader van het Europees publiek-privaat partnerschap voor veerkracht, en bilaterale vergaderingen;
- besprekingen met **ENISA en CERT-EU**;
- besprekingen in het kader van de **in 2012 gehouden conferentie over de digitale agenda**.

3. PROBLEEMOMSCHRIJVING

3.1. Omschrijving van het probleem

Het probleem kan globaal worden omschreven als ***een ontoereikend niveau van bescherming tegen EU-wijde incidenten, risico's en dreigingen in verband met netwerk- en informatiebeveiliging die de werking van de interne markt ondermijnen***.

Aangezien netwerken en informatiesystemen met elkaar verweven zijn en het internet een bij uitstek mondiaal karakter heeft, stoppen veel NIB-incidenten niet aan de grens en brengen zij zodoende de werking van de interne markt in het gedrang.

Inbreuken in verband met beveiliging, zoals de aanvallen waarmee eBay en PayPal zijn geconfronteerd, kunnen tot gevolg hebben dat grensoverschrijdende diensten niet meer beschikbaar zijn, tijdelijk worden uitgeschakeld of worden onderbroken. De aanvallen tegen Diginotar, het Nederlandse internetcertificaatbedrijf, geven een duidelijk voorbeeld van de noodzaak snel tegen problemen op te treden en informatie uit te wisselen wanneer zich een majeur incident voordoet. Naar aanleiding van dergelijke incidenten beginnen de lidstaten nu hun eigen regelgeving in te voeren. Een gebrekkige coördinatie bij het opstellen van regelgeving kan echter versnippering in de hand werken en aanleiding geven tot belemmeringen op de interne markt die nalevingskosten creëren voor in meer dan één lidstaat actieve bedrijven.

Dit probleem raakt alle geledingen van de samenleving en de economie (overheden, ondernemingen en consumenten). Een aantal sectoren levert onmisbare ondersteunende diensten voor onze economie en onze samenleving en speelt bijgevolg een essentiële rol: de beveiliging van hun systemen is dan ook van bijzonder belang voor de werking van de interne markt. Het gaat onder meer om de volgende sectoren: banken, beurzen, opwekking, transport en distributie van energie, lucht-, spoor- en zeevervoer, gezondheidszorg, facilitatoren van essentiële internetdiensten en overheden. In het kader van de openbare raadpleging hebben de belanghebbende partijen zich grote voorstanders getoond van maatregelen ten bate van NIB in deze sectoren en overeenkomstige actie op EU-niveau.

Blijven extra maatregelen om de toename in het aantal incidenten om te buigen uit, dan is het niet ondenkbaar dat het vertrouwen van de consument in online-diensten wordt aangetast en het realiseren van de doelstellingen van de digitale agenda op de helling komt te staan.

3.2. Oorzaken van het probleem

Er zijn meerdere oorzaken die aan de basis liggen van het hierboven omschreven probleem.

In de eerste plaats **verschilt de capaciteit in de EU van lidstaat tot lidstaat**. Dit factor maakt het voor de partijen moeilijk elkaar te vertrouwen, terwijl dat precies een voorwaarde is om samen te werken en informatie uit te wisselen.

In de tweede plaats wordt er **te weinig informatie uitgewisseld over incidenten, risico's en dreigingen**. De meeste NIB-incidenten worden niet gerapporteerd en blijven onopgemerkt omdat bedrijven bang zijn voor reputatieschade of schadeclaims en zich daarom terughoudend opstellen ten opzichte van het uitwisselen van dergelijke informatie. In het kader van de bestaande publiek-private partnerschappen/platforms, zoals het Europees Forum voor de lidstaten en het Europees publiek-privaat partnerschap voor veerkracht, wordt alleen informatie uitgewisseld over de beste praktijken.

4. DOELTREFFENDHEID VAN BESTAANDE MAATREGELEN

4.1. Lacunes in het vigerende regelgevingskader

Op grond van de vigerende voorschriften hoeven andere entiteiten dan telecommunicatiebedrijven geen maatregelen inzake NIB-risicobeheer vast te stellen, noch NIB-incidenten te rapporteren. Toch worden alle spelers die op netwerk- en informatiesystemen zijn aangewezen, geconfronteerd met beveiligingsrisico's. Deze situatie leidt tot een ongelijk speelveld aangezien een telecomaanbieder een bepaald incident wél aan de bevoegde nationale autoriteit moet rapporteren en een bedrijf dat voice-over-IP-diensten aanbiedt en met hetzelfde incident te kampen heeft, dat niet hoeft te doen.

Alle spelers die tevens voor de gegevensverwerking verantwoordelijk zijn (zoals banken en ziekenhuizen), moeten op grond van het regelgevingskader inzake gegevensbescherming beveiligingsmaatregelen nemen die evenredig zijn aan de risico's. Voor de gegevensverwerking verantwoordelijke partijen zijn echter alleen verplicht inbreuken in verband met de beveiliging te melden die een risico inhouden voor persoonsgegevens.

Richtlijn 2008/114/EG van de Raad inzake de identificatie van Europese kritieke infrastructuren en de aanmerking van infrastructuren als Europese kritieke infrastructuren heeft alleen betrekking op de sectoren energie en vervoer. Bovendien hebben de lidstaten tot nu toe slechts enkele infrastructuren als Europese kritieke infrastructuren aangemerkt. De richtlijn behelst geen verplichting voor de exploitanten om significante inbreuken in verband met beveiliging te melden. Evenmin worden bij die richtlijn mechanismen in het leven geroepen om de samenwerking en de reactie van lidstaten bij incidenten in goede banen te leiden.

De EU-instellingen met wetgevingsbevoegdheid buigen zich momenteel over het voorstel van de Commissie voor een richtlijn over aanvallen op informatiesystemen[1]. Dit voorstel heeft uitsluitend betrekking op de strafrechtelijke behandeling van specifieke soorten gedragingen, en niet op de preventie van NIB-risico's en -incidenten, noch op de reactie op NIB-incidenten en de mildering van de impact ervan.

4.2. De beperkingen van een op vrijwilligheid gebaseerde aanpak

De op vrijwilligheid gebaseerde aanpak die tot dusverre is gevolgd, heeft geleid tot een ongelijk niveau van paraatheid en een beperkte mate van samenwerking.

Het Europees Forum voor de lidstaten heeft een beperkt mandaat, aangezien de lidstaten geen informatie over incidenten, risico's en dreigingen uitwisselen en niet samenwerken wanneer zich grensoverschrijdende dreigingen voordoen. Het forum beschikt bovendien niet over de bevoegdheid om van zijn leden te eisen dat zij over een minimumcapaciteit beschikken.

ENISA heeft geen operationele bevoegdheden en kan, bijvoorbeeld, niet ingrijpen om NIB-problemen op te lossen.

Het Europees publiek-privaat partnerschap voor veerkracht heeft geen officiële status en kan de particuliere sector niet verplichten tot het rapporteren van incidenten aan de nationale autoriteiten. Evenmin is dit partnerschap toegerust met een kader voor vertrouwelijke informatie-uitwisseling en voor de melding van informatie over NIB-dreigingen, -risico's en -incidenten.

[1] COM(2010) 517, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0517:FIN:NL:PDF

5. NOODZAAK VAN INGRIJPEN DOOR DE EU, SUBSIDIARITEIT EN EVENREDIGHEID

Het waarborgen van NIB is van essentieel belang voor de goede werking van de interne markt en het welzijn van onze samenleving. Artikel 114 VWEU is een passende rechtsgrondslag voor de harmonisering van NIB-vereisten en voor de invoering van een gemeenschappelijk minimaal beveiligingsniveau in de hele EU.

Ingrijpen van de EU op het gebied van NIB is op grond van het **subsidiariteit**sbeginsel gerechtvaardigd omdat NIB een grensoverschrijdende dimensie vertoont en omdat op EU-niveau vastgesteld beleid doelmatiger zou zijn (met een grotere toegevoegde waarde) dan nationale beleidsmaatregelen die zouden voortvloeien uit EU-beleid.

Samenwerking tussen alle lidstaten kan alleen worden gewaarborgd als zij allemaal over het vereiste minimale capaciteitsniveau beschikken. Bovendien mag duidelijk zijn dat een gezamenlijk en coöperatief NIB-beleid uitermate bevorderlijk kan zijn voor een doeltreffende bescherming van de grondrechten, en met name het recht op de bescherming van persoonsgegevens en het privéleven.

De maatregelen die in het kader van de verkozen optie zouden worden genomen, zijn gerechtvaardigd op grond van het **evenredigheid**sbeginsel aangezien de NIB-vereisten waaraan de lidstaten moeten voldoen, worden vastgesteld op het minimale niveau dat vereist is voor een adequate paraatheid en een op vertrouwen gebaseerde samenwerking, en aangezien de verplichtingen voor bedrijven en overheden om risico's te beheren en incidenten te rapporteren, slechts gelden voor kritieke entiteiten en maatregelen behelzen die evenredig zijn aan de risico's en betrekking hebben op incidenten met een aanzienlijke impact. Bovendien zouden de maatregelen die in het kader van de verkozen optie worden genomen, geen onevenredige kosten met zich brengen.

6. DOELSTELLINGEN

De algemene doelstelling is het verhogen van het niveau van bescherming tegen incidenten, risico's en bedreigingen met betrekking tot netwerk- en informatiebeveiliging in de EU. De specifieke doelstellingen zijn:

- **Doelstelling 1** – Een gemeenschappelijk minimumniveau van NIB in de lidstaten invoeren en zo het algemene niveau van paraatheid en het algemene reactieniveau verhogen.
- **Doelstelling 2** – Samenwerking inzake NIB op EU-niveau verbeteren om grensoverschrijdende incidenten en bedreigingen doeltreffend aan te pakken.
- **Doelstelling 3** – Een cultuur van risicobeheer tot stand brengen en de uitwisseling van informatie tussen de particuliere en de publieke sector verbeteren.

7. BELEIDSOPTIES

In deze effectbeoordeling zijn de volgende beleidsopties beschouwd: ongewijzigd beleid, regelgevingsaanpak en een gemengde aanpak. De mogelijke optie die erin bestaat alle EU-activiteiten inzake NIB stop te zetten, is niet in overweging genomen.

7.1. Optie 1 – Ongewijzigd beleid ("referentiescenario")

Deze optie houdt in dat de Commissie, bijgestaan door ENISA, de huidige op vrijwilligheid gebaseerde benadering voortzet en de lidstaten oproept op nationaal niveau NIB-capaciteit (bijvoorbeeld CERT's, nationale plannen voor cyberincidenten/cybernoodplannen, nationale cyberbeveiligingsstrategieën) te ontwikkelen en op EU-niveau samen te werken (bijvoorbeeld

via het netwerk van CERTs in Europa en een Europees nood-/samenwerkingsplan voor cyberincidenten).

7.2. Optie 2 – Regelgevingsaanpak

Deze optie houdt in dat de Commissie een minimumniveau vaststelt van door de lidstaten te ontwikkelen nationale capaciteit (CERT's, bevoegde autoriteiten, nationale plannen voor cyberincidenten / nationale cybernoodplannen, nationale cyberbeveiligingsstrategieën).

Volgens deze regelgevingsoptie moeten de nationale bevoegde autoriteiten en CERT's deel uitmaken van een **netwerk** voor samenwerking op EU-niveau. De autoriteiten en CERT's zouden in het netwerk informatie uitwisselen en samenwerken om NIB-bedreigingen en -incidenten aan te pakken overeenkomstig een door de lidstaten overeen te komen **Europees nood-/samenwerkingsplan voor cyberincidenten**.

Ondernemingen (met uitzondering van micro-ondernemingen) in specifieke kritieke sectoren, d.w.z. het bankwezen, de energiesector (elektriciteit en aardgas), de vervoerssector, de gezondheidszorg, alsmede actoren die belangrijke internetdiensten mogelijk maken en overheden zouden de risico's die zij lopen moeten beoordelen en passende en op de daadwerkelijke risico's afgestemde maatregelen moeten nemen. Voorts zouden deze entiteiten aan de bevoegde autoriteiten de incidenten moeten melden die de werking van hun netwerken en informatiesystemen ernstig in het gedrang brengen en dus een aanzienlijke impact hebben op de continuïteit van de diensten en de voorziening van goederen die van netwerk- en informatiesystemen afhankelijk zijn. Deze regeling sluit aan bij die van de artikelen 13 bis en 13 tres van de kaderrichtlijn voor elektronische communicatie.

7.3. Optie 3 – Gemengde aanpak

Deze optie behelst dat de Commissie regelgevingseisen ten aanzien van belangrijke particuliere spelers en overheden zou combineren met vrijwillige initiatieven, die een beroep doen op de bereidwilligheid van de lidstaten en gericht zijn op de versterking of de opbouw van NIB-capaciteit in de lidstaten en de oprichting van mechanismen voor samenwerking op EU-niveau.

De vrijwillige initiatieven zouden in wezen overeenkomen met die van optie 1, terwijl de regelgevingseisen dezelfde zouden zijn als die welke in het kader van optie 2 zouden worden opgelegd, zowel wat betreft de betrokken entiteiten als de inhoud van de verplichtingen.

ENISA zou de Commissie, de lidstaten en de particuliere sector bijstaan met ondersteuning en technische deskundigheid, bijvoorbeeld door technische richtsnoeren en aanbevelingen uit te brengen.

8. EFFECTANALYSE

Deze beoordeling heeft, behalve op het beveiligingniveau, betrekking op de economische en sociale effecten van de drie opties. Tevens heeft zij betrekking op de kosten die zouden worden gemaakt in het kader van opties 2 en 3.

Geen van de vastgestelde opties heeft milieueffecten die nauwkeurig kunnen worden voorspeld.

8.1. Optie 1 – Ongewijzigd beleid ("referentiescenario")

Niveau van beveiliging: Het is onwaarschijnlijk dat alle lidstaten vergelijkbare niveaus van nationale capaciteit en paraatheid zouden bereiken die noodzakelijk zijn om de beveiliging te verbeteren en samenwerking en betrouwbare informatie-uitwisseling op EU-niveau mogelijk te maken. Er zou geen gelijk speelveld met betrekking tot risicobeheer of meer transparantie

over incidenten tot stand worden gebracht, waardoor er dus lacunes in de regelgeving zouden blijven bestaan.

Economische effecten: Het effect zou afhangen van de mate waarin de lidstaten de aanbevelingen van de Commissie volgen. Het ontoereikende beveiligingsniveau in de minder ontwikkelde lidstaten zou hun concurrentievermogen en groei ondermijnen en hen blootstellen aan risico's en incidenten. Gezien de huidige tendensen zouden NIB-incidenten in aantal toenemen en zichtbaarder worden voor het bedrijfsleven en de consument en de voltooiing van de eengemaakte markt hinderen.

Maatschappelijke effecten: Het voortduren en de verwachte verergering van de incidenten, risico's en bedreigingen zou een negatieve invloed hebben op het vertrouwen van de consument in online-diensten.

8.2. Optie 2 – Regelgeving

Het beveiligingsniveau: De aan de lidstaten opgelegde verplichtingen zouden ervoor zorgen dat elk van hen adequaat is toegerust en bijdragen aan de totstandbrenging van een klimaat van wederzijds vertrouwen, hetgeen een voorwaarde vormt voor doeltreffende samenwerking op EU-niveau.

De invoering van eisen ten aanzien van overheden en belangrijke particuliere spelers om aan NIB-risicobeheer te doen, zou een sterke prikkel creëren om beveiligingsrisico's doeltreffend te beheersen en in te schatten. De totale aanvullende kosten die de verschillende sectoren in de EU zouden moeten dragen om deze eisen na te komen, zouden **1 tot 2 miljard euro** bedragen. De nalevingskosten **per kleine en middelgrote onderneming** zouden **2 500 tot 5 000 euro** bedragen.

Economische effecten: Door het hogere beveiligingsniveau zouden NIB-risico's en -incidenten minder financiële verliezen veroorzaken. Het vertrouwen van bedrijven en consumenten in de digitale wereld zou toenemen en de eengemaakte markt ten goede komen. De bevordering van een cultuur van versterkt risicobeheer zou ook de vraag naar beveiligde ICT-producten en -oplossingen stimuleren.

Maatschappelijke effecten: Een hoger beveiligingsniveau zou het vertrouwen van de burger in online-diensten verbeteren waardoor hij ten volle de vruchten van de digitale wereld (bijvoorbeeld sociale media, eLeren, eGezondheid) kan plukken.

8.3. Optie 3 – Gemengde aanpak

Het beveiligingsniveau: Zoals bij optie 1 is er geen garantie dat het op nationale NIB-capaciteit en samenwerking op EU-niveau gebaseerde beveiligingsniveau zou verbeteren als gevolg van vrijwillige initiatieven. Anderzijds zou de invoering van beveiligingseisen ten aanzien van overheden en belangrijke particuliere spelers een sterke prikkel geven om beveiligingsrisico's te beheersen en in te schatten. Deze mechanismen zouden echter tekortschieten in lidstaten die de aanbevelingen van de Commissie inzake de ontwikkeling van NIB-capaciteit naast zich neerleggen.

Economische effecten: De snelheid van de ontwikkelingen zou sterk uiteenlopen van lidstaat tot lidstaat. Hun ontoereikende beveiligingsniveau zou het concurrentievermogen en de groei van de minder ontwikkelde lidstaten ondermijnen en hen blootstellen aan de negatieve impact van risico's en incidenten.

Maatschappelijke effecten: Het voortduren en de verwachte verergering van de incidenten, risico's en bedreigingen zouden het vertrouwen in online-diensten negatief beïnvloeden, met name in de lidstaten die NIB niet als een prioriteit beschouwen.

9. VERGELIJKING VAN DE OPTIES

De doeltreffendheid van de opties 1 en 3 hangt af van de vraag of de vrijwillige initiatieven daadwerkelijk een minimumniveau van NIB zouden opleveren, en wat optie 3 betreft, van de bereidheid van de lidstaten om capaciteit te ontwikkelen en grensoverschrijdend samen te werken. Daarom worden deze opties niet als geschikt beschouwd om de beleidsdoelstellingen te verwezenlijken.

De voorkeur gaat uit naar optie 2 aangezien deze optie de bescherming van consumenten, bedrijven en overheden in de EU tegen NIB-incidenten, bedreigingen en risico's aanzienlijk zou verbeteren. Bovendien zou de EU, door haar zaken op orde te brengen, haar internationale invloed kunnen uitbreiden en haar – nu al aanzienlijke – geloofwaardigheid als partner op bilateraal en multilateraal niveau nog meer kracht kunnen bijzetten. De EU zou dan ook in een beter positie verkeren om de fundamentele rechten en essentiële waarden van de EU te bevorderen.

10. MONITORING EN EVALUATIE

In hoofdstuk 10 van het effectbeoordelingsverslag zijn een aantal kernindicatoren voor het meten van vooruitgang op weg naar de verwezenlijking van de doelstellingen vastgesteld. Voorbeelden hiervan zijn:

- Voor doelstelling 1, het aantal lidstaten dat een voor NIB bevoegde autoriteit en een CERT heeft aangesteld of een nationale cyberbeveiligingsstrategie en een nationaal nood-/samenwerkingsplan voor cyberincidenten heeft vastgesteld.
- Voor doelstelling 2, het aantal bevoegde autoriteiten en CERT's van de lidstaten dat deelneemt aan het netwerk en het volume informatie over NIB-risico's en -incidenten dat binnen het netwerk is uitgewisseld.
- Voor doelstelling 3, het niveau van de investeringen in NIB door grote particuliere spelers en overheden en het aantal meldingen van NIB-incidenten met een aanzienlijke impact.