Raad van de
Europese Unie

Brussel, 14 september 2017
(OR. en)

12183/17
ADD 2

Interinstitutioneel dossier:
2017/0225 (COD)

CYBER 127
TELECOM 207
ENFOPOL 410
CODEC 1397
JAI 785
MI 627
IA 139

BEGELEIDENDE NOTA

van:	de heer Jordi AYET PUIGARNAU, directeur, namens de secretaris-generaal van de Europese Commissie
aan:	de heer Jeppe TRANHOLM-MIKKELSEN, secretaris-generaal van de Raad van de Europese Unie
Nr. Comdoc.:	SWD(2017) 501 final
Betreft:	WERKDOCUMENT VAN DE DIENSTEN VAN DE COMMISSIE SAMENVATTING VAN DE EFFECTBEOORDELING bij Voorstel voor een VERORDENING VAN HET EUROPEES PARLEMENT EN DE RAAD inzake Enisa, het agentschap van de Europese Unie voor cyberbeveiliging, tot intrekking van Verordening (EU) nr. 526/2013, en inzake de certificering van de cyberbeveiliging van informatie- en communicatietechnologie ("de cyberbeveiligingsverordening")

Hierbij gaat voor de delegaties document SWD(2017) 501 final.

Bijlage: SWD(2017) 501 final

EUROPESE
COMMISSIE

Brussel, 13.9.2017
SWD(2017) 501 final

WERKDOCUMENT VAN DE DIENSTEN VAN DE COMMISSIE

SAMENVATTING VAN DE EFFECTBEOORDELING

bij

Voorstel voor een VERORDENING VAN HET EUROPEES PARLEMENT EN DE RAAD

inzake Enisa, het agentschap van de Europese Unie voor cyberbeveiliging, tot intrekking van Verordening (EU) nr. 526/2013, en inzake de certificering van de cyberbeveiliging van informatie- en communicatietechnologie ("de cyberbeveiligingsverordening")

{COM(2017) 477 final}
{SWD(2017) 500 final}
{SWD(2017) 502 final}

A. BEHOEFTE AAN ACTIE

Wat is het probleem en waarom is het een probleem?

Digitale technologieën en het internet vormen de ruggengraat van de Europese economie en samenleving. Kritieke economische sectoren zoals vervoer, energie, gezondheidszorg en financiën zijn in steeds grotere mate afhankelijk van netwerk- en informatiesystemen om hun kernactiviteiten uit te voeren. Het internet der dingen verbindt objecten en mensen via communicatienetwerken. Deze nieuwe werkelijkheid zorgt voor ongekende mogelijkheden, maar ook voor kwetsbare punten. Cyberincidenten worden een steeds ernstiger probleem. De complexiteit, veelvuldigheid en reikwijdte van dergelijke incidenten (van toegang tot essentiële diensten tot impact op democratische processen) zullen nog verder toenemen.

In dat kader zijn de volgende onderling samenhangende problemen geconstateerd:

- de versnippering van het beleid en de benaderingen betreffende cyberbeveiliging in de lidstaten;
- de versnippering van de middelen en de benaderingen betreffende cyberbeveiliging binnen de EU-instellingen, -agentschappen en -organen;
- de burgers en bedrijven die zich onvoldoende bewust zijn van cyberdreigingen en onvoldoende informatie krijgen over de beveiligingseigenschappen van de ICT-producten en -diensten die zij aankopen, terwijl steeds meer verschillende nationale en sectorale certificeringsregelingen worden opgezet.

Deze problemen zijn van invloed op de algehele cyberweerbaarheid van de EU en de doeltreffende werking van de interne markt.

Wat is het streefdoel?

De specifieke beleidsdoelstellingen van het initiatief zijn:

1. De vermogens en de paraatheid van de lidstaten en het bedrijfsleven versterken, met name wat betreft kritieke infrastructuurvoorzieningen.
2. De samenwerking en de coördinatie tussen de lidstaten en de EU-instellingen, -agentschappen en -organen verbeteren.
3. De vermogens op EU-niveau versterken ter aanvulling van maatregelen van de lidstaten, met name in het geval van grensoverschrijdende cybercrises.
4. Het bewustzijn van de burgers en het bedrijfsleven met betrekking tot cyberbeveiligingskwesties versterken.
5. De zekerheid inzake cyberbeveiliging van ICT-producten en -diensten in het algemeen transparanter maken zodat het vertrouwen in de digitale eengemaakte markt en in digitale innovatie toeneemt.
6. De versnippering van certificeringsregelingen in de EU en van de daarmee samenhangende beveiligingseisen en evaluatiecriteria in alle lidstaten en sectoren voorkomen.

Wat is de meerwaarde van actie op EU-niveau?

Aangezien de digitalisering en de vervlechting van de economieën en samenlevingen zich op mondiaal vlak voltrekken, rijken de hiermee samenghangende problemen verder dan het grondgebied van een enkele lidstaat. Ingrijpen op EU-niveau is daarom noodzakelijk. In de huidige context en rekening houdend met toekomstige scenario's, lijkt het erop dat individuele maatregelen van lidstaten en een versnipperde benadering ten aanzien van cyberbeveiliging, met name gezien de belangrijke grensoverschrijdende dimensie ervan, de collectieve cyberweerbaarheid van de EU niet kunnen versterken.

B. OPLOSSINGEN

Welke opties dienen zich aan? Is er al dan niet een voorkeursoptie?

In deze effectbeoordeling komt een specifieke reeks beleidsopties aan bod die betrekking hebben op de herziening van het Agentschap van de Europese Unie voor netwerk- en informatiebeveiliging (Enisa) en de ICT-beveiligingscertificering.

Herziening van het Enisa

Optie 0 – **Basisscenario** – Deze optie houdt in dat de huidige toestand wordt gehandhaafd. Het mandaat van het Enisa wordt verlengd en de doelstellingen en taken van het agentschap blijven grotendeels ongewijzigd, waarbij rekening wordt gehouden met de taken die op grond van achteraf vastgestelde EU-wetgeving (bijv. de richtlijn cyberbeveiliging) aan het Enisa zijn toevertrouwd.

Optie 1 – **Het mandaat van het Enisa vervalt** (het Enisa wordt afgeschaft). Deze optie houdt in dat het Enisa aan het eind van het mandaat (juni 2020) wordt afgeschaft en dat de bevoegdheden/activiteiten opnieuw worden verdeeld op EU- en/of nationaal niveau.

Optie 2 – **"Hervormd Enisa"**. Deze optie houdt in dat er wordt voortgebouwd op het huidige mandaat van het Enisa om met een aantal specifieke veranderingen rekening te houden met de ontwikkeling van het cyberbeveiligingslandschap. Het agentschap krijgt een permanent mandaat dat is gebaseerd op de volgende bouwstenen: steun voor de ontwikkeling en implementatie van EU-beleid; capaciteitsopbouw; kennis en informatie; marktgerelateerde taken; onderzoek en innovatie; en operationele samenwerking en crisisbeheersing.

Optie 3 – **EU-cyberbeveiligingsagentschap met volledige operationele vermogens**. Deze optie houdt in dat het Enisa wordt hervormd doordat drie hoofdfuncties bij elkaar worden gebracht: 1. een beleids-/adviesfunctie; 2. een informatie- en expertisecentrum, en 3. een computercrisisteam (Computer Emergency Response Team – CERT). De reikwijdte van het mandaat ondergaat bij deze optie grotendeels dezelfde verandering als bij optie 2. Er komen echter aanvullende taken bij op het gebied van de reactie op incidenten en crisisbeheersing, waardoor het agentschap betrokken is bij de gehele levenscyclus van cyberbeveiliging en het zich bezighoudt met de preventie en opsporing van alsmede de reactie op cyberincidenten.

Certificering

Optie 0 – Basisscenario – Geen maatregelen. Deze optie houdt in dat de Commissie de huidige toestand handhaaft en geen beleids- of wetgevende maatregelen neemt.

Optie 1 – **Niet-wetgevende maatregelen ("soft law")**. Deze optie houdt in dat de Commissie "soft policy"-instrumenten gebruikt (bijv. interpretatieve mededelingen, ondersteuning van EU-brede zelfreguleringsinitiatieven en normalisatiewerkzaamheden) om de transparantie te vergroten en de versnippering terug te dringen.

Optie 2 – Een EU-wetgevingshandeling die ervoor zorgt dat de SOG-IS-overeenkomst voor alle lidstaten geldt. Deze beleidsoptie houdt in dat de Commissie een voorstel doet voor een wetgevingshandeling op basis waarvan alle lidstaten lid worden.

Optie 3 – Een **algemeen EU-kader voor ICT-beveiligingscertificering**. Deze optie houdt in dat er een Europees kader voor ICT-beveiligingscertificering wordt opgezet (met inbegrip van een deskundigengroep waarvan nationale autoriteiten deel uitmaken), voor zover mogelijk voortbouwend op bestaande regelingen voor ICT-beveiligingscertificering. In wezen maakt het kader het mogelijk dat EU-regelingen voor beveiligingscertificering worden opgezet die in alle lidstaten worden aanvaard.

De voorkeursoptie is een combinatie van optie 2 voor het Enisa en optie 3 voor certificering.

Wie zijn de verschillende belanghebbenden? Wie steunt welke optie?

De overgrote meerderheid van de belanghebbenden uit alle categorieën (de lidstaten, het bedrijfsleven, de EU-instellingen, de onderzoeksgemeenschap) die hebben deelgenomen aan de raadplegingen lijkt achter de voorkeursoptie te staan: zij zijn voorstander van de versterking van het Enisa en de totstandbrenging van een Europees kader voor ICT-beveiligingscertificering.

Men is het er met name over eens dat het (minimaal) noodzakelijk is om een goed werkend EU-agentschap met een permanent mandaat te hebben, dat dat agentschap over voldoende middelen moet beschikken en dat het gemachtigd moet zijn om de huidige en toekomstige cyberbeveiligingsuitdagingen aan te gaan. De belanghebbenden zijn het verder in grote lijnen eens over de totstandbrenging van een vrijwillig, schaalbaar Europees kader.

Vanuit de branche wordt deze oplossing voor certificering gesteund door bedrijven die al aan eisen inzake certificering zijn onderworpen en die zouden profiteren van een EU-breed mechanisme dat is gebaseerd op de wederzijdse erkenning van certificaten. Deze oplossing wordt ook gesteund door de kleine en middelgrote ondernemingen die er het meest onder zouden lijden als in de verschillende lidstaten verschillende certificeringsprocedures moeten worden doorlopen. Sommige lidstaten, met name lidstaten die over minder middelen beschikken, en sommige vertegenwoordigers van de branche en de EU-instellingen, staan ook positief tegenover optie 3 voor het Enisa.

C. EFFECTEN VAN DE VOORKEURSOPTIE

Wat zijn de voordelen van de voorkeursoptie (indien er een voorkeur is, anders van de belangrijkste opties)?

De voorkeursoptie houdt in dat de EU beschikt over een agentschap dat erop is gericht ondersteuning te verlenen aan de lidstaten, de EU-instellingen en bedrijven in gebieden waar de meerwaarde van die ondersteuning het grootst is. Daartoe behoren ondersteuning bij de uitvoering van de NIS-richtlijn, ontwikkeling en uitvoering van beleid, kennis en bewustzijn,

onderzoek, operationele samenwerking en crisisbeheer alsmede de markt. In het bijzonder zou het Enisa ondersteuning bieden aan het EU-beleid inzake ICT-beveiligingscertificering door te zorgen voor administratief onderhoud en technisch beheer van een Europees kader voor ICT-beveiligingscertificering. Een dergelijk kader zou op doeltreffende wijze een reeks voorschriften invoeren betreffende de governance van de ICT-beveiligingscertificering in de EU, ter bevordering van een stelsel van wederzijdse erkenning van in alle lidstaten afgegeven certificaten. De oplossing waarbij deze opties worden gecombineerd, wordt beschouwd als de meest doeltreffende manier om deze vastgestelde doelstellingen te bereiken: het verhogen van de vermogens op het gebied van cyberbeveiliging, paraatheid, samenwerking, bewustheid, transparantie alsmede het voorkomen van de versnippering van de markt. Deze optie hangt ook het meest samen met de beleidsprioriteiten, aangezien deze is verankerd in de cyberbeveiligingsstrategie en aanverwant beleid (bijv. de NIS-richtlijn) alsmede in de strategie voor de digitale eengemaakte markt. Bovendien worden bij deze optie de doelstellingen bereikt door middel van een redelijk gebruik van middelen.

Wat zijn de kosten van de voorkeursoptie (indien er een voorkeur is, anders van de belangrijkste opties)?

Hoewel een "hervormd Enisa" nieuwe rollen zal bekleden, zou het een flexibele organisatie blijven. De vereiste financiële bijdrage uit de EU-begroting zou groter zijn dan momenteel het geval is, maar nog steeds betrekkelijk klein in vergelijking met andere agentschappen die ook op kritieke gebieden actief zijn.

De totstandbrenging van een Europees kader voor ICT-beveiligingscertificering zou geen aanloopkosten voor de industrie (met inbegrip van het midden- en kleinbedrijf) vergen. Met het kader kunnen de kosten aanzienlijk worden teruggeschroefd voor bedrijven die hun producten al certificeren of bereid zijn beveiligingscertificering uit te voeren, hetgeen wereldwijd bevorderlijk is voor hun concurrentievermogen. Er zijn wel enkele budgettaire verbintenissen nodig voor het onderhoud van het kader waarin voornamelijk zou worden voorzien door het "hervormd Enisa"-model wat betreft de technische en secretariaatstaken.

Zijn er significante gevolgen voor de nationale begrotingen en overheden?

Nee. De kosten voor het versterken van het Enisa zouden voornamelijk voor rekening van de EU-begroting komen, waarbij de lidstaten wel vrijwillige bijdragen aan het Agentschap zouden kunnen leveren. Wat betreft de certificering zouden de voornaamste gevolgen voor de nationale begrotingen en overheden voortvloeien uit de oprichting van een certificeringsautoriteit, voor zover passend.

Zijn er nog andere significante gevolgen?

Nee.

Evenredigheid

De voorkeursoptie bevat evenwichtige maatregelen die allemaal noodzakelijk worden geacht om de betrokken doelstellingen te bereiken zonder buitensporige lasten voor de desbetreffende belanghebbenden. Het initiatief wordt daarom geacht te voldoen aan het evenredigheidsbeginsel.

D. FOLLOW-UP

Wanneer wordt dit beleid geëvalueerd?

Volgens het voorstel zal de eerste evaluatie vijf jaar na de inwerkingtreding van het wetsinstrument plaatsvinden. De Commissie zal vervolgens aan het Europees Parlement en de Raad verslag uitbrengen over haar evaluatie en wanneer passend een voorstel voor herziening doen. Verdere evaluaties zullen om de vijf jaar plaatsvinden.