EUROPESE
COMMISSIE

Brussel, 16.12.2020
SWD(2020) 344 final

WERKDOCUMENT VAN DE DIENSTEN VAN DE COMMISSIE

SAMENVATTING VAN HET EFFECTBEOORDELINGSVERSLAG

bij

Voorstel voor een Richtlijn van het Europees Parlement en de Raad

betreffende maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in heel de EU en tot intrekking van Richtlijn (EU) 2016/1148

{COM(2020) 823 final} - {SEC(2020) 430 final} - {SWD(2020) 345 final}

Samenvatting

Effectbeoordeling van de *herziening van Richtlijn (EU) 2016/1148 van 6 juli 2016 houdende maatregelen voor een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de Unie (hierna "de NIS-richtlijn")*

A. Behoefte aan actie

Wat is het probleem en waarom is het een probleem op EU-niveau?

Ondanks de opmerkelijke verwezenlijkingen van de NIS-richtlijn, die het pad hebben geëffend voor een significante wijziging van de mentaliteit en de institutionele en regelgevingsbenadering met betrekking tot cyberbeveiliging in talrijke lidstaten, is ondertussen gebleken dat de richtlijn ook haar beperkingen heeft. De digitale transformatie van de maatschappij (nog versterkt door de COVID-19-crisis) heeft het bedreigingslandschap verruimd en leidt tot nieuwe uitdagingen, die een aangepaste, innovatieve reactie vereisen. Het aantal cyberaanvallen blijft toenemen, met steeds geavanceerdere aanvallen afkomstig van uiteenlopende bronnen binnen en buiten de EU.

Op basis van de evaluatie van de werking van de NIS-richtlijn zijn in de effectbeoordeling de volgende problemen vastgesteld: de beperkte cyberveerkracht van ondernemingen die actief zijn in de EU; de verschillen in veerkracht tussen lidstaten en sectoren en de beperkte gemeenschappelijke situationele kennis en het gebrek aan een gemeenschappelijke crisisrespons. Door sommige van deze problemen en factoren zien we bijvoorbeeld situaties waar grote ziekenhuizen in één lidstaat niet onder de NIS-richtlijn vallen en de uit de richtlijn voortvloeiende beveiligingsmaatregelen dus niet hoeven toe te passen, terwijl in een andere lidstaat nagenoeg elk ziekenhuis in het land aan de beveiligingsvoorschriften van de NIS-richtlijn moet voldoen.

Wat moet er worden bereikt?

Met de herziening van de NIS-richtlijn worden drie algemene doelstellingen nagestreefd:

1. **de cyberveerkracht vergroten van een uitgebreid scala aan ondernemingen die in de Europese Unie actief zijn in alle relevante sectoren**, door regels in te voeren die waarborgen dat alle publieke en particuliere entiteiten op de interne markt die een belangrijke functie vervullen voor de economie en de samenleving in haar geheel, passende cyberbeveiligingsmaatregelen treffen;
2. **verschillen in de veerkracht op de interne markt in de sectoren die reeds onder de richtlijn vallen beperken,** door een verdere onderlinge afstemming van (1) het de facto toepassingsgebied, (2) de voorschriften voor de beveiliging en het melden van incidenten, (3) de bepalingen inzake het nationale toezicht en de nationale handhaving en (4) de capaciteiten van de bevoegde autoriteiten in de lidstaten;
3. **de gemeenschappelijke situationele kennis en de collectieve paraatheid en responscapaciteit vergroten,** door maatregelen te nemen om het vertrouwen tussen bevoegde autoriteiten te vergroten, meer informatie uit te wisselen en regels en procedures vast te stellen voor grootschalige incidenten of crises.

Wat is de meerwaarde van optreden op EU-niveau (subsidiariteit)?

De cyberveerkracht in de Unie kan niet doeltreffend zijn als zij op verschillende manieren wordt aangepakt via nationale of regionale silo's. De NIS-richtlijn moest dat probleem oplossen door een kader tot stand te brengen voor de beveiliging van netwerk en -informatiesystemen op nationaal en Unieniveau.

De omzetting en uitvoering van de richtlijn heeft echter ook de inherente gebreken van bepaalde bepalingen of benaderingen aan het licht gebracht, zoals de onduidelijke afbakening van het toepassingsgebied van de NIS-richtlijn. Bovendien is de Europese economie sinds de COVID-19-crisis meer dan ooit afhankelijk geworden van netwerk- en informatiesystemen en zijn sectoren en diensten steeds meer onderling verbonden. De eerste periodieke evaluatie van de NIS-richtlijn bood dan ook de gelegenheid voor verder EU-optreden. EU-optreden dat verder gaat dan de huidige maatregelen van de NIS-richtlijn is hoofdzakelijk gerechtvaardigd vanwege: (i) de grensoverschrijdende aard van het probleem; (ii) het potentieel van EU-optreden om doeltreffende nationale beleidsmaatregelen te verbeteren en te vergemakkelijken; (iii) de bijdrage van op overleg en samenwerking gebaseerde NIS-beleidsmaatregelen aan de daadwerkelijke bescherming van gegevens en van de persoonlijke levenssfeer.

B. Oplossingen

Welke opties zijn er om de doelstellingen te verwezenlijken? Heeft een bepaalde optie de voorkeur? Indien niet, waarom niet?

In de effectbeoordeling werden vier beleidsopties geanalyseerd: (0) handhaving van de status quo; (1) niet-wetgevende maatregelen om de omzetting op één lijn te brengen; (2) beperkte veranderingen in de NIS-richtlijn met het oog op een verdere harmonisatie; (3) systemische en structurele wijzigingen van de NIS-richtlijn. Optie 1 werd al in een vroege fase terzijde geschoven aangezien zij niet wezenlijk afwijkt van de status quo. De conclusie van de effectbeoordeling luidt dat optie 3 (**systemische en structurele wijzigingen van het NIS-kader**) de **voorkeursoptie** is, aangezien deze optie een meer fundamentele wijziging van de aanpak zou beogen om een ruimer segment van de economieën in de Unie te bestrijken, maar met een gerichter toezicht op grotere, belangrijke bedrijven, waarbij het toepassingsgebied tegelijkertijd duidelijk zou worden gedefinieerd. Met deze optie zouden ook de beveiligingsgerelateerde verplichtingen voor bedrijven worden gestroomlijnd en verder worden geharmoniseerd, wat een doeltreffendere omgeving zou creëren voor de operationele aspecten en een duidelijke basis zou verschaffen voor gedeelde verantwoordelijkheden en verantwoordingsplicht van relevante actoren, en informatie-uitwisseling zou stimuleren

Wat zijn de verschillende standpunten van de belanghebbenden? Wie steunt welke optie?

De meeste bevoegde autoriteiten en ondernemingen spraken hun steun uit voor een herziening van de NIS-richtlijn. Zij gaven in verschillende raadplegingen aan dat een herziene NIS-richtlijn aanvullende (sub)sectoren diende te bestrijken en verdere beveiligingsmaatregelen en verslagleggingsverplichtingen op een lijn zou moeten brengen of zou moeten stroomlijnen. De belanghebbenden spraken eveneens hun steun uit voor nieuwe concepten of beleidsmaatregelen die alleen in de voorkeursoptie zijn opgenomen (bv. beveiligingsbeleid voor de toeleveringsketen, institutionalisering van een operationeel kader voor EU-crisisbeheer).

C. Effecten van de voorkeursoptie

Wat zijn de voordelen van de voorkeursoptie (indien van toepassing, anders van de belangrijkste opties)?

De voorkeursoptie zou aanzienlijke voordelen opleveren: uit ramingen op basis van een economisch model dat werd ontwikkeld in het kader van een ondersteunende studie voor de NIS-herziening blijkt dat de voorkeursoptie tot een daling van de kosten van cyberbeveiligingsincidenten met 11,3 miljard EUR zou kunnen leiden.

Het sectorale toepassingsgebied zou aanzienlijk worden uitgebreid binnen het NIS-kader, maar naast

bovenstaande voordelen zouden de lasten die de NIS-voorschriften met zich zouden brengen, met name uit toezichtsoogpunt, ook evenwichtig zijn voor zowel de nieuwe entiteiten die onder het kader zouden vallen als de bevoegde autoriteiten. De reden daarvoor is dat het nieuwe NIS-kader een tweeledige aanpak tot stand zou brengen, waarin de nadruk ligt op grote en essentiële entiteiten en er een onderscheid wordt gemaakt in de toezichtregelingen, waardoor voor een groot aantal van die entiteiten louter ex-posttoezicht wordt toegelaten (d.w.z. reactief toezicht, zonder algemene verplichting om de naleving systematisch te documenteren), met name voor ondernemingen die "belangrijk" maar nog niet "essentieel" worden geacht.

Over het algemeen zou de voorkeursoptie tot efficiënte afwegingen en synergieën leiden en heeft zij van alle geanalyseerde beleidsopties het grootste potentieel om een hoger, consistent niveau van cyberveerkracht van essentiële entiteiten te verzekeren in de gehele Unie, dat uiteindelijk tot kostenbesparingen zou leiden voor zowel de ondernemingen als de samenleving.

Wat zijn de kosten van de voorkeursoptie (indien van toepassing, anders van de belangrijkste opties)?

De voorkeursoptie zou tot bepaalde nalevings- en handhavingskosten leiden voor de betrokken autoriteiten van de lidstaten (er werd een totale verhoging van de middelen met ongeveer 20-30 % geraamd). Het nieuwe kader zou echter ook aanzienlijke voordelen opleveren dankzij een beter overzicht van en een betere interactie met essentiële bedrijven, een betere grensoverschrijdende operationele samenwerking en mechanismen voor wederzijdse bijstand en collegiale toetsing. Dat zou tot een algemene toename van de cyberbeveiligingscapaciteiten in de lidstaten leiden.

Voor de ondernemingen die onder het toepassingsgebied van het NIS-kader zouden vallen, wordt geraamd dat zij hun uitgaven voor ICT-beveiliging in de jaren na de invoering van het nieuwe NIS-kader met maximaal 22 % zouden moeten verhogen (dit zou 12 % zijn voor ondernemingen die al onder het toepassingsgebied van de huidige NIS-richtlijn vallen). Deze gemiddelde stijging van de uitgaven voor ICT-beveiliging zou echter een evenredig voordeel opleveren van dergelijke investeringen, met name vanwege een aanzienlijke daling van de kosten van cyberbeveiligingsincidenten (die op 11,3 miljoen EUR gedurende tien jaar worden geraamd).

Wat zijn de effecten op kmo's en op het concurrentievermogen?

Kleine en micro-ondernemingen zouden op grond van de voorkeursoptie worden vrijgesteld van de NIS-richtlijn. Voor middelgrote ondernemingen valt er een toename van de uitgaven voor ICT-beveiliging te verwachten in de eerste jaren na de invoering van het nieuwe NIS-kader. Tegelijk zou het verhogen van de beveiligingseisen voor die entiteiten ook hun cyberbeveiligingscapaciteiten stimuleren en hun beheer van ICT-risico's helpen verbeteren.

Zullen er significante gevolgen zijn voor de nationale begrotingen en administraties?

Er zouden gevolgen zijn voor de nationale begrotingen en administraties: op korte en middellange termijn zou er een geraamde verhoging van de middelen met ongeveer 20-30 % te verwachten vallen.

Zullen er andere significante gevolgen zijn?

Er vallen geen andere significante nadelige gevolgen te verwachten. De voorkeursoptie zal naar verwachting tot meer robuuste cyberbeveiligingscapaciteiten leiden en zou derhalve een belangrijker beperkend effect hebben op het aantal incidenten, met inbegrip van gegevenslekken, en de ernst ervan. Ze zal waarschijnlijk ook een positief effect hebben op het verzekeren van gelijke voorwaarden in de lidstaten voor alle entiteiten die onder het toepassingsgebied van de NIS-richtlijn vallen en de ongelijke spreiding van informatie over cyberbeveiliging beperken.

Evenredigheid?
De voorkeursoptie gaat niet verder dan wat nodig is om de specifieke doelstellingen op bevredigende wijze te verwezenlijken. De beoogde afstemming en stroomlijning van beveiligingsmaatregelen en verslagleggingsverplichtingen houdt verband met de verzoeken van de lidstaten en ondernemingen om het huidige kader te verbeteren.
D. Follow-up
Wanneer wordt dit beleid geëvalueerd?
De eerste evaluatie zou 54 maanden na de inwerkingtreding van het rechtsinstrument plaatsvinden. De Commissie zou bij het Europees Parlement en de Raad een verslag indienen over haar evaluatie. De evaluatie zou worden voorbereid met de steun van Enisa en de samenwerkingsgroep.