Gooimeer 4-15
1411 DC Naarden

088-1182510
info@cyberveilignederland.nl

Aan: Ministerie van Economische Zaken en Klimaat

Datum: 16 augustus 2020
Betreft: Input Cyberveilig Nederland ten behoeve van consultatie: uitvoeringswet CSA

Geachte heer/mevrouw,

De uitvoeringswet cyberbeveiligingsverordening is in consultatie is gegaan. Cyberveilig Nederland wil u graag enkele suggesties meegeven voor deze verordening.

Cyberveilig Nederland is dé belangenorganisatie voor cybersecurity bedrijven in Nederland. We brengen transparantie aan in de sector door de ontwikkeling van een gedragscode en keurmerk. We nemen actief deel aan het publieke debat en zien cybersecurity niet alleen als een risico, maar juist ook als een kans om Nederland te positioneren als een land dat veilige producten en diensten voortbrengt. We gaan het gesprek aan met de overheid en andere strategische partners om onze kennis en kunde van het cybersecurity werkveld voor het grotere belang in te zetten. We brengen verbindingen tot stand, tussen cybersecurity bedrijven onderling, maar ook brengen we vragers en aanbieders samen. We praten met de overheid en politiek om (toekomstige) knelpunten weg te nemen die de digitale weerbaarheid van Nederland in de weg staan. Maar vooral: we doen! We zijn initiatiefnemer en uitvoerder van het Cybersecurity Woordenboek: tot stand gebracht onder de Cybersecurity Alliantie in samenwerking met 70 publiek-private partners. Zie:
https://cyberveilignederland.nl/woordenboek-cyberveilig-nederland/

Belang van digitalisering voor Nederland

De digitale economie is niet meer weg te denken. Wet- en regelgeving vanuit de Europese Unie zal dan ook gericht moeten zijn op een versnelling van die transformatie. Alleen dan worden de economische en maatschappelijke mogelijkheden optimaal benut. Het vergroten van de weerbaarheid is een belangrijke randvoorwaarde voor Nederland, gezien onze internationale positie van digitale mainport. Immers, discontinuïteit bij organisaties doordat zij slachtoffer zijn van cybercrime is aan de orde van de dag. Diefstal van (intellectuele) eigendommen door statelijke actoren komt steeds vaker voor. Desinformatie ('fake news') en hierdoor de (mogelijke) ondermijning van de democratische rechtsorde is een zorgelijke ontwikkeling. Aandacht voor cybersecurity is daarom geen luxe, maar noodzaak. Het verkleinen van de digitale kwetsbaarheid binnen Europa is een gemeenschappelijke uitdaging die vraagt om een actieve en stimulerende rol van de overheid en politiek. Cyberveilig Nederland geeft in deze brief haar visie op de functie van de uitvoeringswet cyberbeveiligingsverordening in deze digitale transformatie.

Aandachtspunten rondom de cyberbeveiligingscertificering

In de uitvoeringswet cyberbeveiligingsverordening staat uitgebreid beschreven dat door middel van een geharmoniseerde certificatiesystematiek de cyberbeveiliging in de Europese Unie moet worden vergroot teneinde de (digitale) interne markt te versterken. Cyberveilig Nederland is een groot voorstander van een geharmoniseerde certificatiesystematiek, het doel is voor ons volstrekt helder en ook noodzakelijk. Vanuit Cyberveilig Nederland zijn er wel enkele aandachtspunten te benoemen:

1. Het toezicht op de naleving zal worden belegd bij Agentschap Telecom (AT). Cyberveilig Nederland gaat er van uit dat met de uitbreiding van deze taken het Agentschap Telecom ook een personele uitbreiding zal krijgen specifiek voor deze werkzaamheden.
2. Naast toezicht op de naleving is ook handhaving van belang. Gezien de globalisering van de technologiemarkt is het van belang nauwlettend in de gaten te houden of digitale diensten en producten die binnen de Europese grenzen verkocht worden voldoen aan de Europese standaarden. Met name in het licht van de opkomst van IoT (Internet of Things) is handhaving een urgent vraagstuk.
3. Het is belangrijk dat certificaten een erkende waarde hebben. Ze moeten een bepaalde mate van onafhankelijkheid en autoriteit hebben zodat afnemers, gebruikers en andere belanghebbenden erop kunnen vertrouwen dat digitale diensten daadwerkelijk voldoen aan de vastgestelde eisen ten aanzien van betrouwbaarheid, veiligheid en conformiteit wanneer zij van zo’n certificaat zijn voorzien. Op deze manier hoeft er minder te worden geïnvesteerd in (herhaalde) kwaliteitsonderzoeken, inspecties en audits door afnemers.
4. Bij voorkeur moeten de kwalificerende eisen voor certificaten worden vastgelegd in wet- en regelgeving.

Cyberveilig Nederland pleit voor een personele uitbreiding van het Agentschap Telecom voor de aanvullende taken, dat handhaving effectief wordt vormgegeven en dat er zekerheden worden geboden ten aanzien van de betrouwbaarheid, veiligheid en conformiteit van digitale diensten.

Bevorder het gebruik van certificering voor alle digitale diensten

De uitvoeringswet cyberbeveiligingsverordening geeft aan dat er sectoren zijn die van vitaal belang zijn. Cyberveilig Nederland wijst erop dat de definitie van vitale sectoren niet in beton is gegoten. Immers door de impact van COVID-19 bleek de zorgsector toch meer vitaal dan van tevoren werd ingeschat.

Daarnaast zijn vitale partijen in grote mate afhankelijk van toeleveranciers die veelal niet als vitaal zijn aangeduid. Vaak worden diensten die niet binnen de scope van de WBNI vallen, in ketens gebruikt van essentiële, of zelfs vitale diensten. Het is daarom belangrijk om deze impliciete afhankelijkheden te identificeren en hierop te acteren. Er ontstaan namelijk als gevolg hiervan risico's in de dienstverleningsketen waar nu nog weinig aandacht voor is.

Hoewel de uitvoeringswet zich beperkt tot de vitale sectoren, zorgen zowel de verschuivende definitie van 'vitaal' én ketenafhankelijkheid voor een noodzaak tot bredere certificering. Ten aanzien van ICT-producten, -diensten en -processen met een hoog veiligheidsrisico pleit Cyberveilig Nederland ervoor dat certificering versneld een verplichtend karakter moet krijgen en niet gewacht moet worden tot 2023.

Cyberveilig Nederland pleit voor een verplichte certificering voor wat betreft ICT-producten, -diensten en -processen met een hoog veiligheidsrisico.

Versterk de Nederlandse invloed binnen ENISA

De uitvoeringswet cyberbeveiligingsverordening geeft een grotere rol aan ENISA. De taken en bevoegdheden van ENISA worden op verschillende onderdelen uitgebreid. Cyberveilig Nederland vindt het een positieve ontwikkeling dat er meer en beter binnen de Europese Unie wordt samengewerkt op verschillende onderdelen van cybersecurity: van het actief delen van informatie tot het gezamenlijk oefenen en het starten van campagnes om burgers meer kennis en handelend vermogen te geven om cyberweerbaar te worden. Alleen door samen te werken kunnen we als Europa een krachtige vuist maken. Cyberveilig Nederland vindt het echter een belangrijk aandachtspunt dat de Nederlandse betrokkenheid bij ENISA wordt vergroot. Naar ons weten is er op dit moment geen Nederlandse vertegenwoordiging werkzaam bij ENISA. Cyberveilig Nederland pleit ervoor dat deze vertegenwoordiging er wel komt.

Cyberveilig Nederland pleit voor permanente Nederlandse vertegenwoordiging bij ENISA.

Investeer blijvend in cybersecurityonderzoek binnen Europa

De uitvoeringswet cyberbeveiligingsverordening geeft blijk van een ambitieuze cybersecurity agenda voor de Europese Unie. Zoals gezegd is Cyberveilig Nederland hier verheugd over. Echter, gezien de huidige begrotingsonderhandelingen tussen de verschillende lidstaten maken wij ons zorgen over de toekomstige onderzoeksgelden die vanuit Europa beschikbaar worden gesteld. Voor veel van de (met name technische) oplossingen zijn cybersecurity dienstverleners grotendeels afhankelijk van niet-Europese producten. De huidige mondiale spanningen in acht nemend, kan het voor Europa verstandig zijn om een meer zelfstandige kennispositie te hebben op verschillende cybersecurity-domeinen.

Cyberveilig Nederland voorziet dat binnen afzienbare tijd het ambitieniveau van de uitvoeringswet cyberbeveiligingsverordening niet kan worden gerealiseerd indien het *investeringsniveau niet significant hoger is dan het nu lijkt te worden. Om de ambitie te realiseren zijn structureel meer middelen nodig voor Europees cybersecurityonderzoek.*

Geef meer aandacht en middelen aan PPS-constructies en multi-stakeholder samenwerkingen

De uitvoeringswet cyberbeveiligingsverordening geeft relatief weinig aandacht aan het belang van Publiek-Private samenwerkingsvorming als oplossingen om het niveau van cybersecurity te vergroten.

Met alleen juridische instrumenten wordt de weerbaarheid niet vergroot. Ook operationele functies zijn essentieel voor het verbeteren van de weerbaarheid, veiligheid en zelfs certificering. Gelukkig zetten diverse agenda's van onder andere de ministeries van Justitie & Veiligheid en Economische Zaken & Klimaat hier steeds steviger op in. Het blijft een aandachtpunt om hier blijvend in te investeren in publiek – privaat verband. Neem daarom ook de inzet van (financiële) middelen in algemene termen op in de uitvoeringswet cyberbeveiligingsverordening. Zo kan het fungeren als een "vangnet", zodat wordt voorkomen dat initiatieven en samenwerkingen die de weerbaarheid en veiligheid vergroten stranden wegens gebrek aan (financiële) middelen.

Cyberveilig Nederland pleit om de inzet van (financiële) middelen die een directe bijdrage leveren aan de weerbaarheid, veiligheid en certificering op te nemen in de uitvoeringswet cyberbeveiligingsverordening zodat publiek – private samenwerking verder wordt gestimuleerd.

Ik hoop u hiermee voldoende te hebben geïnformeerd.

Met vriendelijke groet,

Cyberveilig Nederland

Deze brief wordt ook ondersteund door Stichting Digitale Infrastructuur Nederland (DINL)