Ministerie van Economische Zaken en Klimaat
T.a.v. hare excellentie mr. drs. M.C.G. Keijzer
Bezuidenhoutseweg 73
2594 AC Den Haag

Verstuurd via: https://www.internetconsultatie.nl/regelingtelecomveiligheid

Onderwerp: Zienswijze Regeling veiligheid en integriteit telecommunicatie

Voorburg, 16 december 2020

Geachte excellentie, geachte mevrouw Keijzer,

Huawei Technologies (Netherlands) B.V. (hierna “Huawei”) maakt graag gebruik van de mogelijkheid om haar zienswijze over de voorgenomen ministeriële regeling inzake veiligheid en integriteit telecommunicatie (hierna: “Regeling”) met u te delen.

Huawei wil haar waardering uitspreken voor de huidige op feiten gebaseerde benadering, welke consistent is met de ENISA 5G risico evaluatie en de EU 5G Toolbox. Huawei onderschrijft het EU 5G Toolbox raamwerk en zal de Nederlandse mobiele operators ondersteunen om te voldoen aan de onderhavige Regeling. We willen ook benadrukken dat elke leveranciersbeoordeling niet alleen gebaseerd moet zijn op feiten, maar ook op het consistent volgen van objectieve principes en het handhaven van technische criteria, om een eerlijk en effectief ondernemersklimaat te creëren.

Op basis van meer dan 30 jaar telecommunicatie ervaring willen wij graag onze inzichten ten aanzien van de voorgestelde 19 organisatorische en technische veiligheidsmaatregelen met jullie delen. Doordat de duiding van kritische netwerkonderdelen door de overheid als vertrouwelijk wordt beschouwd en een multi-interpretabele definitie over ‘aanpalende onderdelen’ (artikel 1 sub c van de Regeling) is geïntroduceerd, zijn wij van mening dat het voor alle leveranciers moeilijk is om de volledige impact van de Regeling te analyseren.

Naar aanleiding van onze analyse vinden wij dat in samenwerking met de Nederlandse operators aan de in de Regeling opgenomen beheersmaatregelen kan worden voldaan. Daarnaast zien we enkele mogelijkheden tot verbetering voor een meer efficiënte en toekomstbestendige implementatie.

Vertrouwen door certificering en standaarden

Om de netwerk operators te faciliteren om aan de verplichte product- en software assessments te voldoen, zoals in de bijlage behorend bij de Regeling wordt genoemd (hierna: “Bijlage”) onder categorie D, beheersmaatregel 3, heeft Huawei cyber security test centra gebouwd. In deze centra kunnen onze klanten en andere stakeholders de veiligheid van onze producten valideren, inclusief bron code validatie.

Om te voorkomen dat er product- en software assessments moeten plaatsvinden voor ieder product, operator en land, willen we het ministerie voorstellen om het certificeringsproces zoals die in de uitvoeringswet cyberbeveiligingsverordening is opgenomen in overweging te nemen. Huawei ondersteunt de inzet van de EU om de veiligheidsevaluatie en certificeringsstandaarden naar hetzelfde hoge niveau te brengen.

De rol van de EU en haar lidstaten zal versterkt worden door deze certificering en daarmee gepaard gaande open en transparant toezicht. Certificering zal onze klanten in Nederland en daarbuiten voorzien van goed onderbouwd bewijsmateriaal als het gaat om de kwaliteit en veiligheid van de producten van alle telecomleveranciers. Op het moment dat de EU frameworks, zoals NESAS/SCAS, gereed zijn, zal Huawei haar producten volgens deze standaarden laten certificeren.

Standaardisatie en certificering zijn het meest effectieve middel om te komen tot op feiten gebaseerde veiligheidsmaatregelen en bieden tevens voordelen voor zowel de operators als de gehele telecommunicatie industrie. Pentesting is een best practice welke door de security teams van operators en onafhankelijke derde partijen worden uitgevoerd na integratie van onze producten in het operator netwerk. Huawei onderschrijft deze manier van werken: telecommunicatie behoort immers tot een mondiale industrie waarin internationale veiligheidsstandaarden nodig zijn. Het definiëren en toepassen van specifieke eisen per leverancier zal niet zorgen voor een veiliger telecommunicatie netwerk.

Voorgestelde aanpassingen ten aanzien van de Regeling

Enkele maatregelen zoals gedefinieerd in deze Regeling zijn naar onze mening te gedetailleerd en daarmee mogelijk niet toekomstbestendig. Als voorbeeld willen we de beveiligingssterkte van tenminste 112 bits noemen zoals die in de Bijlage wordt genoemd onder categorie B, beheersmaatregel 3, implementatievereiste a. Huawei stelt voor om de standaarden te gebruiken die worden gedefinieerd en ontwikkeld door 3GPP en richtlijnen in de EU 5G toolbox. Door deze internationale standaarden aan te nemen, kan regelgeving flexibel en toekomstbestendig worden ingezet.

Als tweede zorgt de gekozen vertrouwelijkheid van informatie tussen de overheid en de operators voor onzekerheid voor alle leveranciers als het gaat om de definitie van kritieke onderdelen van een openbaar elektronisch communicatienetwerk, aangevuld met toekomstige onbekende implementatievereisten vanuit de AMvB inzake veiligheid en integriteit telecommunicatie.

Met name de introductie en definitie van ‘aanpalende onderdelen’ (artikel 1 onder c) in de Regeling lijkt overbodig en is niet duidelijk. Naar onze mening is binnen de core 5G architectuur zoals gedefinieerd in 3GPP TS33.501 een duidelijke richting bepaald waarin alle componenten en communicatiepaden in het netwerk (management, controle en data) worden gescheiden om op deze manier adequate veiligheidscontroles te bewerkstelligen. Het toepassen van deze standaard zorgt al voor de noodzakelijke richtlijn voor nu en in de toekomst.

Tevens geeft de management maatregel weer, onder categorie B, beheersmaatregel 1 van de Bijlage, dat de operator de technische netwerkinfrastructuur moet scheiden in fysieke en/of logisch gescheiden netwerken waarvan de koppelvlakken actief moeten worden beschermd. De maatregel lijkt in contradictie te zijn met de definitie van ‘aanpalende onderdelen’. Gebaseerd op de bovengenoemde beheersmaatregel moet de operator namelijk al een zorgvuldige netwerkscheiding aanbrengen om de risico’s ten aanzien van de kritieke onderdelen te verlagen. Huawei is dan ook van mening dat de demarcatie van het netwerksegment van de kritieke onderdelen tot de verantwoordelijkheid van de Nederlandse operators kan behoren en er zo geen aparte definitie van aanpalende onderdelen benodigd is.

Conclusie

Allereerst wil Huawei benadrukken dat security de hoogste prioriteit heeft binnen ons bedrijf en een integraal onderdeel is van alle interne processen (Security by Design). Dit is dan ook de reden dat we van mening zijn dat een helder en transparant regelgevingskader nodig is, gebaseerd op feiten en (internationale) standaarden.

Door het creëren van een voorspelbaar en gelijk speelveld voor alle leveranciers kan Nederland haar koploperspositie op het gebied van digitalisering en cyber security behouden en verder uitbouwen. Dit is van fundamenteel belang voor een voorspoedige economische groei en herstel na COVID-19.

Naar onze mening zorgt de introductie van de term ‘aanpalende onderdelen’ voor meer onnodige onzekerheid en lijkt deze tevens overbodig gezien de voorgestelde maatregel en implementatievereiste aan de operators om een fysieke en logische scheiding van netwerksegmenten te hanteren. De wereldwijde standaarden en de implementatie daarvan binnen de omgeving van de operator, geven bovendien al veel richting aan de veiligheidsdoelstelling door zowel de logische als de fysieke scheiding van de onderdelen en de gestandaardiseerde interfaces.

Huawei blijft actief samenwerken met de industrie om de wereldwijde standaarden binnen de 3GPP werkgroepen en andere relevante standaardisatieorganen verder te brengen.

Huawei zal haar dialoog met de industrie, de overheid en het ecosysteem in Nederland blijven onderhouden en verbeteren, om de inzet en het beheer van innovatieve en veilige telecommunicatie netwerken te garanderen.

Wij kijken er naar uit om met het ministerie in gesprek te gaan en onze zienswijze nader toe te lichten.

Hoogachtend,

Steven Cai

CEO

Huawei Technologies (Netherlands) B.V.

Huawei Technologies (Netherlands) B.V.
Stationsplein 4
2275 AZ Voorburg

Tel. 020-4300808
Fax. 020-4300888
www.huawei.com

KvK number: 34219858
VAT number: NL813910250B01