Reactie NIS2 Consultatie Huawei Technologies B.V.

Huawei is een gerenommeerd bedrijf op het gebied van cybersecurity. Onze onderneming speelt een actieve rol in het ontwikkelen van internationaal erkende veiligheidsstandaarden[1] en streeft succesvol na aan standaarden en (lokale-) cyberwetgeving te voldoen. In o.a. ons cybersecurity and transparency center in Brussel gaan we actief de dialoog aan en delen we onze expertise met relevante partijen. Deze expertise is opgedaan middels onze R&D-activiteiten en onze werkzaamheden in de 170 markten waarin onze onderneming actief is, in Nederland alweer 20 jaar, op het gebied van telecomnetwerken, Enterprise solutions, consumentenelektronica en duurzame energieoplossingen. Door onze kennis en expertise te delen dragen we bij aan het versterken van de Cbw en daarmee de cybersecurity in Nederland.

NIS2 is gebaseerd op de richtlijn inzake netwerk- en informatiebeveiliging uit 2016, maar met een breder toepassingsgebied en een grotere reeks vereisten. Dit is een noodzakelijke en zeer positieve stap voorwaarts voor het Europese cyberbeveiligingsecosysteem, waardoor het niveau van cyberbeveiliging in alle sectoren en op de markt als geheel wordt verhoogd. Een zero-trust architectuur[2] is hierin essentieel.

Cybersecurity is van essentieel belang in een moderne samenleving en is een van de belangrijkste pijlers om de veiligheid van een (digitale) economie te waarborgen. Juist daarom is cybersecurity een gezamenlijke verantwoordelijkheid van alle betrokken partijen. Alleen door gezamenlijk te werken aan een optimaal niveau van cybersecurity blijft Nederland beschermd.

Digitale transformatie en cyberbeveiliging gaan echter hand in hand. Door de meest recente technologieën in te zetten is het mogelijk om de gegevens van burgers en organisaties het best te beschermen. Dit kan alleen als er wordt ingezet op bescherming van de internationale toeleveringsketen van hardware, software & netwerktechnologie. Dit kan door *technologie neutraal* te acteren.

Voor onze onderneming zijn er ook directe belangen. Deze betreffen met name de harmonisatie tussen EU markten. Wij zien dat een aantal zaken onduidelijk zijn. Graag lichten we het belang toe van objectieve en verifieerbare cybersecurity t.o.v. niet technische criteria.

I. **Proces**

Secundaire wetgeving voor deze wet is nog in ontwikkeling. Hierdoor zijn er een aantal open einden die het momenteel moeilijk maken de impact van de wet te overzien. Deze secundaire wetgeving zal rekening moeten houden met het uitvoeringsbesluit van de EU Commissie over artikelen 21 en 23 van de NIS2-richtlijn waarvan het concept deze zomer wordt verwacht. Met inachtneming van de terechte grondigheid van het wetgevingsproces zijn er zorgen of deze wet tijdig kan worden afgerond.

Verzoek: Zal, en zo ja, wanneer wordt de secundaire wetgeving ter publieke consultatie aangeboden?

II. **Harmonisatie & nationale koppen**

In algemene zin valt op dat in de transponeringstabel is vermeld bij welke artikelen van de richtlijn Nederland de beleidsruimte heeft om nadere regels te stellen, maar dat niet nader is

[1] https://www.huawei.com/en/trust-center/transparency/standard-certification

[2] Zero-Trust Architectuur - Een zero-trust architectuur is een beveiligingsconcept waarbij ervan wordt uitgegaan dat geen enkele entiteit binnen of buiten de netwerkperimeter te vertrouwen is. Dit betekent dat alle toegangspogingen voortdurend worden geverifieerd, ongeacht of ze van binnen of buiten het netwerk komen. De basisprincipes van zero-trust zijn: 1. Verifieer expliciet: Controleer voortdurend de identiteit en toegangsrechten van gebruikers en apparaten. 2. Beperk toegang: Geef gebruikers en apparaten alleen toegang tot de middelen die ze nodig hebben voor hun werk. 3. Geef nooit vertrouwen op basis van locatie: Behandel interne en externe netwerken gelijkwaardig en voer dezelfde strenge controles uit voor beide.

uitgewerkt of en om welke redenen Nederland hiervan gebruik heeft gemaakt. Aanbevolen wordt om voor iedere bepaling waarin dit het geval is een toelichting op te nemen in de memorie van toelichting.

Mede omdat er secundaire regelgeving wordt verwacht zijn er in het huidige voorstel een beperkt aantal aanvullingen. Anders dan in de directe buurlanden Duitsland & België kiest de Nederlandse regering er bijvoorbeeld voor alle gemeenten toe te voegen aan de essentiële entiteiten lijst. Ook stelt het wetsvoorstel verplichtingen vast die verder gaan dan die in NIS2. Deze hebben betrekking op:

1. Algemene beveiligingsaudits: bevoegdheid voor de toezichthoudende autoriteit om de resultaten van een onderzoek binnen een redelijke termijn op te vragen en om de aanbevelingen voortvloeiend uit het onderzoek binnen een redelijke termijn te implementeren. Verdere regels kunnen worden gesteld in secundaire wetgeving.

2. Ad hoc beveiligingsaudits: bevoegdheid om een essentiële entiteit aan een ad hoc beveiligingsaudit te onderwerpen wanneer deze niet heeft voldaan aan andere verplichtingen die bij of krachtens de wet zijn opgelegd.

Verzoek: Wij maken hier een kanttekening over de bevoegdheden en proportionaliteit voor het bedrijfsleven. Zodoende vragen wij hier om een nadere toelichting over de regeldruk voor het bedrijfsleven in de memorie van toelichting, waarin wordt ingegaan op de aanleiding voor uitbreiding van de genoemde toezichtsbevoegdheden ten opzichte van de richtlijn.

Verder zijn er nog beperkt variaties te melden in het huidige wetsvoorstel. Het wetsvoorstel bevat echter wel al een basis voor delegatie door of krachtens een algemene maatregel van bestuur om verdere regels vast te stellen om de meldingsverplichting uit te voeren. Deze bepaling biedt de mogelijkheid om de regels verder te specificeren met betrekking tot aanvullende aspecten en drempelwaarden die in acht worden genomen om te bepalen of er sprake is van een significante gebeurtenis, waarin onderscheid kan worden gemaakt tussen sectoren en sub-sectoren, en de gegevens die het vroegtijdig waarschuwing, notificatie, tussentijds rapport en eindrapport in ieder geval moeten bevatten en de wijze waarop dit wordt gedaan.

Deze delegatiebasis zal worden gebruikt voor een ministeriële regeling van de verantwoordelijke minister, na overleg met de minister van Justitie en Veiligheid en de sector, om regels vast te stellen over meldbare incidenten per sector, subsector of type entiteit. De overheid zal ook de implementatiewet uitvoeren die de Europese Commissie vaststelt voor cybersecuritymaatregelen en rapportageverplichtingen. De nadere regels zullen in overeenstemming moeten zijn met het uitvoeringsbesluit van de Commissie.

Verzoek: Wij vragen of het Ministerie nader uiteenzet op welke wijze de nadere regels op het uitvoeringsbesluit van de Commissie zullen worden afgestemd en welk proces daarbij wordt gehanteerd.

III. **Uitvoerbaarheid & evenredigheid**

In de memorie van toelichting is op pagina 54 het aantal entiteiten genoemd waarop de wet betrekking heeft en wat de verwachte implementatiekosten zijn:

1. *Het aantal organisaties dat onder dit wetsvoorstel valt is van significant grotere orde dan onder de Wbni. Momenteel wordt dit aantal **geschat** op ongeveer 8.100 entiteiten.*

2. *In de impact assessment opgesteld door de Europese Commissie, wordt geschat dat nieuwe entiteiten een toename van maximaal 22% aan ICT-beveiligingskosten*

benodigd hebben om aan de eisen te voldoen. Voor entiteiten die reeds onder de Wbni vielen, is de schatting maximaal een toename van 12%. Hierbij dient wel vermeld te worden dat de impact assessment is geschreven op basis van het originele voorstel, dat op sommige punten afwijkt van de uiteindelijk aangenomen richtlijn;

Onze tussenconclusie is dat enerzijds het aantal entiteiten nog op een schatting berust en omdat de impact assessment op basis van een oudere versie is gedaan er een zekere mate van onvoorspelbaarheid is. Daarbij is het van belang te kijken naar de uitvoerbaarheid van de wet en de arbeidsmarkttekorten in de ICT-sector:

3. De ICT-sector kampt met aanzienlijke arbeidsmarkt tekorten. Tot 2030 wordt in Nederland een tekort van 300.000 fulltime-equivalenten (fte) verwacht[3]. Deze tekorten kunnen de uitvoerbaarheid van de NIS2-richtlijn ernstig belemmeren, aangezien er simpelweg niet genoeg gekwalificeerde professionals beschikbaar zijn om aan de verhoogde eisen te voldoen. Cybersecurity is een complex vakgebied dat gespecialiseerde kennis vereist. Kleinere entiteiten hebben moeite om professionals met de benodigde expertise aan te trekken en te behouden, wat leidt tot capaciteitsproblemen. Volgens Deloitte[4] legt de NIS2-richtlijn risicobeheermaatregelen op die een hoog niveau van expertise vereisen, wat moeilijk te handhaven is voor kleinere entiteiten;

Kosten en beschikbaarheid van middelen spelen hierin een rol. Om een beeld te krijgen bij de kosten voor het bedrijfsleven heeft Huawei SPC[5] gevraagd dit te onderzoeken. Dit onderzoek voegen wij toe als bijlage. Uit dit onderzoek blijkt dat de kosten per jaar in Nederland ongeveer 1,514 miljard euro bedragen. Voor nieuwe sectoren (bijv. sectoren die niet onder Wbni vallen) zullen de kosten hoger zijn dan voor sectoren die er al onder vallen.

Aanbeveling: Vanwege bovenstaand plaatsen wij een kanttekening bij de uitvoerbaarheid en evenredigheid. Wij doen de suggestie om niet meer entiteiten aan te wijzen dan qua uitvoerbaarheid realistisch is en het exacte aantal concreter te maken.

IV. **Wijziging begrip bestuursorgaan**

In het huidige wetsvoorstel wordt voor het begrip "bestuursorgaan" verwezen naar de leden van het bestuur zoals bepaald in het Nederlandse Burgerlijk Wetboek. Het ontwerp wijzigde de bewoording van de NIS2-richtlijn ("management body") naar "bestuur van de relevante essentiële entiteit of belangrijke entiteit". Het Nederlandse Burgerlijk Wetboek bevat geen definitie van het bestuur. Het bestuur in de zin van het Nederlandse Burgerlijk Wetboek bestaat uit de personen die als zodanig zijn benoemd. Behoudens beperkingen in de statuten is het bestuur verantwoordelijk voor het beheer van de vennootschap.

Belangrijk is dat indien een rechtspersoon lid is van het bestuur van een essentiële entiteit of een belangrijke entiteit, de verantwoordelijkheden en opleidingsverplichtingen hoofdelijk rusten op iedere persoon die bestuurder is van die rechtspersoon.

V. **Aansprakelijkheid**

De toezichthoudende autoriteit kan, in geval van een overtreding van een verplichting onder deze wet, handhavingsmaatregelen nemen tegen de entiteit die de overtreding begaat, maar ook tegen degenen die worden beschouwd als de principaal van de overtreding die door de entiteit is begaan en degenen die feitelijk het verboden gedrag hebben geleid. Dit

[3] https://www.nldigital.nl/nieuws/minister-adriaansens-ontvangt-aanvalsplan-chronisch-tekort-icters/
[4] https://www2.deloitte.com/nl/nl/pages/risk/articles/the-nis2-directive.html
[5] Kwantitatieve impact van de kosten van NIS2 op de economie van Nederland, rapport van SPC networks, 2024.

kunnen leden van het bestuur zijn, maar ook andere personen binnen de entiteit met beslissingsbevoegdheid. Over het algemeen zijn alle sancties die op basis de Awb kunnen worden toegepast van toepassing op overtredingen van de (ontwerp)wet.

De bestuurlijke sancties zijn onder andere beveiligingsonderzoek, bekendmaking van de beschikking, bindende beschikking, bestuurlijke dwang, bestuurlijke boete.

Strafrechtelijke sancties kunnen van toepassing zijn in gevallen van overtredingen van de (ontwerp)wet die ook als strafbaar feit kwalificeren.

Op basis van artikel 70, 70a & 80 is het echter onduidelijk of de beslissing van de bevoegde autoriteit om een beveiligingsonderzoek te eisen een beslissing is op grond van het bestuursrecht en open staat voor bezwaar en beroep door de onderneming.

Aanbeveling: Wij bevelen aan dat voor de genoemde beslissingen van de bevoegde autoriteit wordt bepaald dat deze zijn te beschouwen als besluit in de zin van de Awb waartegen bezwaar en beroep open staat. Dit geldt te meer aangezien Nederland kiest voor een scherpere invulling van de toezichtinstrumenten ten opzichte van de richtlijn als hiervoor omschreven. Dan dienen ook de gebruikelijke rechtsmiddelen open te staan zonder dat hierover onzekerheid bestaat.

VI. **(Bestuurlijke) Sancties**

De sancties die zijn vastgesteld onder het wetsvoorstel met betrekking tot de implementatie van Cbw zijn zowel bestuurlijk als tot op zekere hoogte strafrechtelijk. De hoogte van de mogelijke sancties hangt af van de overtreding. Het maximale bedrag is ten minste 2% van de totale wereldwijde jaaromzet van de groep in het voorgaande boekjaar.

Het niet voldoen aan de verplichtingen vermeld in artikel 77 (bestuurlijke boetes voor essentiële entiteiten) en artikel 88 (bestuurlijke boete voor domeinnaamregistratieservices) resulteert in:

1. Voor essentiële entiteiten: een bestuurlijke boete van maximaal 10.000.000 euro of 2% van de totale wereldwijde jaaromzet van de onderneming, exclusief belastingen (welk bedrag hoger is).

2. Voor belangrijke entiteiten: een bestuurlijke boete van maximaal 7.000.000 euro of 1,4% van de totale wereldwijde jaaromzet van de onderneming, exclusief belastingen (welk bedrag hoger is).

Aanbeveling: Gezien de serieuze omvang van de sancties is het belangrijk om eerdergenoemde evenredigheid en uitvoerbaarheid nader te onderbouwen.

VII. **Objectieve en verifieerbare cybersecurity**

De toenemende complexiteit van wereldwijde toeleveringsketens vereist een proactieve aanpak om potentiële risico's te identificeren en te beperken. Vooral cyberbedreigingen vormen een groot gevaar voor de integriteit en functionaliteit van deze onderling verbonden systemen. Om ervoor te zorgen dat de toeleveringsketen weerbaar is tegen de veranderende cyberbedreigingen, zijn duidelijke richtlijnen voor het uitvoeren van grondige risicobeoordelingen van de toeleveringsketen van cruciaal belang. Weliswaar met als uitgangspunt om technologie-neutraal te kunnen opereren.

Om het concurrerend en innovatief vermogen van de sector te behouden voor de Nederlandse maatschappij is het noodzaak dat het vertrouwen in objectieve, transparante

internationale standaarden en certificeringen[6] (ETSI, ENISA etc.) als uitgangspunt wordt genomen en niet wordt ondergraven door geopolitieke aspecten. Standaarden en certificeringen komen met reden tot stand; op basis van uitgebreide dialoog tussen bedrijven, overheden en specialisten. Deze hebben alle potentie om meer dan voldoende objectieve handvatten te bieden voor cybersecurity.

Verzoek: We vragen de Nederlandse wetgever:

a. Aandacht voor duidelijke technische objectieve, transparante internationale standaarden en certificeringen zoals normen, binnen het toepassingsgebied van Cbw. Dit voorkomt dubbelzinnigheid en bevordert de transparantie van de toeleveringsketen. Dit kan op zijn beurt leiden tot meer efficiëntie en voorkomt marktverstoringen.

b. Erkenning van bestaande internationale en EU-brede standaarden dan wel normen, als middel om de naleving van cyberveiligheidseisen en keteneisen onder de wet aan te tonen.

Conclusie
Wij verwelkomen het voorstel en zien een sterke verbetering van de nationale Cyberveiligheid. Dit steunen wij van harte. We vragen de regering zoveel mogelijk aan te sluiten bij EU-regels om de harmonisatie van wetgeving ten goede te komen. Nationale koppen zijn onwenselijk en drijven de kosten van de Cbw op en raken de handhaafbaarheid. Het voorstel lijkt nog niet afgebakend over het aantal entiteiten en de kosten kunnen worden verduidelijkt. Dit komt mede omdat de secundaire regelgeving nog ontbreekt. Wij vernemen graag wanneer deze ter consultatie wordt aangeboden. Tot slot vragen wij te allen tijde om technologie neutrale cybersecurity die verifieerbaar is op objectieve, transparante internationale standaarden, certificeringen en op basis van een zero-trust architectuur.

Tot slot danken we de Nederlandse wetgever voor de gelegenheid onze zienswijze te delen middels deze consultatie en zijn we beschikbaar voor nader dialoog.

Kind regards,

Guy Hendricks
Head of Regulatory & Government Affairs

Jaap Meijer
Cyber Security & Privacy Officer

Huawei Technologies (Netherlands) B.V.
Laan van Vredenoord 56
2289 DJ Rijswijk, The Netherlands
KVK: 34219858
https://www.huawei.com/nl/

[6] https://www.huawei.com/en/trust-center/5g-cyber-security