Aan:
Ministerie van Justitie en Veiligheid
t.a.v. Directie Cybersecuritybeleid
Den Haag

Onderwerp: Reactie MSP ISAC op internetconsultatie Cyberbeveiligingswet en -besluit
Geachte heer/mevrouw,

Namens het collectief van Managed Service Providers (MSP's) die diensten verlenen aan de vitale infrastructuur en overheid, verenigd in het MSP ISAC willen wij u hartelijk danken voor het openstellen van de internetconsultatie over het concept-Cyberbeveiligingsbesluit, behorend bij de implementatie van de Cyberbeveiligingswet. De mogelijkheid tot inspraak waarderen wij zeer, en wij leveren dan ook graag onze gezamenlijke bijdrage.

Wie wij zijn
De MSP ISAC is een informeel samenwerkingsverband van Managed (Multi) Service Providers in Nederland die actief zijn in het leveren van essentiële en digitale diensten aan een breed scala van sectoren – van zorg tot industrie en van financiële instellingen tot overheidsorganisaties. Binnen deze Information Sharing and Analysis Community (ISAC), opererend onder de koepel van het Nationaal Cyber Security Centrum (NCSC), delen wij op gestructureerde wijze actuele dreigingsinformatie, kwetsbaarheden en best practices op het gebied van cybersecurity. Onze leden hebben dagelijks te maken met het operationeel beveiligen van netwerken, systemen en data van derden, en hebben daardoor een unieke kijk op de praktische uitvoerbaarheid van wet- en regelgeving in het cybersecuritydomein.

Waardering voor het voorliggende besluit
Wij willen onze waardering uitspreken voor de wijze waarop het Cyberbeveiligingsbesluit is vormgegeven en de zorgvuldigheid waarmee het juridisch en beleidsmatig is onderbouwd. Het is duidelijk dat er veel aandacht is besteed aan de aansluiting bij de NIS2-richtlijn, en wij herkennen ons in de richting die wordt ingeslagen. De expliciete aandacht voor proportionaliteit, risico gebaseerde benadering en de rol van toeleveranciers sluit aan bij de dagelijkse realiteit waarin wij opereren.

Onze inbreng
Onze reactie omvat inhoudelijke aandachtspunten met betrekking tot zowel het ontwerpbesluit (AMvB) als de bijbehorende nota van toelichting. Deze aandachtspunten zijn gestructureerd opgenomen in twee overzichtelijke tabellen, waarin per artikel of relevant onderdeel onze opmerkingen, duidingen en aanbevelingen zijn opgenomen (zie tabel 1 en tabel 2). Op die manier hopen wij helder en constructief bij te dragen aan de verdere totstandkoming en verfijning van het besluit.

Consultatiereactie MSP ISAC – Conceptbesluit Cyberbeveiligingswet (AMvB)

Artikel / Paragraaf	Onderdeel / Citaat	Opmerking MSP ISAC	Aanbeveling / Voorstel tot wijziging
Artikel 6	Beleid over beveiliging van netwerk- en informatiesystemen	Nu onder NIS2 het bestuur hoofdelijk aansprakelijk is, is het opmerkelijk dat geen expliciete goedkeuring van het beleid door het bestuur wordt vereist.	Voeg aan het artikel toe dat het vastgestelde beveiligingsbeleid aantoonbaar door het bestuur wordt goedgekeurd of ondertekend. Dit sluit aan bij de bestuurlijke verantwoordelijkheden zoals benoemd in NIS2.
Artikel 9	Bedrijfscontinuïteit en crisisbeheer	De huidige tekst suggereert dat het bedrijfscontinuïteitsplan bij elk incident geactiveerd moet worden. In de praktijk wordt een dergelijk plan alleen geactiveerd bij ernstige verstoringen. Voor overige incidenten is het reguliere incidentmanagementproces leidend.	Herformuleer de bepaling zodat het plan wordt geactiveerd bij *ernstige* incidenten of wanneer vooraf vastgestelde criteria zijn bereikt.
Artikel 10, lid 2	Beveiliging toeleveringsketen	De formulering “waar mogelijk” bij het maken van afspraken met leveranciers biedt ruimte voor interpretatie en mogelijk vrijblijvendheid, terwijl de toeleveringsketen cruciaal is voor de beveiliging.	Schrap “waar mogelijk” of specificeer onder welke omstandigheden afwijking mogelijk is. Maak het uitgangspunt dat afspraken schriftelijk of aantoonbaar vastgelegd worden.
Artikel 17, lid 5	Attenderingen, adviezen en informatie	Strikte toepassing van dit artikel kan leiden tot aanzienlijke administratieve lasten. De tekst suggereert dat voor elk ontvangen bericht – ook algemene informatie of attenderingen – schriftelijk moet worden vastgelegd of deze beoordeeld is. Voor MSP’s, waar dagelijks honderden berichten verwerkt worden, is dit disproportioneel en praktisch onuitvoerbaar.	Beperk de documentatieverplichting tot berichten die expliciet gericht zijn aan de entiteit of waarin sprake is van specifieke relevantie. Geef in de toelichting aan dat algemene dreigingsinformatie hier niet onder valt.
Artikel 20, lid 5	Doel van de training	In de formulering “de gevolgen daarvan voor de diensten die door de entiteit worden verleend” wordt geen rekening gehouden met entiteiten die naast diensten ook producten leveren. In bepaalde sectoren (bijv. voedsel, water) is dit onderscheid relevant.	Breid de reikwijdte van dit artikel uit met “…en, indien van toepassing, de producten die door de entiteit worden geleverd”.
Artikel 28, lid 3(b)	Verstrekking overige informatie	Een MSP beheert veel domeinnamen namens klanten. De verplichting tot verstrekking van deze gegevens is onduidelijk: moeten alle domeinen worden gedeeld of alleen domeinen die direct aan de dienstverlening van de MSP zijn gekoppeld?	Specificeer welke domeinnamen verstrekt moeten worden (bijv. domeinen die door de MSP zelf worden gebruikt voor dienstverlening), en overweeg een toevoeging over het onderscheid tussen eigenaar en technisch beheerder.
Artikel 30	Bewaring van persoonsgegevens	Volgens de letterlijke tekst van lid 1 en 2 mag informatie over een persoon niet langer dan 60 maanden worden bewaard of	Verwijs expliciet naar de toepasselijkheid van de AVG/GDPR en maak duidelijk dat de

Artikel / Paragraaf	Onderdeel / Citaat	Opmerking MSP ISAC	Aanbeveling / Voorstel tot wijziging
		ongewijzigd blijven. In de praktijk (bijv. bij langdurig dienstverband) is dit niet haalbaar.	bewaartermijnen hieraan ondergeschikt zijn of hiermee in overeenstemming moeten zijn.

Consultatiereactie MSP ISAC – Nota van Toelichting bij het Cyberbeveiligingsbesluit

Artikel / Paragraaf	Onderdeel / Citaat	Opmerking MSP ISAC	Aanbeveling / Voorstel tot wijziging
Artikel 17 / Artikel 14 van de toelichting	Verplichting tot documenteren van afweging na attendering op informatie	Er is momenteel onvoldoende duidelijkheid over het verschil tussen het gericht attenderen van een entiteit op informatie en het algemeen beschikbaar stellen van informatie. Indien dit onderscheid niet helder wordt gemaakt, ontstaat het risico dat organisaties geacht worden voor elk ontvangen bericht – ook algemene dreigingsinformatie – een schriftelijke impactanalyse op te stellen. Voor securityteams die dagelijks honderden meldingen en signalen verwerken, is dit onwerkbaar en leidt het tot aanzienlijke en onnodige regeldruk.	Verduidelijk in de nota van toelichting of in uitvoeringsrichtlijnen wanneer sprake is van “gericht attenderen” en wanneer van algemene informatie. Neem expliciet op dat enkel relevante, gerichte informatie documentatieplichtig is.
Bijlage II (art. 7 lid 2) – punt j	“wanneer gepast, het gebruik van multifactor-authenticatie- of continue-authenticatieoplossingen...”	De zinsnede “wanneer gepast” wekt de indruk dat MFA optioneel is. In het huidige dreigingslandschap is MFA of een sterker alternatief essentieel. Het ontbreken ervan vormt in de meeste gevallen een ernstige verzwakking van de beveiliging.	Formuleer MFA als normatief uitgangspunt, bijvoorbeeld: “het gebruik van multifactor-authenticatie- of continue-authenticatieoplossingen, tenzij gemotiveerd aangetoond wordt dat dit niet proportioneel is”.
Bijlage II (artikelen 7a/7b van Richtlijn 2024/2690)	Definitie "significant incident"	Door het ontbreken van een impactcriterium (zoals aard van de dienst of ernst van verstoring), bestaat het risico dat MSP’s disproportioneel incidenten gaan melden. Richtlijn 2022/2555 (art. 23) hanteert bredere criteria zoals financiële schade en ernstige operationele verstoring – deze ontbreken in het besluit.	Harmoniseer de terminologie en beoordelingscriteria met de bredere, proportionele benadering uit NIS2 artikel 23. Licht dit ook toe in de nota van toelichting.
Toelichting – Paragraaf "Gevolgen"	Kostenraming en impact meldplicht	De toelichting onderschat de governance-impact van de meldplicht op MSP’s. Door de CBW ontstaat een zelfstandige meldplicht, los van die van klanten. Dit vereist structurele afstemming met klanten, wat per klant minstens één uur tijdsinvestering betekent voor zowel klant als MSP.	Neem expliciet op dat de CBW-meldplicht leidt tot extra governance-afstemming. Herzie de kostenraming op dit punt met een realistische inschatting van benodigde tijd en capaciteit.

Artikel / Paragraaf	Onderdeel / Citaat	Opmerking MSP ISAC	Aanbeveling / Voorstel tot wijziging
Toelichting – Paragraaf "Gevolgen"	Verhouding tussen meldplicht klant en MSP	De CBW introduceert een duale meldplicht. In tegenstelling tot de AVG, kunnen onder de NIS2 zowel toeleveranciers als klanten meldplichtig zijn. Tegelijkertijd bestaat onduidelijkheid over het delen van klantinformatie door DSP's.	Geef aan dat wetgeving vraagt om duidelijke contractuele afspraken over meldverantwoordelijkheid. Neem op dat DSP's zorgvuldig moeten omgaan met klantvertrouwelijkheid.
Toelichting – Paragraaf "Gevolgen"	Onzekerheid voor autoriteiten bij incidentanalyse	Door afzonderlijke, mogelijk ongecoördineerde meldingen van MSP's en klanten kan het voor autoriteiten zoals het NCSC onduidelijk zijn of meldingen samenhangen. Dit leidt tot risico op verwarring, met name in crisissituaties.	Overweeg een proces of richtlijn, bijvoorbeeld via het NCSC, om meldingen van gerelateerde incidenten beter te correleren en inzichtelijk te maken.
Toelichting – Paragraaf "Gevolgen"	Spanningsveld geheimhouding vs. meldplicht	De meldplicht kan in conflict komen met bestaande geheimhoudingsverplichtingen tussen MSP's en klanten. De wet biedt hierover onvoldoende duidelijkheid.	Geef aan hoe MSP's met deze spanning kunnen omgaan. Overweeg in wet of toelichting een juridische uitzondering of duiding op te nemen voor meldingen in het algemeen belang.
Toelichting – Paragraaf "Kosten"	Uurtarief van €58 per FTE	Het gebruikte uurtarief van €58 is niet realistisch voor MSP's. In de praktijk liggen de werkelijke kosten van een cybersecurity-FTE tussen de €150 en €200 per uur.	Pas het uurtarief aan op basis van marktconforme tarieven voor gespecialiseerde IT- en securityrollen.
Toelichting – Paragraaf "Kosten"	Kosten boardroomtraining	In de kostenraming voor boardroomtrainingen zijn alleen de trainingskosten meegenomen, niet de inzet van boardmembers zelf. Het gebruikte uurtarief is ook hier niet realistisch.	Voeg een realistische inschatting toe van indirecte kosten zoals boardtijd en voorbereiding. Herzie het gehanteerde uurtarief ook voor deze doelgroep.

Tot slot

Als MSP ISAC geloven wij sterk in publiek-private samenwerking als fundament van onze digitale weerbaarheid. Wij staan open voor verdere dialoog over dit onderwerp en hopen dat onze bijdrage als dienstverleners, met een centrale rol in het digitale ecosysteem, wordt meegenomen in de verdere beleidsvorming.

Met vriendelijke groet,

Namens de leden van het MSP ISAC,

Wijnand Goedhart | Voorzitter MSP ISAC