

Ministerie van Justitie en Veiligheid
Postbus 20301
2500 EH DEN HAAG

Datum: 29 maart 2025
Onderwerp: Reactie Schoonmakend Nederland op internetconsultatie
Cyberbeveiligingsbesluit en Ministeriële Regeling

Schoonmakend Nederland vindt het goed dat er aan de cybersecurity van Nederlandse bedrijven en organisaties wordt gewerkt met de Cyberbeveiligingswet. Dat is nodig gezien de sterk toenemende, internationale dreigingen. We merken ook dat veel van onze leden hier al mee bezig zijn.

Tegelijkertijd maken we ons zorgen over de lastendruk die deze wet kan geven aan onze leden. Een deel van de bedrijven in onze branche zullen te maken krijgen met deze wet via hun opdrachtgevers die direct onder de wet vallen (essentiële of belangrijke entiteiten) waarvan zij een directe leverancier zijn. We hebben dan ook met name aandacht voor het deel “toeleveringsketen” artikel 10. Hierop geven we graag onze reactie op de consultatie, in drie punten.

Definitie actueel

In het besluit wordt gesproken over het ‘actueel houden van de afspraken met de toeleveringsketen’¹. Wij vragen ons af wat dat voor consequenties zal hebben voor directe leveranciers waarvan is vastgesteld dat er een risico is. Voor het actueel houden van hun informatie en risico dienen de essentiële of belangrijke entiteiten contact te hebben met hun leveranciers. Er staat echter niet duidelijk met welke frequentie dit gevraagd wordt. Dagelijks, wekelijks, maandelijks of jaarlijks? Wij zouden jaarlijks een logische en haalbare frequentie achten.

Situatie-afhankelijke risicobeoordeling

De voorgestelde voorbeelden in artikel 10 van de nota van toelichting zijn twee uitersten. Het ene voorbeeld levert duidelijk geen risico op, het andere voorbeeld duidelijk wel. De issues zullen met name liggen rondom de scheidslijn waarbij het minder duidelijk is. Gezien de complexiteit van relaties tussen bedrijven, vergaande integraties en specifieke afspraken en de individueel te maken risicoanalyse is het praktisch onmogelijk om een duidelijke scheidslijn op papier te zetten. Dat is logisch.

Veel bedrijven geven elkaar toegang tot systemen via EDI en toegang tot werk- en productieruimtes. Deze verschillende vormen van toegang zijn vaak ook al contractueel afgesproken omdat er sprake is van vergaande integrator-oplossingen en Just-in-Time systemen die noodzakelijk zijn in de keten. Aangezien de scheidslijn niet

¹ Artikel 10, punt 3 uit het voorgestelde Cyberbeveiligingsbesluit

Schoonmakend Nederland
Bond Den Bosch
Pettelaarpark 130-B
5216 PV 's-Hertogenbosch
T 073 648 38 50

info@schoonmakendnederland.nl

IBAN NL18INGB0005023908
BTW NL0025.99.958.B01
KvK 40258433

schoonmakendnederland.nl

te maken is, zouden we liever geen concrete voorbeelden opnemen. De NIS2 bedrijven en organisaties zullen die in de praktijk zelf wel maken voor hun eigen specifieke situatie op basis van de verplichte risicoanalyse.

In plaats van voorbeelden stellen wij voor om te kiezen voor een situatie-afhankelijke risicobeoordeling. De risico's en bijbehorende maatregelen verschillen namelijk van leverancier tot leverancier. Door ruimte te bieden voor een individuele aanpak blijft het uitvoerbaar en beheersbaar voor mkb-bedrijven. Verder pleiten we voor een graduele beoordeling van risico's. Dat wil zeggen dat er bij lage risico's minder maatregelen moeten worden genomen dan bij hoge risico's. Een graduele aanpak zorgt ervoor dat de eisen proportioneel blijven en uitvoerbaar zijn voor verschillende leveranciers.

Schrappen vervanging leveranciers

In artikel 10 staat ook dat een entiteit moet beoordelen of het cyberbeveiligingsniveau dat een leverancier aanbiedt passend is, en dat er anders eventueel een andere leverancier moet worden gekozen. We verzoeken om te schrappen dat leveranciers vervangen zouden moeten worden bij onvoldoende naleving. Dit leidt tot onnodige onrust, kosten en complexiteit binnen de keten, waar niemand baat bij heeft.

In plaats van leveranciers te vervangen, pleiten wij voor het aangaan van een gesprek met leveranciers. Door dialoog en samenwerking kunnen risico's effectiever worden aangepakt zonder onnodige verstoring in de keten.