Reactie Cyber Weerbaarheidscentrum Brainport op Consultatie Cyberbeveiligingswet (NIS-2)

Dit is een gezamenlijke reactie vanuit het Cyber Weerbaarheidscentrum Brainport, een stichting waarin meer dan 100 bedrijven uit de High Tech Maakindustrie en toeleverende keten met elkaar samenwerken om meer cyberweerbaar te worden. Ten aanzien van de implementatie van de cyberbeveiligingsweten vragen wij het volgende:

- Meer duidelijkheid over of bedrijven wel of niet onder de Cyberbeveiligingswet vallen én wat er van bedrijven wordt verwacht in het kader van de Cyberbeveiligingswet;
- Consultatie op de nog te ontwikkelen en publiceren Algemene Maatregel van Bestuur;
- Aandacht voor het beperken van regeldruk voor alle bedrijven die direct of indirect te maken krijgen met de Cyberbeveiligingswet, bijvoorbeeld in de verdere uitwerking in de Algemene Maatregel van Bestuur;
- Dat één lid van het bestuur de gevraagde cyberkennis aantoonbaar heeft in plaats van alle leden een bestuur;
- Werken op basis van door de overheid aangegeven kaders, bijvoorbeeld voor governance en één standaard t.b.v. aantonen niveau van cyberweerbaarheid;
- Afstemming tussen verschillende ministeries en instanties m.b.t. de diverse wet- en regelgeving op het gebied van cyberveiligheid die op bedrijven afkomt.

Toelichting op reactie

Wij zijn er van overtuigd dat het goed is dat er meer wettelijke kaders komen als het gaat om cybersecurity. Dit zal meer bedrijven motiveren om de noodzakelijke stappen te zetten om hun ‘basis op orde’ te krijgen.

Duidelijkheid & consultatie AMvB

In de Cyberbeveiligingswet, zoals deze nu voorligt, is nog veel onduidelijk. Het is belangrijk dat er duidelijk wordt gemaakt welke bedrijven onder de Cyberbeveiligingswet vallen en wat er van bedrijven wordt verwacht. We realiseren ons dat er nog een Algemene Maatregel van Bestuur komt waarin de wet verder wordt uitgewerkt. Wij vragen de overheid dat hierop ook een internetconsultatie wordt gedaan.

Ter illustratie geven we hieronder een aantal voorbeelden van zaken die nog onduidelijk zijn voor bedrijven, maar deze lijst is niet uitputtend:

- Welke bedrijven vallen wel of niet onder de Cyberbeveiligingswet? En waarom wordt er niet voor gekozen om bedrijven aan te wijzen?
- Als een concern meerdere vestigingen heeft, binnen en buiten de EU, welke nationale wetgeving is er dan van toepassing?
- Hoe ziet hulp aan bedrijven er uit? En hoe ziet hulp aan bedrijven die niet onder NIS2 vallen, maar wel een belangrijke schakel in de keten zijn, er uit? Is daar hulp of financiering voor?
- Wat wordt bedoeld met het begrip passende maatregelen? Hoe wordt beoordeeld of de genomen maatregelen passend zijn als er zich een significant incident heeft voorgedaan?
- Hoe wordt een discussie voorkomen met de autoriteit of risico's wel of niet goed zijn beoordeeld en afgedekt?
- Welke definitie wordt gehanteerd voor een kleine onderneming? Een middelgrote onderneming? Een grote onderneming? En wat zijn vertrouwensdiensten?
- Welke gegevens moeten door bedrijven worden aangeleverd t.b.v. het register dat in de wet wordt omschreven?
- Wat maakt een incident significant? En hoe moet dit gemeld worden?

Verminderen regeldruk voor bedrijven
In de verdere uitwerking van de Cyberbeveiligingswet vragen we nadrukkelijk aandacht voor de regeldruk bij bedrijven. Deze is de afgelopen jaren sterk toegenomen. En in combinatie met problemen die bedrijven ervaren, zoals personeelstekort, is het belangrijk om de richtlijnen goed uitvoerbaar te maken. Het beperken van de regeldruk is ook belangrijk voor bedrijven die indirect onder de Cyberbeveiligingswet vallen (via de keten). Dit komt de, nu nog achterblijvende, betrokkenheid vanuit het midden- en kleinbedrijf ook ten goede.

Scholingsverplichting bestuursleden
Vanuit onze community worden zorgen geuit over artikel 26 waarbij alle leden van het bestuur aantoonbaar trainingen moeten hebben gevolgd en kennis aantoonbaar actueel moeten houden. De vraag die wordt gesteld is of het niet voldoende is dat minimaal één lid van het bestuur deze kennis aantoonbaar heeft? Dit in lijn met de gebruikelijke portefeuilleverdeling op andere thema's, zoals financiën en HR.

Kaders & één standaard
Het gemis aan kaders van de training op dit moment kan een probleem zijn. Dit kan resulteren in een grote hoeveelheid inhoudsloze, maar dure, trainingen die later niet blijken te voldoen. Ook vragen we van de overheid dat ze bijvoorbeeld het toetsingskader openbaar maken, zodat bedrijven weten waar ze aan moeten voldoen. Dit kan mogelijk in vertrouwelijkheid via OKTT-organisaties c.q. het cyberweerbaarheidsnetwerk.

De Cyberbeveiligingswet vraagt van bedrijven dat ze hun (kritische) toeleveranciers gaan beoordelen op hun niveau van cybersecurity. Bedrijven werken vaak samen in dezelfde keten. En voor bedrijven 'lager' in de keten betekent dit dat zij van meerdere bedrijven eisen en voorwaarden gesteld krijgen, die net een beetje anders zijn. Waardoor ze veel tijd bezig zijn met het aantonen van hun cybersecurity richting hun klanten, terwijl daar helemaal geen personeel en budget voor is. Wij verzoeken de overheid om te gaan werken met één standaard, waardoor bedrijven in één keer hun niveau van cybersecurity kunnen aantonen en dit richting alle bedrijven in de keten kunnen gebruiken ter verantwoording. Vanuit CWB hebben we hiertoe, samen met partners, CYRA (cyberrating) ontwikkeld.

Combinatie met andere wet- en regelgeving
Naast de Cyberbeveiligingswet komt er nog heel veel andere wetgeving op de bedrijven af. Bijvoorbeeld de Artificial Intelligence Act, Cyber Resilience Act en Digital Services Act. In het kader van de eerdergenoemde regeldruk is het belangrijk dat er aandacht wordt besteed aan hoe dit samenkomt bij bedrijven. Wij vragen ons af of er zicht is op de impact die al deze wetgeving gaat hebben op de bedrijven in Nederland? En of er wordt samengewerkt om dit behapbaar te houden?