28-06-2024

Geachte heer, mevrouw,

Met veel interesse hebben wij kennisgenomen van het wetsvoorstel voor de Cyberbeveiligingswet (NIS2). Met deze reactie koppelen wij graag de volgende punten terug:

1. Het document behoeft meer duidelijkheid en zelfstandige leesbaarheid. Het bevat nu (onnodig) veel verwijzingen die het document slecht leesbaar maken. Ook bevat het enkele incorrecte verwijzingen en incomplete items. Een sortering van de artikelen en een eenvoudige structuur zouden de duidelijkheid en leesbaarheid ten goede komen. Tevens is het belangrijk om eenduidige definities aan te houden, zonder mogelijkheid voor verschillen in interpretatie.

2. Het voorstel lijkt nu voornamelijk een procesbeschrijving; een herhaling vanuit de Europese NIS2-richtlijnen, maar dan juist minder concreet. De tekst is complex en laat onduidelijk voor organisaties wat ze precies moeten doen (omdat een verdere detaillering is uitgesteld tot de AMvBs). Termen zoals “passende en evenredige maatregelen” passen bij een risico gebaseerde aanpak, maar laten tegelijkertijd (te) veel ruimte voor interpretatie.

3. Er mist een duidelijke beschrijving van wanneer organisaties nu exact wel of exact niet in scope zijn. Waar vanuit de Europese NIS2-richtlijnen het lijkt te gaan om “kritieke functie voor maatschappij” lijkt de Nederlandse vertaling hier niet naar te kijken. Veel organisaties snappen niet waarom zij in scope vallen, en velen weten niet dat ze in scope (gaan) vallen.

4. De wetgeving benadrukt een risico gebaseerde aanpak door entiteiten. Met de huidige reikwijdte van entiteiten die als “kritiek voor de maatschappij” gescoped zijn, neigt NIS2 echter naar een compliance gebaseerde benadering. Hierdoor wordt de ‘toon’ van het document anders; in plaats van ondersteuning voor betere weerbaarheid, neigen de structuur en onduidelijkheid meer naar het (kunnen) “sanctioneren” van organisaties.

5. De opzet, scope en verantwoordelijkheden van de CSIRTs zijn momenteel onduidelijk beschreven. Zo is het ons niet duidelijk: of er 7 CSIRTs zullen zijn (1 per bevoegde autoriteit), wat precies onder hun taken en verantwoordelijkheden valt, en wat entiteiten precies van de CSIRT(s) aan (proactieve) ondersteuning kunnen verwachten. Zoals de CSIRT taken en verantwoordelijkheden nu beschreven staan, lijkt het CSIRT een centrale monitoringrol voor entiteiten in te nemen. Het dient duidelijk te zijn dat dit aanvullend is op wat entiteiten zelf moeten inrichten aan monitoring.

6. Het document beschrijft niet duidelijk wat de scope van incidenten is; m.a.w. of het enkel om cyberincidenten gaat of incidenten in het algemeen, met invloed op de operationele continuïteit. Daarnaast moet de drempelwaarde voor het melden van incidenten per sector nog worden vastgesteld. Hiervoor lijkt een centrale aanpak waarop de sectoren zich kunnen baseren te ontbreken. Het document beschrijft niet duidelijk of OT en IT voor OT meegenomen zijn. Wij weten dat dit vanuit de Europese NIS2 en de intentie van de Nederlandse overheid wel zo is.

7. Voor zover wij begrijpen zijn overheidsinstanties uitgesloten van bestuurlijke aansprakelijkheid. Dit is vanuit ons perspectief vreemd, aangezien de overheid een essentieel onderdeel is van het maatschappelijke ecosysteem. Alles en iedereen dient samen te werken om een veiligere maatschappij te realiseren. Daar hoort ook verantwoordelijkheid en aansprakelijkheid bij van de overheid (ook al is dat met de huidige wetgeving misschien niet mogelijk). Daarnaast is aangegeven dat instanties rond nationale veiligheid (zoals het Ministerie van Justitie & Veiligheid en Ministerie van Defensie) zijn uitgesloten. Wij begrijpen mogelijke uitsluiting van enkele onderdelen, maar niet alles van MinJenV valt onder nationale veiligheid. Ons advies is enkel zeer beperkte functies uit te sluiten (vanwege confidentialiteit) en de rest te laten voldoen, om samen te werken aan een veiligere maatschappelijk ecosysteem.

8. Totdat de AMvB's geïmplementeerd zijn, blijft er grote onduidelijkheid over de daadwerkelijke eisen die gesteld gaan worden (mogelijk pas Q2 2025 of veel later). Dat is ongewenst; duidelijkheid is nodig vanaf het begin zodanig dat organisaties voorbereidingen kunnen treffen in de juiste richting. Naar onze mening is het ook ongewenst dat er verschillen ontstaan onder toezichthouders (in baseline eisen, drempelwaarden, aanpak, etc.), met name voor bedrijven die werken in meerdere sectoren en landen. Tevens is het uiterst inefficiënt omdat de toezichthouders allemaal de juiste mensen met cyber kennis van IT en OT moeten hebben om dit te kunnen doen (in een reeds krappe markt). Waarom geen centralisatie? Zoals ook in enkele andere landen, met 1 brede autoriteit, en centralisatie van de CSIRT kennis.

9. Drie losse opmerkingen die niet direct gerelateerd zijn aan de internetconsultatie:
    a. Wat zijn de gevolgen van het niet zelf registreren? Het niet verkrijgen van hulp is geen reden voor bedrijven om wel te registreren.
    b. Er wordt centraal in Nederland, bij de autoriteiten en bij bijvoorbeeld ENISA, veel informatie opgeslagen. Worden hier passende maatregelen opgenomen?
    c. Wij hebben vernomen dat het ook mogelijk wordt om anonieme meldingen van incidenten te doen? Dat is mogelijk onwenselijk vanuit het oogpunt van beveiliging. Daarmee is “trollen” mogelijk, alsmede kunnen cybercriminelen zelf meldingen maken en slachtoffers onder druk zetten om te betalen om melding te voorkomen. Belangrijk daarbij is de balans: overheid ziet het als helpen maar bedrijfsleven ziet het (mogelijk) als toezicht.