Reactie Cyber Weerbaarheidscentrum Brainport op Consultatie Algemene Maatregel van Bestuur (Cyberbeveiligingsbesluit) en Ministeriële Regeling (Cyberbeveiligingswet)

Dit is een gezamenlijke reactie vanuit het Cyber Weerbaarheidscentrum Brainport, een stichting waarin 100 bedrijven uit de High Tech Maakindustrie en toeleverende keten met elkaar samenwerken om meer cyberweerbaar te worden. Onze reactie bestaat uit de volgende onderdelen:

1. Algemene reactie
2. Inhoudelijke reactie per artikel
3. Taalkundige reactie per artikel

Algemene reactie

Ten aanzien van de Algemene Maatregel van Bestuur vragen wij het volgende:

- Meer balans tussen procedures en actiegerichtheid;
- Aanpassing in de eisen die worden gesteld t.a.v. opleiden;
- Een beschrijving van de rechten voor bedrijven die onder de wet vallen;
- Meer duidelijkheid over de invulling van de zorgplicht in de toeleveranciers keten;
- Meer duidelijkheid over invulling van beoordeling door de toezichthouder;
- Aandacht voor de punten zoals beschreven in de uitwerking van het mkb-panel;
- Inzicht in afstemming tussen wetgeving in Nederland en andere Europese landen;
- Verminder het gebruik van vakjargon in de Nota van Toelichting of leg uit.

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. Maar we zijn ook van mening dat de huidige invulling door de Algemene Maatregel van Bestuur en de Ministeriële Regeling op een aantal punten aangepast moeten worden, om dat doel te bereiken:

- *Balans tussen procedures en actiegerichtheid*
  De huidige opzet van de wetgeving mist een evenwichtige balans tussen procedurele vereisten en praktische uitvoerbaarheid. De gestelde eisen zijn gericht op beleid en procedures en lijken geïnspireerd op kaders als ISO27001. Hoewel deze normen waardevol kunnen zijn, zijn ze voor veel beoogde entiteiten niet haalbaar en in sommige gevallen zelfs onnodig. De verwachte administratieve lasten nemen hierdoor fors toe. Vooral voor bedrijven met complexe structuren — actief in meerdere landen of sectoren — dreigt dit een onuitvoerbare opgave te worden.
- *Opleiding- en trainingseisen*
  De voorgestelde opleidings- en trainingseisen roepen meerdere bezwaren op. Ten eerste is het onrealistisch om te veronderstellen dat álle bestuursleden een bepaalde training moeten volgen. Daarnaast kunnen de eisen die worden gesteld aan trainers en aanbieders van opleidingen de werking van bestaande samenwerkingsverbanden in het toekomstige Cyberbeveiligingsnetwerk (CWN) ondermijnen. Wij spreken ons dan ook uit tegen de artikelen 20, 21, 22 en 23 in het cyberbeveiligingsbesluit. Ook wijzen wij op de terechte

zorgen van het mkb-panel: de voorgestelde regeling lijkt bepaalde opleiders onevenredig voordeel te geven. Verder is het de vraag hoeveel tijd bestuurders krijgen om aan deze eisen te voldoen. Een eendaagse training volstaat simpelweg niet, zeker niet gezien de reeds volle agenda's. Een betere stimulans zou zijn om het lidmaatschap van een CWN-organisatie aantrekkelijk en lonend te maken.

- *Rechten van bedrijven*
  Hoewel de wetgeving zeer gedetailleerd ingaat op de verplichtingen van bedrijven, blijft een duidelijke beschrijving van hun rechten achterwege. Het is onduidelijk wat deze rechten concreet inhouden — bijvoorbeeld het recht op bijstand — en waar bedrijven terecht kunnen voor hulp of informatie. Ook is het onduidelijk welke ondersteuning beschikbaar is voor bedrijven die niet onder NIS2 vallen, maar wel een essentiële schakel in de keten vormen. Wordt voor hen hulp of financiering voorzien? En welke ondersteuning mogen bedrijven in het algemeen verwachten van het NCSC?
- *Zorgplicht in de toeleveringsketen*
  Er is nog onvoldoende duidelijkheid over de reikwijdte van de zorgplicht binnen de toeleveringsketen. Wat wordt verwacht van organisaties als hun directe leveranciers of dienstverleners niet onder de Cbw vallen? Het is van belang om helderheid te bieden over de grenzen van de verantwoordelijkheid van Cbw-plichtige entiteiten in zulke situaties. In Artikel 10 van het cyberbeveiligingsbesluit wordt beschreven welke verplichtingen de essentiële en belangrijke entiteiten hebben. Terwijl in artikel 6 van de Ministeriële Regeling de verplichting van de rechtstreekse leveranciers en dienstverleners wordt uitgewerkt.
- *Beoordeling door toezichthouder*
  De wijze waarop beleid wordt opgesteld kan variëren van zeer gedetailleerd tot meer op hoofdlijnen. Het is daarom van belang dat er meer duidelijkheid komt over hoe de toezichthouder deze invulling zal beoordelen. Veel hangt immers af van de interpretatie en uitvoeringspraktijk van de toezichthouder. In tegenstelling tot artikel 29 van het Cbb, pleit het CWB voor het aanwijzen van maximaal één toezichthouder per entiteit, met als doel overlappend toezicht te voorkomen. Deze aangewezen toezichthouder zou dan ook verantwoordelijk moeten zijn voor het informeren van andere relevante toezichthouders over bevindingen in het kader van de Cbw. Er worden termen gehanteerd als 'regelmatig', 'tijdig' en 'globaal'. Dit werkt verschillende interpretatie in de hand en dat kan leiden tot verschillen tussen sectoren. Dat helpt bedrijven niet in het verbeteren van hun cyberveiligheid.
- *Inbreng mkb-panel*
  Tijdens het mkb-panel zijn een aantal relevante zorgen en aanbevelingen naar voren gebracht. Zo is er behoefte aan praktische ondersteuning bij het inschatten van risico's en moet worden voorkomen dat de nadruk te eenzijdig komt te liggen op administratieve verplichtingen. De vraag is in hoeverre deze signalen uit het mkb daadwerkelijk zijn verwerkt in de huidige wettekst en toelichting.

- *Afstemming met Europese wetgeving*
  Het overkoepelende doel is een hoger, gezamenlijk niveau van cyberbeveiliging binnen de Europese Unie. Het is dan ook belangrijk om inzicht te krijgen in de mate waarin de Cbw, het Cbb en de ministeriële regeling aansluiten op de implementatie van NIS2 in andere Europese lidstaten. In hoeverre wijken de Nederlandse bepalingen af, en is er sprake van een gelijk speelveld?
- *Vakjargon*
  Cyberveiligheid kent technische termen die niet voor iedereen direct begrijpelijk zijn. In de nota van toelichting is het daarom belangrijk om terughoudend te zijn met vakjargon. Als het gebruik van specialistische termen nodig is, licht deze dan kort toe bij het eerste gebruik. Onduidelijke toelichtingen kunnen leiden tot verkeerde interpretatie van verantwoordelijkheden of maatregelen, wat de effectiviteit van de cyberbeveiliging ondermijnt. Duidelijke communicatie is essentieel voor een goede uitvoering en naleving.

Inhoudelijke reactie per artikel

Cyberbeveiligingsbesluit

- Artikel 9 lid 3 sub b: hoe kan er met het CSIRT gecommuniceerd worden?
- Artikel 24: Uit het besluit blijkt nog niet precies hoe wordt bepaald of een incident als significant wordt aangemerkt. De huidige formulering in de wet (‘als het een ernstige operationele verstoring van de diensten of financiële verliezen voor de betrokken entiteit veroorzaakt’). Neem in de ministeriële regeling duidelijke, toetsbare criteria op voor wat als een significant incident geldt, aangevuld met praktijkvoorbeelden. Dit bevordert een eenduidige toepassing van de meldplicht en voorkomt onnodige meldingen of onduidelijkheid bij organisaties.

Nota van Toelichting van het Cyberbeveiligingsbesluit

- Artikel 7, pag 9, eerste alinea:
  - ‘Het beheersen van de risico’s met betrekking tot de netwerk- en informatiesystemen behoort onderdeel van het bredere risicobeheersproces van de entiteit te zijn.’ Dit impliceert **de plicht** om aan bedrijfscontinuïteitsmanagement te doen. Daar is de Cbw / NIS2 niet voor bedoeld, dit is een Network & Information Directive, geen plicht tot Business Continuity Management.
- Artikel 8.1, pag. 9, tweede alinea:
  - Wat is tijdig in dit verband? (Tijdig betekent dat iets op tijd of binnen de gestelde termijn gebeurt).
- Artikel 8.4, pag. 9:
  - ‘Hierbij wordt opgemerkt dat de logging extern kan worden uitbesteed’. Hieraan toevoegen dat logging mogelijk plaatsvindt door een andere vestiging van de entiteit die zich in het buitenland bevindt (als onder 8.2).

Reactie Cyber Weerbaarheidscentrum Brainport op Consultatie Algemene Maatregel van Bestuur (Cyberbeveiligingsbesluit) en Ministeriële Regeling (Cyberbeveiligingswet)

- Artikel 9.2, pag. 10:
    - entiteiten waarborgen dat back-ups onbruikbaar worden. Dit impliceert **de plicht** om unmutable back-ups te gebruiken. Als dat klopt, dat ook schrijven.
- Artikel 10, pag. 10:
    - aub uitbreiden reikwijdte met voorbeelden. Bijvoorbeeld: indien toegang tot elkaars netwerk- en informatiesystemen (bv. Tbv onderhoud machines). Of; indien in het bezit van gevoelige data (bv. (een deel van) intellectueel eigendom)
- Artikel 12.1, pag. 12 (in laatste zin):
    - Om cyberhygiëne te borgen kan, de entiteit bijvoorbeeld denken aan… 'Bijvoorbeeld' impliceert dat er alternatieven zijn. Welke dan?
- Artikel 12.1, pag. 12:
    - En wat is regelmatig? Welke frequentie is toereikend?
- Artikel 13.1, pag. 12, laatste twee zinnen:
    - …cryptografische middelen moeten met minimale inspanning gewijzigd kunnen worden…afhankelijk van de geïdentificeerde risico's. Dit klink eenvoudig, maar is dat ook zo in de praktijk?
- Artikel 15.2, pag. 13:
    - toevoegen aan 'het beheer van logbestanden van toegang, identiteiten, authenticaties en autorisaties' door derden. Dit wordt ook gedaan in artikel 8.2. Waarom niet in dit artikel?
- Artikel 16.2, pag. 14:
    - Onduidelijk: 'Het beleid moet ook regels omvatten voor het aanvaardbaar gebruik van en procedures voor het omgaan met informatie en gerelateerde netwerk- en informatiesystemen'. Wat wordt hiermee bedoeld? Valt er een voorbeeld ter verduidelijking te geven?
- Artikel 17, pag. 14:
    - Aanpassen? Wanneer entiteiten deze attenderingen, adviezen en informatie moeten zij (laten) beoordelen of […]. De beoordeling kan ook door derden, daarom 'laten' toevoegen.
- Artikel 21.2, pag. 15, laatste zin:
    - 'Globale kennis…' Wat is globaal?
- Artikel 22.1, pag. 15:
    - …gekwalificeerd…. Wat is gekwalificeerd? Welke criteria gelden?
- Artikel 22.2, pag. 16:
    - …vereiste specifieke kennis en kunde… Wie bepaalt dat? Wat zijn de criteria?
- Artikel 24.2, pag. 16:
    - ten minste elke vier jaar (in zin 1) versus zeer snelle technologische ontwikkelingen (in zin 4). Dit bijt elkaar. Zou eerder tweejaarlijks moeten én indien relevant.

- Artikel 25, pag. 16:
    - Waarom wordt in dit artikel alleen geschreven over genomen maatregelen? Terwijl in de rest van de toelichting geschreven wordt over genomen én te nemen maatregelen?
- Artikel 25, pag. 16:
    - 'Hiermee kan onder meer beter worden ingeschat of en hoe respons mogelijk is.' Respons door wie?
- Artikel 28.1.b (pag. 17):
    - versus eerste alinea op pag. 18: 28.1.b. schrijft voor dat men het KvK-nummer moet aanleveren versus het authenticatiemiddel dat automatisch het KvK-nummer registreert. Dit is dubbelop en staat haaks op een deel van de één na laatste zin op pagina 17… 'en de entiteiten niet te veel worden belast'.
- Artikel 28.3.a, pag. 17:
    - …moeten aangeven van welk soort zij zijn. Het is niet algemeen bekend wat met 'soort' wordt bedoeld.
- Artikel 30.1, pag. 18:
    - De maximale bewaartermijn van 60 maanden, na de eerste verwerking. Dit lijkt niet erg praktisch.
- Artikel 30.2, pag. 19:
    - Wat als er niets wijzigt in 5 jaar? Overigens weten wij vanuit de praktijk dat het belangrijk is om bedrijven minimaal één keer per jaar, maar vaker indien nodig, te attenderen op het controleren van hun gegevens.
- Artikel 31, pag. 19, tweede alinea:
    - Waar melden bedrijven die niet onder de NIS2 vallen incidenten? Ook daar kunnen dingen gebeuren die relevant zijn voor de essentiële en belangrijke entiteiten.
- Artikel 32, pag. 20, één na laatste alinea:
    - 'De implementatie van de NIS2-richtlijn doorkruist dit ook grotendeels niet.' Wat/waar doorkruist het wel?
- Artikel 36, pag. 21:
    - Als er sprake is van gefaseerde inwerkingtreding, mag dit nooit ten nadele van de entiteiten zijn. Bijvoorbeeld als entiteiten wel aan de verplichtingen moeten voldoen, maar nog geen aanspraak kunnen maken op hun rechten. Of als de ene toezichthouder wel overgaat tot sancties en een andere (nog) niet.

Ministeriële regeling

- Artikel 6a en 6b, pag. 6:
    - Hoezo? Wat als rechtstreekse leveranciers en rechtstreekse dienstverleners niet Cbw-plichtig zijn?

- Artikel 7.1.b:
    - Reeds onderdeel van Cyber Resilience Act. Belangrijk om dit 1-1 aan te laten sluiten.
- Artikel 7.3.c:
    - 'binnen een redelijke termijn'. Wat is redelijk? (ook in artikel 11.3, tweede alinea)
- Artikel 7.3.c:
    - We snappen niet wat wordt bedoeld met: 'De essentiële en belangrijke entiteit kan beveiligingsvoorschriften vaststellen met betrekking tot de ontwikkelingsomgevingen, beveiligingstestprocessen vaststellen en toepassen in de omgevingscyclus, gegevens over beveiligingstests op passende wijze selecteren, beschermen en beheren en testgegevens saneren en anonimiseren.' Daarbij lijkt het erg veel gevraagd.
- Artikel 7.3.c, tweede alinea:
    - Hier kunnen wij ons iets bij voorstellen. Bijvoorbeeld als de patch de bedrijfscontinuïteit in gevaar brengt. Maar de manier waarop deze toelichting nu geformuleerd is, is onduidelijk en roept vragen op.

Taalkundige reactie per artikel

In het Cyberbeveiligingsbesluit hebben we meerdere moeilijke woorden gesignaleerd.
Deze vereisen nadere uitleg en/of verwijzing naar het Cybersecurity Woordenboek.

Nota van Toelichting van het Cyberbeveiligingsbesluit

- pag. 3:
    - gap assessment*; in het woordenboek is alleen sprake van een gap analyse.
    - Wat zijn out-of-pocket kosten?
- pag. 4:
    - discretionaire ruimte = met de vrijheid om zelfstandig te oordelen of te handelen.
- pag. 8:
    - cyclisch = periodiek terugkerend
    - all hazard* = gelijktijdig analyseren van verschillende typen risico's ; komt niet voor in laatste versie van Cybersecurity Woordenboek
- pag. 11:
    - security by design = tijdens het ontwerp al rekening houden met security
    - security by default = standaard instelling; de default moet op veilig ingesteld staan (vinkjes) alternatief = verwijzen naar Cybersecurity woordenboek (want beide termen staan daar in)

- pag. 14, art. 18, 5e regel:
    - Het is aan entiteiten zelf om in te schatten ….. dat deze maatregelen moeten worden geëvalueerd. Hier ontbreekt een woord op de plek van de puntjes. Welk woord? Dat of Wanneer?
- pag. 15, tweede alinea:
    - Veel te ingewikkeld verwoord. Alternatief: De grondslag in artikel 19 Cbb betreft de maatregelen genoemd in artikel 21, eerst lid en derde lid Cbw.
- pag. 16, in artikel 25:
    - cascade-effecten: onvoorziene keten van gebeurtenissen c.q. kettingreactie.
- pag. 17, artikel 28.1, eerste alinea:
    - triage. Dit woord staat niet in de laatste versie van het Cybersecurity Woordenboek.
- Pag. 17, artikel 28.3.b:
    - Deze alinea valt samen te vatten tot: Domeinnamen en/of IP-adressen aanleveren, is verplicht zodat CSIRT's hun wettelijke taken effectief kunnen uitvoeren. IP-adressen zijn ook belangrijk in het kader van waarschuwen.
- pag. 18, artikel 30:
    - botnet. Staat in het Cybersecurity Woordenboek.
- pag. 19, artikel 31, derde alinea:
    - AFM of DNB. Beide afkortingen aub voluit schrijven.
- pag. 20, artikel 34:
    - Wwke. Aub voluit schrijven

Ministeriële regeling

- Pag. 5, artikel 5.f én pag. 11 eerste regel laatste alinea:
    - redundantie(s). Aub uitleggen, want niet in het Cybersecurity Woordenboek.
- Pag. 11, tweede alinea:
    - interferentie
- Pag. 13, eerste alinea:
    - Security by design én zero trust architectuur

Daarnaast zijn ons bij het doornemen van het cyberbeveiligingsbesluit en de Ministeriële Regeling een aantal taalfouten opgevallen. Hieronder worden deze artikelsgewijs opgesomd.

Nota van Toelichting van het Cyberbeveiligingsbesluit

- pag. 10, eerste alinea, tweede regel: 'moeten hebben vaststellen'
- pag. 10, tweede alinea, derde regel: tijdens het incident ipv de incident
- pag. 10, vierde alinea, eerste regel: essentiële entiteiten 'en' belangrijke entiteiten ('en' ontbreekt)
- pag. 11, tweede alinea, laatste alinea: Ook moet deze entiteiten
- pag. 16, artikel 25. De slotzin is een letterlijke herhaling van wat al eerder in het artikel staat en kan worden geschrapt.

- pag. 18, artikel 30, in zevende regel van onder ontbreekt een woord: …bijvoorbeeld de benodigde analyse is in de praktijk te kort gebleken…

Ministeriële regeling

- Pag. 10, tweede alinea van onder: Onderdeel d stelt dat de procedure moet vastleggen op welke wijze uit het de risico worden geëvalueerd.
- Pag. 11, eerste alinea, derde regel: risicobehandelingen en/of risicobeheersmaatregelen ‘en/of’ ontbreekt.
- Pag. 11, derde alinea, eerste zin: …de wijze moet vastleggen ~~wijze~~ waarop…