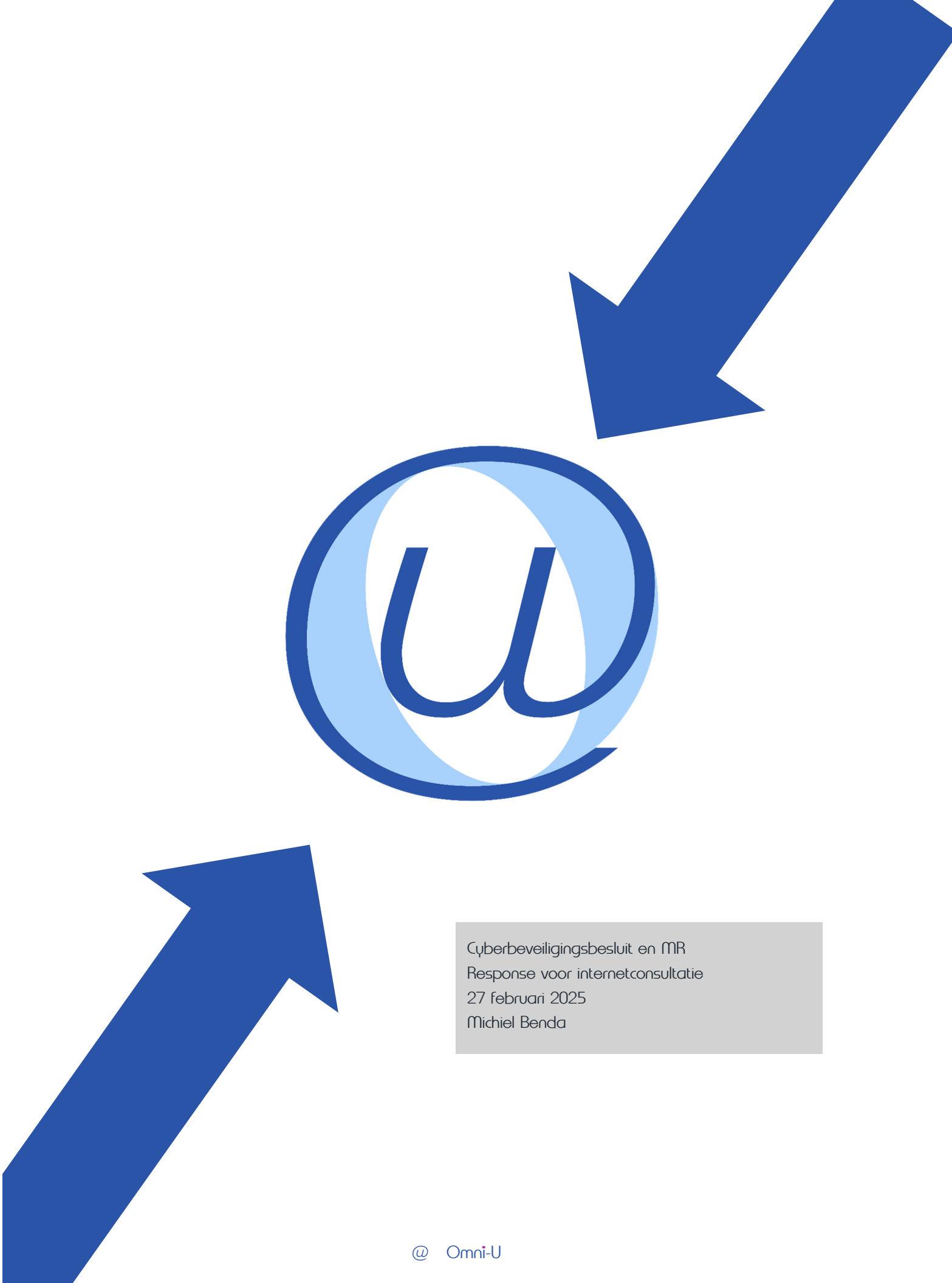

Cyberbeveiligingsbesluit en MR
Response voor internetconsultatie
27 februari 2025
Michiel Benda

Contents

Cyberbeveiligingsbesluit (CBB)

Artikel 2:

Een CSIRT heeft volgens de NIS2 richtlijn, artikel 11 een aantal expliciete verantwoordelijkheden, zowel qua dienstverlening als qua inrichting. Het lijkt me onwenselijk voor Onze Minister om deze inrichting te doen. Waarom niet het NCSC aanwijzen in lid 1 als het CSIRT? Dan kunnen daar volgens lid 2 prima aanpassingen gedaan worden per sector, subsector of soort entiteit.

Artikel 6 t/m 18 algemeen:

Opmerking 1:

Het lijkt erop dat ervoor gekozen wordt om voor alles naar opzet, bestaan en werking te gaan kijken. Al snap ik de waarde hiervan en ben ik groot voorstander, is dit voor menig bedrijf wat de scope in komt en nog nooit serieus informatiebeveiliging heeft gehanteerd een grote stap. In feite vraag je van deze bedrijven om ineens van CMM volwassenheidsniveau 0/1 naar volwassenheidsniveau 3/4 te gaan. Ik betwijfel de realistische haalbaarheid hiervan, afgezien van de enorme kosten die ermee gemoeid zijn. Ik zou voor de maatregelen vooralsnog naar opzet en bestaan sturen en wellicht voor het risicobeheer wel opzet, bestaan en werking.

Opmerking 2:

Er lijkt een definitie issue te zitten in de beschrijvingen. Steeds als er iets staat over beleid staat erin dat in het beleid procedures beschreven moeten worden. Dit is niet de bedoeling van beleid. Procedures geven invulling aan beleid en zijn aparte documenten die apart beheerd worden (en hopelijk niet door het bestuur goedgekeurd behoeven te worden).

Opmerking 3:

Er staan veel verplichtingen in dit Besluit om formele beleidstukken en procedures op te stellen. Dit is voor veel entiteiten een flinke administratieve belasting die in de NIS2 niet aangegeven wordt. Integendeel, op diverse plekken in de Richtlijn, zoals overweging 15 en overweging 81 hieronder weergegeven, wordt juist aangeduid dat de administratieve belasting zoveel mogelijk beperkt moet worden.

(15) Entiteiten die voor de naleving van de maatregelen voor het beheer van cyberbeveiligingsrisico's en de rapportage- verplichtingen binnen het toepassingsgebied van deze richtlijn vallen, moeten worden ingedeeld in twee categorieën, essentiële entiteiten en belangrijke entiteiten, naargelang de mate waarin zij kritiek zijn door hun sector of het soort door hen verleende diensten, alsook hun omvang. In dat verband moet, in voorkomend geval, terdege rekening worden gehouden met relevante sectorale risicobeoordelingen of richtsnoeren van de bevoegde autoriteiten. De toezichts- en handhavingsregelingen voor die twee categorieën entiteiten moeten worden gedifferentieerd om te zorgen voor een billijk evenwicht tussen op risico gebaseerde eisen en verplichtingen enerzijds en de administratieve lasten die voortvloeien uit het toezicht op de naleving anderzijds.

(81) Om te voorkomen dat aan essentiële en belangrijke entiteiten onevenredige financiële en administratieve lasten worden opgelegd, moeten de maatregelen voor het beheer van cyberbeveiligingsrisico's in verhouding staan tot de risico's voor het betrokken netwerk- en informatiesysteem, rekening houdend met de stand van de techniek van dergelijke

maatregelen en, in voorkomend geval, de relevante Europese en internationale normen, alsook met de kosten voor de uitvoering ervan.

Artikel 6, lid 2:

"De entiteit zorgt ervoor dat conflicterende rollen, verantwoordelijkheden en bevoegdheden gescheiden worden."

Dit is een maatregel die, afhankelijk van de organisatie, disproportioneel is. Een midden-grote organisatie van 50 medewerkers zal hier mogelijk veel moeite mee hebben.

Artikel 6, lid 4:

Mee eens, maar dit is niet in de context van de maatregel beleid die hier staat. Ik zou deze eerder gerelateerd zien aan het Governance artikel 24 van de CBW.

Artikel 7, lid 2b:

Dit is geen onderdeel van beleid. Hier zou een lid 3 beter passen waarin de verplichting voor de procedures wordt vastgesteld.

Artikel 8, lid 1:

Eens als de scope teruggebracht wordt naar significante incidenten. Dit voor ieder incident aantoonbaar toepassen lijkt me disproportioneel.

Procedures zijn geen onderdeel van beleid. Hiervoor zou een apart lid opgenomen moeten worden.

Artikel 8, lid 2:

De essentiële entiteit of belangrijke entiteit stelt ~~als onderdeel~~ **ten behoeve** van het beleid, bedoeld in het eerste lid, procedures vast om activiteiten in haar netwerk- en informatiesystemen te monitoren en te registreren teneinde incidenten, bijna-incidenten, cyberdreigingen en kwetsbaarheden te detecteren, analyseren en classificeren. De entiteit past deze procedures aantoonbaar toe.

Artikel 8, lid 3:

De essentiële entiteit of belangrijke entiteit stelt ~~als onderdeel~~ **ten behoeve** van het beleid, bedoeld in het eerste lid, procedures vast om de gevolgen van een incident te mitigeren, de oorzaak van een incident weg te nemen en te herstellen van een incident. De entiteit past deze procedures aantoonbaar toe.

Artikel 9, lid 1:

Het is ongewoon om een organisatie te verplichten om een plan toe te passen bij een incident. De organisatie kan allerlei redenen hebben om dat niet te doen in een bepaalde situatie. Waarom zou je wettelijk dit willen verplichten? Het opstellen, testen en oefenen lijkt ruim voldoende. De

organisatie zal dan het plan logischerwijs toepassen als dat de beste oplossing lijkt zonder dat hiervoor een wettelijke verplichting bestaat.

Een bedrijfscontinuïteitplan en een noodvoorzieningenplan zijn twee verschillende plannen. Dat is hier niet zo verwoord. Als dat hier ook bedoeld wordt moet de tweede zin beschreven worden vanuit meerdere plannen, niet een enkelvoudig plan.

Een bedrijfscontinuïteitplan is niet voor ieder incident. Dat wordt hier wel verplicht. De organisatie moet, op basis van de duur van de verstoring en de maximaal toegestane uitvalsduur zelf kunnen bepalen om het plan te activeren. Dat gaat dan waarschijnlijk om een selecte set significante incidenten.

Artikel 9, lid 3, punt b:

Deze zin is onduidelijk. Er staat nu dat het crisisbeheersingsplan een beschrijving geeft van communicatiemiddelen tussen de entiteit, het CSIRT en de bevoegde autoriteit. In basis heeft de bevoegde autoriteit geen rol in de crisis. Het CSIRT heeft alleen een actieve rol als de entiteit dit wenst. Waarom is de specificatie van communicatiemiddelen hier belangrijk? Ik snap de noodzaak voor contactgegevens, maar dat staat er niet. De specificaties leiden er overigens waarschijnlijk toe dat dit alles is wat menig entiteit in het plan beschrijft. Daarmee is het plan geen plan omdat het iedere beschrijving van uitvoering mist.

De CBW, artikel 21, lid 3, punt c gaat over crisisbeheer. Dat is een activiteit, geen plan. De eis in het besluit lijkt dus niet aan te sluiten op de wet. Hetzelfde geldt overigens over bedrijfscontinuïteit.

Noodvoorzieningenplannen zoals hier beschreven en ook in de CBW beschreven zijn ontstaan uit een vertaalfout die zich uitsluitend in de Nederlandse versie van de richtlijn lijkt te bevinden. De andere talen van de NIS2 richtlijn beschrijven “Disaster Recovery”. Door de vertaling naar Noodvoorzieningenplannen wijken zowel de Nederlandse richtlijn, de CBW, en het Besluit allemaal af van de NIS2 richtlijn intentie op twee punten: 1. Het gaat om de activiteit van rampenherstel en 2. Het gaat om rampenherstel, niet om noodvoorzieningen.

Artikel 10, lid 1:

De toelichting is niet consistent. Het gaat over beleid over de beveiliging van de toeleveringsketen, maar de bepalingen die gespecificeerd worden gaan alleen over de directe leveranciers en dienstverleners.

Artikel 10, lid 2:

Dit lid geeft geen invulling aan de NIS2 eis om iets met de toeleveringsketen te doen. De toeleveringsketen is meer dan alleen de leveranciers. Overweging 85 uit de NIS2 richtlijn zegt hierover hetvolgende:

(85) “Het aanpakken van risico’s die voortvloeien uit de toeleveringsketen van een entiteit en uit haar relatie met haar leveranciers, zoals leveranciers van diensten op het gebied van gegevensopslag en -verwerking of leveranciers van beheerde beveiligingsdiensten en softwareredacteuren, is bijzonder belangrijk gezien de prevalentie van incidenten waarbij entiteiten het slachtoffer zijn geweest van cyberaanvallen en waarbij kwaadwillende daders

> de beveiliging van de netwerk- en informatiesystemen van een entiteit in gevaar hebben kunnen brengen door gebruik te maken van kwetsbaarheden die van invloed zijn op producten en diensten van derden. Essentiële en belangrijke entiteiten moeten daarom de algemene kwaliteit en weerbaarheid van de producten en diensten, de daarin vervatte maatregelen voor het beheer van cyberbeveiligingsrisico's, en de cyberbeveiligingspraktijken van hun leveranciers en dienstverleners beoordelen en er rekening mee houden, met inbegrip van hun veilige ontwikkelingsprocedures. Essentiële en belangrijke entiteiten moeten met name worden aangespoord om maatregelen voor het beheer van cyberbeveiligingsrisico's op te nemen in de contractuele regelingen met hun directe leveranciers en dienstverleners. Die entiteiten kunnen ook risico's in aanmerking nemen die voortvloeien uit de activiteiten van leveranciers en dienstverleners op een ander niveau."

Met name de laatste zin van deze overweging maakt expliciet dat de richtlijn de volle toeleveringsketen bedoeld en niet alleen de directe leveranciers. Mijn advies zou zijn om hiervoor een verplichting op te nemen waarin directe leveranciers verplicht worden om de cyberbeveiligingseisen door te zetten naar relevante subleveranciers en dat de eis om dit door te zetten daarin ook wordt meegenomen.

Artikel 10, lid 2:

"De entiteit houdt de afspraken actueel." Dit lijkt een lastig uitvoerbare verplichting. Afspraken actueel houden betekent met regelmaat de contractuele afspraken met leveranciers en dienstverleners herzien. Dat is voor de meeste partijen onwenselijk. Een alternatief zou zijn om partijen te motiveren om contract clausules in te voegen die de leverancier en dienstverlener verplichten om de maatregelen relevant voor de risico's te houden waarbij rekening wordt gehouden met de stand van de techniek zoals dit ook voor de entiteit zelf in artikel 21 lid 2 van de CBW wordt verwoord.

Artikel 10 lid 3:

Dit is eenvoudig te interpreteren als het bijhouden van de contracten met leveranciers en dienstverleners. Wat is de bedoeling van deze clausule anders dan een administratieve handeling opleggen aan de entiteiten?

Artikel 11, lid 1:

Dit lid verwacht alleen dat eisen vastgesteld worden, niet dat de beveiliging wordt doorgevoerd.

Artikel 11, lid 3:

De hele vastlegging van de procedures is in een volwassen organisatie al een uitdaging. Voor veel entiteiten die onder de CBW vallen is dit een administratieve belasting die relatief weinig toevoegd. De intentie van Artikel 21, lid 3, punt e is om de netwerken en informatiesystemen te beveiligen. Zonder de beschreven administratieve vastlegging kan een organisatie nog steeds prima aan die eis voldoen.

Artikel 12:

Zowel lid 1 als lid 2 gaat alleen in op bewustwording van medewerkers, niet op de daadwerkelijk basis cyber hygiëne. Dat maakt de invulling in het Besluit incompleet. Vanuit de NIS2 richtlijn wordt basis cyber hygiëne beschreven in overweging 89:

(89) Essentiële en belangrijke entiteiten moeten een breed scala aan basispraktijken op het gebied van cyberhygiëne toepassen, zoals zero trust-beginselen, software-updates, configuratie van apparaten, netwerksegmentatie, identiteits- en toegangsbeheer of gebruikersbewustzijn, opleidingen voor hun personeel organiseren en het bewustzijn van cyberdreigingen, phishing of social engineeringtechnieken vergroten. Voorts moeten die entiteiten hun eigen capaciteiten op het gebied van cyberbeveiliging evalueren en, in voorkomend geval, streven naar de integratie van technologieën ter bevordering van cyberbeveiliging, zoals artificiële intelligentie of machine- leersystemen, om hun capaciteiten en de beveiliging van netwerk- en informatiesystemen te verbeteren.

Artikel 14:

Dit artikel mist de invulling die door de NIS2 richtlijn wordt gegeven. Daarin wordt voor beveiligingsaspecten ten aanzien van personeel verwezen naar EU richtlijn 2022/2557 waarin in Artikel 13, lid 1, punt e en Artikel 14, lid 3 de volgende aspecten staan:

Artikel 13, lid1:

De lidstaten zorgen ervoor dat kritieke entiteiten passende en evenredige technische, beveiligings-, en organisatorische maatregelen nemen om voor hun weerbaarheid te zorgen, op basis van de door de lidstaten verstrekte relevante informatie over de lidstaat-risicobeoordeling en van de resultaten van de risicobeoordeling door een kritieke entiteit, met inbegrip van maatregelen die nodig zijn om:

e) te zorgen voor adequaat beheer van personeelsbeveiliging, naar behoren rekening houdend met maatregelen zoals het vaststellen van categorieën personeelsleden die kritieke functies vervullen, het vaststellen van het recht van toegang tot gebouwen, kritieke infrastructuur en gevoelige informatie, het instellen van procedures voor antecedentenonderzoek in overeenstemming met artikel 14 en het aanwijzen van categorieën van personen die aan een dergelijk antecedentenonderzoek moeten worden onderworpen, en het vaststellen van passende opleidingsvoorschriften en kwalificaties;

Artikel 14, lid 3:

3. Bij een in lid 1 bedoeld antecedentenonderzoek wordt ten minste:

a) de identiteit bevestigd van de persoon op wie de achtergrondcontrole betrekking heeft;

b) het strafregister geraadpleegd van die persoon wat betreft strafbare feiten die relevant zijn voor een specifieke functie.

Artikel 15:

De titel van dit artikel “beveiligingsaspecten ten aanzien van toegangsbeleid” is niet in overeenstemming met de verklaring van artikel 21, lid 3, punt i van de CBW. Het artikel uit de CBW is letterlijk overgenomen uit de Nederlandstalige NIS2 richtlijn. De Engelse versie hiervan beschrijft punt i als: “(i) human resources security, access control policies and asset management;” De tekst “beveiligingsaspecten ten aanzien van” duiden dus uitsluitend op het personeel. De invulling van dit Artikel 15 moet dus gaan over “access control policies” ofwel toegangsbeleid.

Artikel 15, lid 2:

Toegangsbeleid gaat in basis over autorisaties, niet over identiteiten en authenticaties zoals in lid 1 ook beschreven staat van dit artikel. Het beheren van authenticaties is een vreemde activiteit. Wat ga je dan beheren? Authenticatie methoden zou kunnen als dit ondanks dat het hier in basis om autorisaties gaat erin moet komen.

Artikel 15, lid 3:

Periodiek beoordelen van authenticaties klinkt ongewoon. Wat wordt er dan beoordeelt? Autorisaties en gebruik maken van autorisaties kan beoordeeld worden. Vanuit een SOC perspectief kan gekozen worden om alerts te genereren over authenticaties, maar dat is geen periodieke beoordeling van de authenticatie zoals het lid 3 van dit artikel impliceert.

Artikel 16:

De titel van dit artikel “beveiligingsaspecten ten aanzien van beheer van assets” is niet in overeenstemming met de verklaring van artikel 21, lid 3, punt i van de CBW. Het artikel uit de CBW is overgenomen uit de Nederlandstalige NIS2 richtlijn. De Engelse versie hiervan beschrijft punt i als: “(i) human resources security, access control policies and asset management;” De tekst “beveiligingsaspecten ten aanzien van” duiden dus uitsluitend op het personeel. De invulling van dit Artikel 16 moet dus gaan over “asset management” ofwel middelenbeheer/assetbeheer.

Artikel 16, lid 1:

De invulling die hier staat is niet in overeenstemming met de verwachting van de CBW en de NIS2 richtlijn. Assetbeheer gaat over het beheren van alle assets. De “alle gevaren” specificatie van de richtlijn in acht nemend, gaat dit beheer dus niet alleen over netwerk en informatiesystemen maar alle informatiemiddelen die hierbij horen. Daar horen dus ook fysieke locaties, hardware, software en mensen bij. Hardcopy zou er in relatie tot cyberbeveiliging uitgelaten kunnen worden. De intentie van assetbeheer is om kwetsbaarheden en daarmee risico’s te kunnen identificeren. Dat komt nu in de uitleg van het artikel niet aan de orde.

Artikel 16 lid 2:

De classificatie in punt a zou van toepassing moeten zijn op alle relevante assets zoals hierboven beschreven.

Artikel 16, lid 3:

Een inventaris van informatie is onmogelijk. Het moet hier gaan om een inventaris van informatiemiddelen.

Artikel 18:

Schriftelijke vastlegging is vooral een administratieve belasting die niet voor alle maatregelen nodig is. Algemene aantoonbaarheid zou genoeg moeten zijn. Overigens beschrijft CBW artikel 21, lid 3, punt f het hebben van beleid en procedures, niet de vastlegging van effectiviteitsmetingen. Dit is een extra eis die het Besluit introduceert die een behoorlijke belasting legt op de entiteiten.

Artikel 20:

De overzetting naar CBW heeft geleid tot een subtiele fout. De NIS2 richtlijn beschrijft namelijk dat de leden van de bestuursorganen “voldoende kennis en vaardigheden verwerven om risico’s te kunnen identificeren en **risicobeheerspraktijken** op het gebied van cyberbeveiliging en de gevolgen ervan voor de diensten die door de entiteit worden verleend, te kunnen beoordelen.” In de CBW is de term risicobeheerspraktijken veranderd naar risicobeheersmaatregelen. Dit geeft een andere lading aan de eis die de NIS2 beschrijft.

Artikel 21, lid 2:

Dit deel van de trainingsvereisten is een gevolg van de term verandering van risicobeheerspraktijken naar risicobeheersmaatregelen. Formeel is dit volgens de richtlijn dus niet nodig, al moet de bestuurder wel toezien op de implementatie en onderhoud van de maatregelen. Dit laatste is overigens verdwenen uit Artikel 24, lid 1 van de CBW, hetgeen niet in lijn is met de instructie die de EU heeft gegeven aan de lidstaten bij het opstellen van de wet.

Artikel 25, punt c:

De informatie die in punt c benoemd wordt is bedoeld in de notificatie die binnen 72 uur verwacht wordt. Voor de vroegtijdige melding zorgen deze specificaties voor vertraging in de melding (entiteiten gaan eerst oorzaken onderzoeken in plaats van direct te melden). De intentie van de vroegtijdige waarschuwing gaat juist om in een zo vroeg mogelijk stadium informatie te krijgen waarop het CSIRT kan handelen en eventueel adviseren. Ik zou deze eis hier dus niet stellen om vertraging te voorkomen.

Artikel 29:

Welke bevoegde autoriteiten refereert het Besluit aan? De bevoegde autoriteiten t.b.v. de CBW zijn in Artikel 15 van die wet al aangewezen.

Artikel 31:

Deze aanpassing lijkt in strijd met CBW Artikel 41 (informatieverstrekking in verband met incidenten met betrekking tot financiële entiteiten): “Indien het centrale contactpunt informatie van de bevoegde autoriteiten uit hoofde van de Verordening (EU) 2022/2554 ontvangt over incidenten met betrekking tot financiële entiteiten, kan hij deze informatie doorsturen naar een CSIRT of een bevoegde autoriteit.”

Artikel 41 lijkt dus te stellen dat de centrale contactpunt informatie over incidenten al doorgeeft aan een CSIRT of bevoegde autoriteit. Waarom zouden we deze entiteiten dan nog verplichten om een extra administratieve belasting aan te gaan en een extra melding onder de CBW te maken?

Artikel 36:

Deze specificatie maakt inwerkingtreding voor entiteiten enorm lastig. Formeel moeten entiteiten al sinds 17 oktober 2024 voldoen aan de wet die afgeleid is uit de NIS2 richtlijn. Zodra de wet uitkomt zal de Staat direct formeel moeten handhaven. Bedrijven moeten daarmee dus minimaal voldoen aan de eisen uit artikel 21 lid 3 van de CBW. Als we dan vervolgens andere eisen gaan stellen door het Besluit op een later tijdstip creëert dat onnodige administratieve belasting en kosten voor de

organisatie. Er lijkt geen reden te zijn om dit (aangepaste) Besluit direct en volledig in werking te laten treden bij de inwerkingtreding van de CBW.

Ministeriele regeling

Artikel 3, lid 3:

Beleid gaat niet over specifieke maatregelen maar over kaderstellingen waarbinnen activiteiten uitgevoerd worden. De maatregelen moeten dus invulling geven aan het beleid, maar het beleid gaat niet in op de specifieke maatregelen. Bij punten a, b en c zou ik dus adviseren de referentie naar de maatregelen uit artikel 21 eruit te halen. Mocht dat niet gebeuren dan moet de referentie gecorrigeerd worden. De maatregelen staan namelijk in artikel 21, lid 3, niet artikel 21, lid 1.

Artikel 4, lid 1:

Hier wordt gerefereerd aan procedures, maar de punten die hier staan zijn beleidspunten, geen procedure stappen.

Artikel 7, lid 3, punt a en b:

De term “waar passend” in punt a en b hoort er niet. De bron moet altijd geverifieerd worden en er moet altijd getest worden voordat er geïnstalleerd wordt.

Artikel 7, lid 3, punt c:

“redelijke termijn” is vaag en voegt dus geen verplichting toe.

Artikel 7, lid 3, punt e:

Organisaties worden niet blootgesteld aan kwetsbaarheden maar aan risico’s. Kwetsbaarheden zitten in de assets. Evalueren van blootstelling aan dreigingen heeft geen toegevoegde waarde als er geen risico’s zijn.

Artikel 7, lid 3, punt g:

Onduidelijk. Gaat het hier om een motivatie waarom kwetsbaarheden die een risico vormen niet verholpen worden of alle kwetsbaarheden. Wat als de risico’s als acceptabel gezien worden. Moet daar voor alle risico’s een verantwoording komen? Dit lijkt op een enorme administratieve belasting die voor de meeste organisaties slechts minimale voordelen brengt.

Artikel 7, lid 3, punt h:

Onduidelijk. Wat voor segmentatie? De manier waarop de tekst nu staat duidt dat op micro-segmentatie (iedere informatie systeem een eigen segment). Dit is een enorme administratieve belasting die ook nog eens heel foutgevoelig is. Als hier functionele segmentatie wordt bedoeld, wat zijn dan de eisen van die segmentatie? Rekening houden met locatie tussen betrouwbare netwerken- en informatie systemen lijkt in strijd met de Zero trust principles die de NIS2 richtlijn onder basis cyber hygiëne verstaat (overweging 89).

Artikel 9:

De bedoeling van de eis uit de CBW is verkeerd opgepakt in het Besluit en deze regeling. Zie uitleg onder Artikel 15 en Artikel 16 van het Besluit in dit document.

Artikel 9, lid 2:

Artikel 21, lid 3, punt j van de CBW geeft de mogelijkheid tussen MFA en continu authenticatie. Dat wordt door deze regeling uitgesloten. Is dat de bedoeling? M.a.w. is continu authenticatie geen toegestane alternatieve maatregel meer?