Memo

Onderwerp: reactie internetconsultatie Cyberbeveiligingsbesluit.

De Nederlandse ggz (deNLggz) maakt graag gebruik van de mogelijkheid om input te leveren op de concept tekst van het Cyberbeveiligingsbesluit (Cbb). In breder verband zijn wij blij met wetgeving om verdere invulling te geven aan de NIS2 / CBW en daar waar mogelijk te komen tot sectorspecifieke richtlijnen en afspraken.

Naar aanleiding van de tekst in consultatie die nu voorligt signaleren wij de volgende punten:

<u>Vooraf</u>

In de toelichting op de website internetconsultatie Cyberbeveiligingsbesluit (Cbb) staat bij “In het kort” het volgende: “Voor de ministeries van Binnenlandse Zaken en Koninkrijksrelaties en van Volksgezondheid, Welzijn en Sport geldt dat de uitwerking van de zorgplicht uit de Cyberbeveiligingswet (Cbw) voor het overgrote deel in lijn is met bestaande normenkaders voor cyberbeveiliging in de sectoren overheid en gezondheidszorg. Voor de overheid gaat dit om de Baseline Informatiebeveiliging Overheid (BIO)2. Voor de zorg gaat het om de NEN7510 en ISO27001.” In de bijgevoegde concept ministeriele regeling wordt het ministerie van VWS niet genoemd, waaruit op te maken valt dat deze concept ministeriele regeling niet van toepassing is op de zorg sector. Artikel 19 Cbb biedt de ruimte om ook voor de zorgsector ministeriele regelingen op te stellen die gerelateerd zijn aan de NEN 7510. Zolang er geen ministeriele regeling komt vanuit het ministerie van VWS moet de zorgsector zich verhouden tot de algemene eisen in de Cbw en Cbb. Dit geeft onduidelijkheid in hoeverre de NEN 7510 voor de zorgsector nu wel als uitgangspunt voorliggend is. Wij roepen de minister van VWS op tot het opstellen van een ministeriële regeling voor de zorgsectoren en om deze ook in consultatie te brengen.

<u>Regeldruk gevolgen</u>

We maken ons ernstig zorg over de regeldrukgevolgen die de Cbb zal gaan hebben voor de belangrijke -en essentiële entiteiten. Dit naar aanleiding van de toelichting beschreven in onderdeel 3 van de Nota van Toelichting. Nog los van de wijze waarop de regeldruk en de eenmalige- en structurele kosten zijn becijferd, vragen wij ons wel af of het uitvoerbaar gaat zijn voor zorgorganisatie die nu geconfronteerd gaan worden met extra eisen en voor een deel nog onduidelijke regelgeving (zie onderdeel “vooraf”).

<u>Beleid over risicomanagement</u>

Met betrekking tot artikel 7 Cbb (blz 8 e.v. memorie van toelichting), signaleren wij het volgende. In de beschrijving ligt de duiding ten aanzien van risicobeheersing op een *all Hazard benadering* waarbij in de uitleg aangegeven wordt dat een te beschermen belang datgene is wat belangrijk is

voor de entiteit om goed te kunnen functioneren en om de continuïteit van haar dienstverlening te borgen. Wij vragen ons af of hier geen sprake is van oprekken van de reikwijdte van de oorspronkelijke beoogde insteek van de NIS2, waarbij de focus ligt op beveiliging tegen cyberrisico's. Op het moment dat voor deze benadering wordt gekozen is het in aanvullende ministeriele regelingen waarschijnlijk lastig om voor een andere, minder brede, interpretatie te kiezen die bijvoorbeeld wel aansluit bij de huidige risicobeheersingssystematiek van de zorgsector (zoals de NEN 7510).

Training

Artikel 24 Cbw gaat in op de training die ieder lid van het bestuur moet volgen.

In artikel 20 Cbb wordt gesteld: "De training moet bestuursleden in staat stellen om risico's voor de beveiliging van netwerk- en informatiesystemen te kunnen identificeren en de maatregelen inclusief gevolgen te beoordelen, om zo tot een goede afweging en afgewogen besluitvorming rondom de beveiliging van netwerk- en informatiesystemen te komen." Concreet betekent dit dat alle bestuurders een technische achtergrond moeten hebben om invulling te kunnen geven aan reikwijdte van deze definitie. Ook de voorbeelden die genoemd worden in artikel 21 duiden op deze strekking. Dit kan ons inziens niet de bedoeling zijn van de NIS2 / Cbw. Wij vragen aandacht voor een omschrijving in de Cbb waarbij het in de kern gaat om aantoonbaarheid en betrokkenheid bij het domein van beveiliging van netwerk- en informatiesystemen, waarbij de insteek van risicobeheersing en risicoafweging (zoals ook in de NEN 7510 reeds is geborgd) centraal staat. Technische kennis op het vlak van de dreiging van malware, *insiders threat* en DDoS-aanvallen voert ons inziens veel te ver om onderdeel van een training te laten zijn.

Drempelwaarde in het kader van significante incidenten

Met betrekking tot artikel 24 Cbb (blz 16 memorie van toelichting), signaleren wij het volgende. Vanuit het ministerie van VWS is opdracht verstrekt aan een adviesbureau om het veld te betrekken bij totstandkoming van de criteria op basis waarvan gesteld kan gaan worden of er sprake is van een significant incident als bedoeld in artikel 25 tweede lid Cbw. De opbrengst van deze opdracht is teruggekoppeld aan vertegenwoordigers van diverse subsectoren binnen de zorgsector. Wij concluderen dat deze opbrengst en daarmee het voorstel voor criteria onnodig ingewikkeld is en niet het draagvlak heeft van onze achterban. Wij roepen de vakminister van VWS op om nogmaals met het veld in gesprek te gaan om te komen tot betere criteria die aansluiten bij de dagdagelijkse praktijk van incidentprocedures bij zorginstellingen.

Graag zijn wij bereid onze reactie toe te lichten. Hiervoor kunt u contact opnemen met de Nederlandse ggz; info@denederlandseggz.nl