Memo

Onderwerp
Reactie internetconsulatie CBW / NIS 2

Contactpersoon
Afdeling Informatiebeleid

Datum
27 juni 2024

De Nederlandse ggz maakt graag gebruik van de mogelijkheid om te reageren op de online consultatie van het conceptwetsvoorstel “Cyberbeveiligingswet.” Met dit wetsvoorstel wordt de Europese richtlijn NIS2 geïmplementeerd.
De Nederlandse ggz merkt op dat, vanuit het standpunt van CISO’s & IV professionals, de Cyberbeveiligingswet als helpend wordt gezien om het vakgebied van de informatiebeveiliging verder te professionaliseren. De rol die de Raden van Bestuur en indirect de Raden van Toezicht hierin krijgen zullen daar zeker aan bijdragen. Tegelijkertijd moet met deze wetgeving worden voorkomen dat er onnodige extra lasten bij de zorgaanbieders worden gelegd (zowel in relatie tot de bestaande NEN normen, als de effecten ervan in het primaire proces)

de Nederlandse ggz vraagt bij de implementatie van de NIS2 in de Cyberbeveiligingswet aandacht voor:

- Draag zorg dat invoering van deze wet geen extra regeldruk en administratieve last geeft in het primaire en ondersteunende proces.
- Draag zorg dat geen strengere nationale regelgeving wordt opgesteld dan vastgelegd in de Europese wetgeving
- Voorkom separate certificeringstrajecten (in het kader van NEN7510 en NIS2), en streef bij uitwerking naar eenvoud
- Geef instellingen tijd en ruimte om toe te groeien naar het voldoen aan deze wetgeving
- Houd rekening met de effecten voor kleinere instellingen en realiseer waar mogelijk handreikingen.

Het wetsvoorstel geeft ons aanleiding tot specifieke vragen en opmerkingen op de volgende onderdelen.

- Reikwijdte van de wet in relatie tot de verschillende domeinen binnen het zorgstelsel.
    - Uit bijlage 1 maken wij op dat de reikwijdte van de wet met betrekking tot de sector gezondheidszorg zich op dit moment, voor wat betreft de ggz, beperkt tot zorgaanbieders als bedoeld in artikel 1 van de Wet kwaliteit, klachten en geschillen zorg (Wkkgz). Hiermee zijn zorgaanbieders die zorg verlenen in het kader van de Wet maatschappelijk ondersteuning 2015 (Wmo 2015) en/of Jeugdwet uitgesloten van de Cyberbeveiligingswet. Dit geldt in beginsel ook voor instellingen die enkel bestemd zijn voor forensische zorg en waarbij de Beginselenwet verpleging ter beschikking gestelden (Bvt) van toepassing is, namelijk de Forensisch Psychiatrische Centra (FPC’s). Tegelijk dienen deze organisaties op basis van andere wetten en

richtlijnen wel maatregelen in het kader van informatiebeveiliging te nemen. We vragen aandacht voor de gevolgen die het in de praktijk kan hebben als entiteiten zowel Zvw, als zorg vanuit Wmo/Jeugdwet bieden. Denk hierbij bijvoorbeeld aan de meldplicht.

- De fasen van een melding
    - In de tekst ad 1 op blz 25 wordt gesproken over een “significant incident” en dat de entiteit dit “onverwijld” maar uiterlijk binnen 24 uur dient te melden. De term significant incident komt niet voor in de definitielijst van de NIS2, daar wordt gesproken over “significante cyberdreiging”. In deze context vragen we aandacht voor eenduidige terminologie. Tevens vragen we aandacht voor de situaties waar bij een constatering in eerste aanleg nog niet direct tot melding hoeft te leiden, terwijl bij nadere analyse alsnog geconcludeerd wordt dat er wel sprake is van een significante cyberdreiging. Voorkomen moet worden dat elke dreiging geïnterpreteerd moet worden als significant; om achteraf discussie over het niet voldoen aan termijnen te voorkomen. Dat maakt immers de werkzaamheden van entiteiten en CSIRT’s en de toezichthoudende instantie extra complex (het zou helpend zijn als er in dit kader drempelwaarden worden toegevoegd en voorbeelden of handreikingen hiervoor beschikbaar worden gesteld.)
    - Verder vragen wij aandacht voor de extra administratie en procedures die ingeregeld moeten worden om te kunnen voldoen aan de eis dat altijd binnen 24 uur gemeld moet worden bij de CSIRT en toezichthoudende instanties; waarbij wij sterk adviseren om te komen tot één meldloket om zo administratieve druk in te perken.
- Ketenverantwoordelijkheid richting belangrijke Leveranciers die niet direct op eigen ICT systemen zijn aangesloten
    - In onderdeel 5.3.4 sub D staat nu ten aanzien van toeleveringsketen het volgende vermeld: “Ten aanzien van de beveiliging van de toeleveringsketen (punt d) wordt in artikel 21, tweede lid, onderdeel d, en derde lid, NIS2-richtlijn aangegeven dat dit met inbegrip is van beveiliging gerelateerde aspecten met betrekking tot de relaties tussen elke entiteit en haar rechtstreekse leveranciers of dienstverleners. Wanneer essentiële entiteiten en belangrijke entiteiten overwegen welke maatregelen in dit verband passend zijn, moeten zij rekening houden met de specifieke kwetsbaarheden van elke rechtstreekse leverancier en dienstverlener en met de algemene kwaliteit van de producten en de cyberbeveiligingspraktijken van hun leveranciers en dienstverleners, met inbegrip van hun veilige ontwikkelingsprocedures.” Wij vragen ons af op welke wijze essentiële en belangrijke entiteiten zicht kunnen krijgen op specifieke kwetsbaarheden van elke rechtstreekse leverancier en dienstverlener. Het lijkt erop dat dit ook leveranciers en dienstverleners betreft waarbij geen sprake is van ICT gerelateerde (systeem)koppelingen oid. Dat zou kunnen betekenen dat voor elke leverancier van een zorgorganisatie getoetst moet gaan worden op de cyberbeveiligingspraktijken met inbegrip van hun veilige ontwikkelingsprocedures, terwijl er geen directe ICT gerelateerde risico’s te verwachten zijn (denk aan de groenvoorziening, of de aannemer die een verbouwing realiseert). We vragen in dit kader aandacht voor proportionaliteit ter voorkomen van allerlei onnodige administratieve lasten.
- Opleiding en de aantoonbaarheid hiervan
    - In onderdeel 5.4 Governance wordt als eerste genoemd de noodzaak dat het bestuur over voldoende kennis en vaardigheden beschikt om de risico’s voor de beveiliging van de netwerk- en informatiesystemen van de entiteit te kunnen

identificeren, de risicobeheerspraktijken te kunnen beoordelen en de gevolgen van die praktijken voor de door de entiteit aangeboden diensten te kunnen beoordelen. Hierbij ontstaat de indruk dat dit voor alle bestuurders geldt terwijl er in veel gevallen sprake is van een portefeuilleverdeling binnen het bestuur. In het vervolg wordt gesteld dat bestuursleden een cruciale rol spelen in het neerzetten van een sterke cyberweerbaarheidscultuur. Naast de beoordeling van de digitale gezondheid van essentiële entiteiten en belangrijke entiteiten is het ook daarom van belang dat bestuursleden **een training** volgen. Wij ondersteunen de noodzaak dat bestuursleden en RvB dienen te beschikken over een adequaat kennisniveau op dit vakgebied. Wel vragen wij om duidelijkheid over het begrip 'training'. In de NIS2 is geen definitie van training opgenomen en ook in deze wettekst ontbreekt die. Voor besturen is het van belang dat duidelijk is aan welke eisen een training dient te voldoen. Zeker omdat met de zinsnede "en moedigen werknemers binnen hun organisatie aan soortgelijke trainingen te volgen" de suggestie wordt gewekt dat een training voor bestuurders een vergelijkbare inhoud heeft als een training voor het personeel, terwijl dit onzes inziens niet het geval zou moeten zijn.

- Inzet controlefunctionaris
    - We zien een risico bij de inzet van een controlefunctionaris bij met name de kleinere instellingen. Kleinere instellingen zullen geen passende functionaris hebben die deze rol op zich kan nemen. Deze instellingen worden daarmee direct geconfronteerd met extra kosten.

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