Internetconsultatie Cyberbeveiligingsbesluit
Datum
28 Maart 2025

Auteur
Nederlandse Vereniging voor Ziekenhuizen (NVZ)
Contactpersoon Heleen Reijerse, beleidsmedewerker Informatiebeveiliging, Compliance en Privacy, h.reijerse@nvz-ziekenhuizen.nl

Onderwerp
Reactie op de internetconsultatie betreffende het uitvoeringsbesluit van de Cyberbeveiligingswet.
Ingediend op 2. maart 2025, via de website Overheid.nl | Consultatie Cyberbeveiligingswet en het Besluit Weerbaarheid Kritieke entiteiten.
Link naar consultatie Cyberbeveiligingsbesluit:

Overheid.nl | Consultatie Cyberbeveiligingsbesluit

Inleiding
De Nederlandse Vereniging van Ziekenhuizen (NVZ) maakt graag van de mogelijkheid gebruik om te reageren op het concept van het Cyberbeveiligingsbesluit (Cbb). Wij waarderen de mogelijkheid om onze input te kunnen geven. De NVZ draagt graag bij aan een effectieve uitvoering van de Cyberbeveiligingswet (Cbw) voor de aangesloten instellingen. In het algemeen ondersteunen wij het doel om de digitale weerbaarheid van de kritieke sectoren te versterken en de bescherming van (bijzondere) persoonsgegevens te waarborgen.

Echter, wij hebben enkele specifieke aandachtspunten en aanbevelingen op het uitvoeringsbesluit van de Cbw. Daarnaast is tot onze teleurstelling de Ministeriële Regeling niet voor de zorg beschikbaar gekomen, wel voor sommige andere sectoren. Kunnen wij deze nog verwachten, en zo ja komt deze nog voor consultatie beschikbaar? En zo nee, hoe wordt er dan inhoud gegeven aan bijvoorbeeld de eisen ten aanzien van de drempelwaarden voor het melden van incidenten? De delegatiegrondslagen bieden VWS de mogelijkheid om met sectorspecifieke regels te komen, zoals voor de drempelwaarden van de incidenten, maar ook voor het bepalen van proportionele sancties voor de zorg. Het zou fijn zijn als VWS gebruik maakt van deze kans, net als dat voor de andere vitale sectoren is gebeurd.

De NEN7510 of ISO 27001 als de basis voor cyberbeveiliging
De NVZ betreurt het zeer dat in het uitvoeringsbesluit geen onderscheid is gemaakt tussen bestaande vereisten vanuit de wet en de al bestaande NEN 7510 en/of ISO 27001 norm.
Dat brengt onnodige verzwaring van administratieve lasten met zich mee.
Nu staan er grotendeels eisen in het uitvoeringsbesluit die ook al in de normen staan. Het is aan de instellingen zelf om te onderzoeken wat er nog extra moet worden gedaan. In de toelichting en op de website wordt wel de ISO 27001 genoemd, maar in het Cbb missen wij het benoemen van de NEN 7510 en/of ISO 27001 norm als basis voor de cyberhygiëne van een organisatie. Zouden

deze normen wél als basis genoemd worden, dan konden er vanuit het Cbb aanvullend eisen worden gesteld waaraan moet worden voldaan om de cybersecurity op orde te krijgen. Denk aan uitbreiding van het leveranciersmanagement met een ketenverantwoordelijkheid of de aantoonbaarheid daarvan. Of aan de maatregel ten aanzien van de "doorlopende" monitoring van back-ups, wat nu niet in de norm staat. Onze conclusie is dat het veel sterker en logischer is om vanuit wetgeving naar de normen te verwijzen. En in het besluit aanvullende maatregelen te eisen conform de Cbw.

Het risico gestuurd werken conform de NEN 7510 en de Cbw is de basis van een goed cybersecuritybeleid. Het is echter niet gepast om via de nota van toelichting op de Cbb de reikwijdte van de Cbw (NIS2) te vergroten tot het bredere risicobeheerproces van een entiteit. Hiermee ontstaat een verschil met de oorspronkelijke Europese tekst en de Nederlandse omzetting daarvan. Deze huidige situatie werkt tevens verwarring in de hand omdat een instelling met deels overlappende tekst te maken krijgt. De NVZ voorziet veel discussie met auditoren van de NEN7510, met name over de aantoonbaarheid van de toepassing. Ons advies is: geef onder hoofdstuk 4.3 expliciet aan dat een organisatie aantoonbaar moet voldoen aan de laatste versie van de norm, in dit geval NEN7510:2024 en/of ISO 27001:2022. En haal datgene wat ook in de norm staat uit het uitvoeringsbesluit; dat maakt de implementatie onnodig complex.

Administratieve lasten beperken

Er zijn bepaalde uitgewerkte maatregelen die een enorme administratielast gaan opleveren en niet automatisch zullen leiden tot verbetering van de informatiebeveiliging. Denk daarbij aan:

- Artikel 8, het niet alleen registreren maar ook moeten analyseren en classificeren van de bijna-incidenten en kwetsbaarheden. Dagelijks ontvangen onze leden grote hoeveelheden meldingen, adviezen over kwetsbaarheden en updates/patches vanuit bijvoorbeeld softwareleveranciers. Kan worden verhelderd of het aantoonbaar uitvoeren van reguliere patchrondes, waarbij leveranciers vele kwetsbaarheden oplossen, voldoende zijn als dergelijk bewijslast? Of dient ieder melding apart voorzien te worden van een beoordeling met bijbehorende schriftelijk bewijslast? Afhankelijk van de duiding kan voorgaande verplichting namelijk leiden tot extra administratieve lasten ten aanzien van het vastleggen van die schriftelijke bewijslast.
- Artikel 10 beveiliging van de toeleveringsketen. In lid 2 en 3 ontbreekt de risico gebaseerde benadering. Als de tekst, zoals bij sub 1 gesteld, vaststelt aan welk eisen de relatie met leveranciers moet voldoen, kan ook vastgesteld worden dat bij geringe afhankelijkheid geen aanvullende maatregelen nodig zijn. Daar bieden sub 2 en 3 nu geen ruimte voor.
- Artikel 17, hoe om te gaan met attenderingen, adviezen en informatie. Het besluit geeft nu aan dat deze altijd beoordeeld moeten worden en de uitkomst daarvan moet worden vastgelegd. Waarom is niet gekozen voor een risico-gestuurde aanpak? In relatie tot de dagelijkse hoeveelheid meldingen die binnenkomen is dat niet in verhouding.
- 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 Cbb introduceert, en die een behoorlijke belasting legt op de entiteiten.
- Artikel 28, verstrekking overige informatie. , Lid 3, sub b: bij elke domeinnaamregistratie moet ook melding gedaan worden bij het Nationaal register. Kan hier geen verplichting gesteld worden aan de eigenaar van het domeinregister (SIDN of andere partijen) in plaats van bij de zorgaanbieder?

Bovenstaande voorbeelden passen niet bij de afspraken zoals gemaakt in het IZA om de administratieve last maximaal op 20% van de werktijd te houden van een zorgverlener.
Daarnaast zien wij als NVZ een disbalans tussen compliance en de praktische werkbaarheid en uitvoerbaarheid van de eisen. De specifieke benamingen sluiten niet aan bij wat er nu gehanteerd wordt binnen de zorg op basis van de NEN 7510. Het besluit vraagt tevens om het veelvuldig opstellen en invullen van diverse documenten, waarvan de meeste al aanwezig zijn conform de NEN 7510.
Maar het is vooral de plicht om het toepassen van beleid aan te tonen, die ons zorgen baart. Dit leidt tot een behoorlijke toename van de administratieve regeldruk, terwijl de NIS2-richtlijn juist stelt dat er een billijk evenwicht moet zijn tussen de op risico gebaseerde eisen en verplichtingen enerzijds en de administratieve lasten die voortvloeien uit het toezicht op de naleving anderzijds. De regeldruk ingevolge de Cbw zal veel capaciteit en middelen van onze leden vragen terwijl die juist vooral nodig zijn voor het investeren in noodzakelijke cybersecuritymaatregelen en het toetsen van de effectiviteit ervan.

Hoofdstuk 4 Zorgplicht
De NVZ constateert dat het in de praktijk, met name voor de kleinere instellingen, heel veel moeite kost om de rollen, verantwoordelijkheden en bevoegdheden gescheiden uit te laten voeren. Het kost al heel veel moeite om überhaupt geschikt personeel te vinden op het gebied van security. De toevoeging: "daar waar mogelijk", doet meer recht aan de werkelijkheid.
Het is belangrijk dat het uitvoeringsbesluit evenwichtig is en rekening houdt met de specifieke uitdagingen waar de zorgsector voor staat. Dat is ook dat de kosten en baten in balans moeten zijn om patiëntenzorg te kunnen blijven bieden. Voor kleinere instellingen in de zorg en ook voor andere kleine, vitale organisaties, is er tevens het verzoek om op basis van het beginsel van zorgvuldigheid oog te hebben voor de proportionaliteit in de wet en het besluit, zowel op het gebied van de sancties als de audit- en administratieve last.

Hoofdstuk 5 Training
In artikel 20 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 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 in de NEN 7510 reeds is geborgd) centraal staat. Het voert ons inziens te ver om technische kennis op het vlak van de dreiging van malware, insiders threat en DDoS-aanvallen onderdeel van een training te laten zijn. Het gaat om de risico's en de daarbij behorende impact op de zorgprocessen en te nemen maatregelen.

Investeringen in bewustwordingscampagnes en opleiding van personeel zijn cruciaal om cyberdreigingen te verminderen. Dat geldt niet alleen voor de raad van bestuur (RvB), maar ook voor leden van het Medische stafbestuur (MSB). Zij zijn direct betrokken zijn bij het integraal risicomanagement, dus ook op het gebied van cybersecurity. Deze groep zou expliciet als betrokkenen kunnen worden genoemd in de Ministeriële Regeling. Dat geeft herkenning. Juist kennis van de risico's maakt dat er beter gehandeld wordt vanuit de top van de organisatie. Het onderschrijft ook het belang van een breed draagvlak in de organisatie voor dit onderwerp. Een realistisch vereist kennisniveau bevordert het gevoel van eigenaarschap, niet alleen bij de RvB, maar ook bij het MSB. Dat gaat over het belang van een goed functionerend Information Security Management Systeem (NEN7510) en daarmee inzicht hebben in de risico's en bijbehorende beheersmaatregelen.

De NVZ pleit er tevens voor dat er naast de beschreven eisen voor de opleiding voor bestuurders, ruimte is voor andere vormen van kennisoverdracht, in plaats van om de 2 jaar dezelfde training moeten volgen. Denk aan een variant waarbij bestuurders hun kennis op peil houden door bijvoorbeeld CPE-punten te verkrijgen middels webinars, congressen, of een masterclass. De punten die daarbij verkregen kunnen worden zijn samen dan gelijk aan de punten voor een training zoals beschreven in het Cbb. Dat is vergelijkbaar met hoe ook de informatiebeveiligers hun kennis up-to-date houden na het behalen van hun certificaat. Dit bevordert regelmatige scholing, waarbij er altijd aandacht zal zijn voor de risico's en de daarbij behorende beheersmaatregelen die op dat moment actueel zijn, zoals over nieuwe technieken als post quantum cryptografie, AI of nieuwe risico's op basis van de geopolitiek.

Hoofdstuk 6 Melding van significant incidenten, incidenten, bijna-incidenten, significantie cyberdreigingen, cyberdreigingen en kwetsbaarheden

Het doel van het melden is om onze zorgsector samen veiliger te maken. Dat betekent dat er goed nagedacht moet worden over wat we waar en wanneer melden. De melding moet een bijdrage leveren aan dat doel. De NVZ pleit opnieuw voor een evenwichtige benadering van meldplicht bij incidenten, waarbij duidelijke minimale grenswaarden zijn aangegeven. Laten we daarbij proberen de administratieve last tot een minimum te beperken, zowel voor onze leden als voor Z-CERT. Geef duidelijk aan wat wordt verstaan onder *significant* in de Ministeriële Regeling, specifiek voor de zorgsector. Het lijkt ons tevens niet de bedoeling dat ook de incidenten gemeld moeten worden die niet direct een impact hebben op de bedrijfsvoering.

De NVZ heeft meegewerkt aan het onderzoek, in opdracht van VWS, dat heeft geleid tot een rapport met drempelwaarden om incidenten te melden in het kader van de nieuwe wetgeving. Bij de review voelden wij als geïnterviewden vanuit de zorg en Z-CERT ons niet gehoord. Het was nog steeds niet concreet, en het gevoel bleef dat er met onze opmerkingen niets werd gedaan. Er staan te vage drempelwaarden in die onze leden niet gaan helpen bij de beslissing of een incident significant is en dus gemeld moet worden conform dit besluit.
De NVZ hoopt dat in de Ministeriële Regeling heldere en concrete drempelwaarden worden opgenomen. Ons advies is: leg de focus op continuïteit van de dienstverlening bij het opstellen van de drempelwaarden voor de meldplicht, en voorkom een stapeling van drempelwaarden. Na afstemming met de diverse brancheorganisaties binnen zorg willen we VWS verzoeken om zoveel mogelijk in te zetten op aansluiting bij bestaande incidentprocessen (calamiteiten bij de IGJ en datalekken bij de AP) en daar gehanteerde en bekende parameters.
Daarnaast lijkt het ons verstandig om in het eerste jaar een referentiekader op te bouwen en te evalueren, samen met Z-CERT en de betrokken instellingen, om de criteria bij te kunnen stellen.

Als de criteria, zoals aangegeven in het besluit, pas na vier jaar mogelijk worden herzien, wordt ingeboet op actualiteit en de mogelijkheid om maatregelen te nemen om administratieve last te verminderen of nieuwe vormen van incidenten toe te voegen.

Bewaartermijn Logging
Het gaat in het uitvoeringsbesluit voornamelijk om "technische" logging. Maak daar onderscheid in ten opzichte van logging van patiënt/persoonsgegevens (nu 5 jaar bij wet). Bij technische logging is het ongebruikelijk om langer dan een jaar terug te kijken. Waarom is hier voor 60 maanden gekozen? Bij een incident kijk je vooral naar recente logging. Het geeft steeds meer druk op de opslagcapaciteit en energiegebruik en dus de daarbij behorende kosten. Ons advies is: pas dit aan naar 1 jaar, dat geeft duidelijkheid en veel ruimte voor organisaties om al hun technische logging maar 1 jaar te hoeven bewaren. Er komt alleen maar meer data bij in de loop der tijd, probeer daar waar het kan met regelgeving te minimaliseren.

Samengevat zijn dit de belangrijke punten:

- Herzie de huidige opzet van het Cbb en stel het besluit op aan de hand van duidelijke doelvoorschriften, zoals het aantoonbaar voldoen aan de NEN 7510 of ISO 27001, waarbij de invulling in termen van risico-gebaseerde en proportionele maatregelen aan onze leden zelf is.

- Beperk de administratieve belasting, terwijl de NIS2-richtlijn juist stelt dat er een billijk evenwicht moet zijn tussen de op risico gebaseerde eisen en verplichtingen enerzijds en de administratieve lasten die voortvloeien uit het toezicht op de naleving anderzijds, ziet de NVZ in het Cbb juist het tegendeel gebeuren.

- Kies expliciet voor een risico-gebaseerde benadering voor toezicht en handhaving, waardoor met name de kleinere zorgorganisatie naar eigen inzicht de ruimte krijgen voor de specifieke invulling van hun beheersmaatregelen in relatie tot hun geïdentificeerde risico's.

- Stel een Ministeriële Regeling op voor de Zorg en met een evenwichtige benadering van de meldplicht bij incidenten, met duidelijke minimale drempelwaarden en voorbeelden. Heb daarbij oog voor de proportionaliteit, zowel op het gebied van de sancties als op het gebied van de audit- en administratieve lasten.

Laten we samen blijven werken aan een veilig en veerkrachtig digitaal landschap.
Namens de NVZ waarderen wij uw inzet en bijdrage aan de totstandkoming van dit uitvoeringsbesluit op het gebied van cyberbeveiliging. De NVZ kijkt uit naar de herziene versie en de Ministeriële Regeling voor de Zorg.

Veronique Esman, directeur
NVZ - Nederlandse Vereniging van Ziekenhuizen