Overheid.nl | Consultatie Cyberbeveiligingsbesluit

DATUM
28 maart 2025

KENMERK
B20250328HH

BETREFT
Consultatie Cyberbeveiligingswet

BIJLAGEN
-

CONTACT
HAN HUIZINGA

TELEFOON
06-13197186

E-MAIL
HHUIZINGA@VGN.NL

Geachte lezer,

De VGN maakt graag gebruik van de mogelijkheid om te reageren op het voorgestelde Cyberbeveiligingsbesluit (Cbb). In grote lijnen ondersteunen wij het doel van het versterken van de digitale weerbaarheid van zorgaanbieders, maar wij hebben wel enkele aandachtspunten bij de tekst die nu voorligt.

Cyberbeveiligingsbesluit en NEN7510
Wat ons betreft is onvoldoende helder welke aanvullende eisen het Cbb stelt bovenop de eisen vanuit de NEN7510. Hiermee ontstaat het risico van discussie over de vraag wanneer een organisatie wel of niet voldoet aan de gestelde eisen. Wij verwachten dat de door ons gewenste duidelijkheid kan worden bereikt door de verschillende eisen niet op te nemen in het Cbb, maar te verwijzen naar de onderliggende normen. De normen worden bovendien periodiek geactualiseerd zonder dat daar wetswijzigingen voor nodig zijn. De actuele norm is dan de eenduidige maatstaf waaraan zorgaanbieders moeten voldoen.

Administratieve lasten
Veel van de eisen in het Cbb roepen het beeld op van een administratieve werkelijkheid die niet per se bijdraagt aan betere zorg en veiliger omgaan met data. Met name de eis om aantoonbaar toe te passen (art. 6 lid 1) vereist wat ons betreft een meer specifieke omschrijving, zodat vooraf helder is op welke manier precies moet worden aangetoond dat wordt voldaan aan de gestelde eisen.

Zorgplicht
In de gehandicaptenzorg zijn veel kleine zorgorganisaties actief, waarbij een strikte scheiding van rollen, verantwoordelijkheden en bevoegdheden niet altijd in persoon te realiseren is. Daarnaast is het aanbod van deskundigheid op het gebied van cybersecurity beperkt en duur. Wij zien op dit punt dan ook

Bezoekadres
Oudlaan 4
3515 GA Utrecht

Postadres
Postbus 413
3500 AK Utrecht

+31 (0)30 273 93 00
info@vgn.nl
vgn.nl

graag een nuancering van de zorgplicht, die recht doet aan wat er redelijkerwijs mogelijk is, zodat organisaties in staat worden gesteld om hun beveiliging op niveau te brengen en houden zonder dat zij daarvoor buitensporige kosten hoeven te maken.

Training
Verminderen van cyberbedreigingen vraagt wat ons betreft integraal risicomanagement. Daarin hebben bestuurders een rol, maar zeker ook Raden van Toezicht, managers, ICT-coördinatoren en zorgmedewerkers. Deze betrokkenen wordt recht gedaan wanneer ook hun rol met betrekking tot cybersecurity wordt genoemd in het Cbb.
Daarnaast is het belangrijk dat heldere kaders worden gesteld. Wat is de minimale verplichting van een bestuurder? En hoe blijft een organisatie gecertificeerd? Wij zien graag meer duidelijkheid over de minimale vereisten aan een training, zodat discussies daarover worden voorkomen. Daarbij is het zeker zo belangrijk om cybertraining voor medewerkers goed te organiseren. Het is ons niet duidelijk of en welke eisen daaraan worden gesteld.

Meldingsplicht
Om te kunnen leren van elkaars kwetsbare punten is het belangrijk om inzicht te hebben in meldingen (referentiekader). Dat kan in onze ogen goed in de vorm van een monitor waarmee op hoofdniveau inzichtelijk is hoe vaak er iets wordt gemeld, wat de impact/urgentie is en welke maatregelen worden getroffen. Een belangrijke voorwaarde is dat de informatie niet herleidbaar is naar een specifieke organisatie.

Artikelgewijs
In aanvulling op bovengenoemde punten geven wij hieronder nog enkele opmerkingen bij specifieke artikelen mee.

Artikel 8. (Incidentbehandeling)
In dit artikel wordt gesproken over registreren (loggen). Wat wij hier missen is de opvolging van incidenten in de vorm van maatregelen die essentieel zijn om in de toekomst preventief te kunnen handelen.

Artikel 12 (basispraktijken op het gebied van cyberhygiëne en opleiding op het gebied van cyberbeveiliging)
Bij dit artikel 12 zouden wij ook graag een beschrijving zien welke (verplichte) rollen van belang zijn (denk aan een security-officer), een afdeling die bewustwording van medewerkers continue opvolgt en af en toetst of medewerkers correct reageren bij cyber-aanvallen (denk ook aan het verzenden van nep-berichten door de eigen organisatie om te checken of

medewerkers goed handelen; dit geeft tevens het volwassenheidsniveau weer van een organisatie).

Artikel 14 (beveiligingsaspecten ten aanzien van personeel)
Hier wordt gesproken over personeel en andere binnen de entiteit werkende personen. In onze ogen is het duidelijker wanneer gesproken wordt over medewerkers binnen de organisatie en externen.

Artikel 15 (beveiligingsaspecten ten aanzien van toegangsbeleid)
Dit artikel gaat over toegang van het netwerk. Er wordt eenvoudig verwezen naar beleid, maar organisaties zullen wel het netwerk voor medewerkers én cliënten gescheiden moeten houden. In de gehandicaptenzorg maken cliënten en medewerkers vaak gebruik van één infrastructuur, die dus goed dient te worden ingeregeld. Wij adviseren om dit aspect te benoemen in de toelichting bij dit artikel.

Ter afsluiting
De VGN ondersteunt in grote lijnen het doel van het versterken van de digitale weerbaarheid van zorgaanbieders. Daarbij hebben we enkele aandachtspunten die betrekking hebben op het verduidelijken van de bedoeling en enkele aandachtspunten die voortkomen uit de specifieke situatie in de gehandicaptenzorg. Wij verwachten dat onze opmerkingen bijdragen aan een beter besluit met draagvlak onder zorgaanbieders. Wanneer u naar aanleiding van onze inbreng vragen heeft, kunt u contact opnemen met Han Huizinga, beleidsadviseur E hhuizinga@vgn.nl of M 06-13197186.

Met vriendelijke groet,

Theo van Uum
directeur