Onderwerp Internetconsultatie Cyberbeveiligingsbesluit
Datum 27 maart 2025

ActiZ maakt graag gebruik van de mogelijkheid om te reageren op de internetconsultatie van het cyberbeveiligingsbesluit. Wij onderschrijven het belang van het Cyberbeveiligingsbesluit (Cbb) als uitwerking van de Cyberbeveiligingswet (Cbw). Tegelijkertijd zien wij op cruciale punten onduidelijkheden voor de zorgsector.

Relatie met NEN7510 en ISO27001
In de toelichting bij de internetconsultatie van het Cyberbeveiligingsbesluit (Cbb) wordt bij "In het kort" vermeld dat het Cbb grotendeels aansluit op bestaande normenkaders (NEN 7510 en ISO 27001). De bijgevoegde concept ministeriële regeling noemt het ministerie van VWS echter niet. Dit creëert onzekerheid over de rol van de NEN 7510 als normatief uitgangspunt voor de zorg. in het uitvoeringsbesluit geen onderscheid gemaakt op wat aanvullend vereist wordt vanuit de wet op de al bestaande NEN 7510 en ISO 27001 norm. Duidelijkheid vanuit het ministerie van VWS over deze verhouding is gewenst.

Terminologie en beleidseisen
Het Cbb schrijft voor in artikelen zoals 6 en 7 dat essentiële en belangrijke entiteiten schriftelijk vastgesteld beleid moeten hebben en dit aantoonbaar toepassen. Bijvoorbeeld beleid voor incidentbehandeling (NEN7510 heeft het over een proces), beleid voor de beveiliging van de toeleveringsketen, beleid voor beheer en de werking van netwerk- en informatiesystemen. Daarnaast spreekt de Cbb consequent over beleid over beveiliging van netwerk- en informatiesystemen. ISO27001 hanteert de term informatiebeveiligingsbeleid. Hiermee wijkt de Cbb af of hanteert in ieder geval andere terminologie van de normteksten op deze gebieden in ISO27001 en NEN7510.

Omdat andere termen worden gebruikt is het onduidelijk of deze Cbb eisen afwijken van NEN7510:2024 of ISO27001:2022 en is het dus de vraag of Cbb beoogd aanvullende eisen stelt aan organisaties die voldoen aan NEN7510:2024 of ISO27001:2022.

Dit roept de volgende vragen op:

- Wat verstaat het Cbb onder beleid over beveiliging van netwerk- en informatiesystemen, is dat gelijk aan het informatiebeveiligingsbeleid conform definitie van ISO27001 en NEN7510?
- Wat betekent dit voor organisaties die (al) aantoonbaar voldoen aan NEN7510:2024 of ISO27001:2022?

Het zou onrust wegnemen als er op korte termijn duidelijkheid hierover zou zijn, dan weten organisaties die nu met implementatietrajecten bezig zijn waar ze aan toe zijn.

Sectoraal maatwerk

Artikel 19 van de Cbb biedt de mogelijkheid om de zorgplicht sectoraal in te vullen via ministeriële regelingen, maar ook hier is het belangrijk dat er snel duidelijkheid komt. Ook hierover leven vragen:

- Houdt VWS rekening met het voorkomen van dubbele normering, gezien het feit dat de zorgsector reeds aantoonbaar moet voldoen aan de NEN7510, NEN7512 en NEN7513?
- Komen er aanvullende maatregelen bij, vervallen er maatregelen uit het besluit of worden bestaande maatregelen aangepast om deze beter in lijn te brengen met de NEN 7510 zoals bijvoorbeeld de betrouwbaarheidseisen. De extra betrouwbaarheidseisen in het Cbb komen in de NEN7510 al terug onder mensgerichte beheersmaatregelen (NEN7510 6.1 - screening). Is de NEN7510 hiermee voldoende of wordt een uitgebreidere screening verlangd?

Definitie "past aantoonbaar toe"

Het begrip 'past aantoonbaar toe' (artikel 6, lid 1) vraagt om verduidelijking. Concrete richtlijnen hierover, in aansluiting op bestaande toetsingskaders zoals NEN 7510-certificeringen en auditrapportages, zouden helpen.

Beveiligingsincidenten

Artikelen 25 en 26 geven onduidelijkheid over de regie bij beveiligingsincidenten: ligt de verantwoordelijkheid bij de zorgorganisatie, de leverancier of het aangewezen CSIRT (Z-CERT voor de zorg)? Dit roept praktische vragen op, bijvoorbeeld bij incidenten met of zonder datalekken, of kwetsbaarheden in applicaties en devices. Het is essentieel dat voor alle betrokken partijen helder is wie verantwoordelijk is, zodat mitigerende maatregelen snel kunnen worden geïmplementeerd. Tegelijkertijd moet een pragmatische aanpak worden gehanteerd. Een centraal incidentenregister zou kunnen voorkomen dat meerdere zorgorganisaties afzonderlijk hetzelfde beveiligingsincident melden bij het aangewezen CSIRT (Z-CERT voor de zorg). In samenwerking met de brancheorganisaties, zoals ActiZ, zouden er bijvoorbeeld duidelijke afspraken met Z-CERT en belangrijke softwareleveranciers kunnen worden gemaakt.

Testen met leveranciers

Artikel 9 roept vragen op over het organiseren van testen met SaaS-leveranciers. Wordt verwacht dat zorgorganisaties jaarlijks samen met de leverancier een failover-test uitvoeren? Een handreiking met minimale testfrequenties en types, afgestemd op de kriticiteit van de geleverde diensten, kan hierbij helpen.

Drempelwaarde voor significante incidenten

De memorie van toelichting bij artikel 24 van het Cbb verwijst naar criteria voor het duiden van een significant incident als bedoeld in artikel 25, tweede lid, van het Cbw. In opdracht van het ministerie van VWS heeft een adviesbureau deze criteria ontwikkeld, waarbij het veld is betrokken. De uitkomsten hiervan zijn teruggekoppeld aan vertegenwoordigers van verschillende subsectoren binnen de zorg. Tegelijkertijd constateren wij dat het voorgestelde kader voor deze criteria onnodig complex is en niet aansluit bij de praktijk van incidentprocedures binnen zorginstellingen. Er ontbreekt draagvlak onder onze achterban.

Het is wenselijk dat het ministerie van VWS helderheid schept over de toepassing van deze criteria in de zorgsector en in overleg met het veld komt tot eenvoudigere, praktijkgerichte uitgangspunten. Daarbij zou het helpend zijn als het ministerie sub sectoraal onderzoek doet om zorginstellingen vanuit hun dagelijkse praktijk te betrekken. Dit voorkomt onduidelijkheid en zorgt ervoor dat instellingen die nu hun processen willen inrichten, weten waar zij aan moeten voldoen.