Graag maak ik van de gelegenheid gebruik om commentaar te geven op de implementatie van de NIS2 Richtlijn zoals die thans voor consultatie voorligt. Ik baseer mij daarbij op 40 jaar ervaring met betrouwbaarheidszorg binnen met name de Rijksoverheid en de Ziekenhuissector.
Voor de volledigheid: deze reactie is geschreven op persoonlijke titel.

KERN

Kern van mijn reactie:
1) Verkeerde naam (belemmert implementatie)
2) Onvoldoende aandacht voor problematiek van schaarse deskundigheid (zowel kennis als ervaring); dit werkt in de onderdelen hierna door;
3) Slechte uitwerking van de 'overall' governance:
   a) Versnipperde en daarmee onvoldoende slagvaardig voor grootschalige incidenten (overall en qua CSIRT);
   b) Strijdigheid met scheiding der machten en daarmee risico's op gebrek aan eenduidigheid/transparantie dan wel onvoldoende ingrijpen waar dat nodig is (toezicht);
   c) Vraag of er ook daadwerkelijk ingegrepen gaat worden tegen monopolisten en grote (buitenlandse) leveranciers wanneer dat nodig is om tot toereikende beveiliging te komen.
4) Geen aandacht voor de praktijk:
   a) Zelfregulering via voldoen aan ISO-27000 serie (c.q. NEN-7500 serie)
   b) Certificering van auditors en hackers/pentesters
   c) Goede beveiliging geen 100% garantie
   d) Het tegengestelde bereiken van wat beoogd wordt
   e) Verkeerde inschatting kennis bestuurders c.q. wat zij kunnen verwerven
5) Diverse slordigheden/inconsistenties
6) Te vrijblijvende teksten in Memorie van Toelichting (MVT).

NADERE UITWERKING

Onderstaand volgt een nadere uitwerking van deze kernpunten.

1. Advies voor andere naam van de wet
   De NIS2 richtlijn wordt geïmplementeerd via Cyberbeveiligingswet. Cyber is een toevoeging aan informatiebeveiliging / security die pas een aantal jaren in zwang is vanuit de opkomst van het internet. Blijkens de inhoud van het Memorie van Toelichting gaat het echter niet alleen om ' cyber' maar ook om het domein van fysieke beveiliging. Mijn ervaring is dat fysieke beveiliging in organisaties veelal op geheel andere plaatsen is belegd dan informatiebeveiliging (huisvesting en techniek versus ICT). Ook is gebleken dat deze onderdelen veelal geen behoefte hebben om informatiebeveiliging mee te nemen en zich maar moeilijk van de vele raakvlakken laten overtuigen. Als hen verteld wordt dat zij zich moeten houden aan een wet die begint met 'cyber' dan zal dat al een reden van weerstand zijn. [Door geheimhoudingsplicht kan ik dit niet met voorbeelden onderbouwen!].

2. Schaarse deskundigheid (zowel kennis als ervaring)
   In de gehele westerse wereld is er een tekort aan deskundigen op het gebied van (cyber) security. Dit betreft dan zowel theoretische kennis als praktische ervaring. Organisaties moeten de grootste moeite doen om vacatures vervuld te krijgen. In Bijlage 1 van de Nationale Technologiestrategie, Agenda Cybersecurity Technologies, geeft de overheid zelf aan dat het pas in 2035 zal lukken om deze problematiek op te lossen.
   Dit wetsvoorstel schetst het beeld van een enorme extra behoefte aan medewerkers met de juiste kennis en ervaring. Dit raakt zowel de organisaties zelf, de CSIRTs als het toezicht. [Dit aspect komt

ook terug in het onderliggende onderzoek naar de gewenste CSIRT structuur maar is m.i. daarin verkeerd gewaardeerd en daardoor onvoldoende gewogen]. Los van de constatering dat deze deskundigheid er onvoldoende is, zal dit leiden tot onderlinge concurrentie en hogere salarissen om die vacatures te vervullen dan wel bestaande medewerkers te behouden. Het bij elkaar wegkopen van mensen is voorst slecht voor de continuïteit van kennis en ervaring.

3. Slechte uitwerking van de 'overall' governance
   Het wetsvoorstel lijkt erop gericht om alle betrokkenen zoveel mogelijk tegemoet te komen. Er lijkt geen aandacht voor voornoemde problematiek van schaarse deskundigheid, het belang van een eenduidige commandostructuur en heldere informatie- en rapportagelijnen zoals vereist om (grootschalige) incidenten te kunnen aanpakken. Er is sprake van versnippering met teveel communicatielijnen en coördinatiepunten. Op enkele elementen zoom ik hierna nader in.
   a. Andere keuze voor inrichting CSIRT; advies: één organisatie
      Om redenen als schaarse kennis en ervaring, efficiency, transparantie/eenduidigheid en snelheid van handelen zou mijn voorkeur uitgaan naar één centrale CSIRT. Iedere aparte CSIRT zal moeite hebben met verkrijgen en behouden van voldoende personeel. Aparte CSIRT leiden tot extra kosten van management en ondersteuning. Voorts gaat dit ten kosten van de slagvaardigheid terwijl bij grootschalige cyber incidenten juist snel en voortvarend gereageerd moet kunnen worden. Zowel van organisaties naar CSIRT, omgekeerd als naar andere betrokkenen. Daarbij zijn mijn ervaringen met Z-CERT zodanig dat dit geen aparte CSIRT voor de sector rechtvaardigt. Daar waar er binnen de zorg nu juist een sectorale norm ligt via NEN-7510 (zie ook verderop onder 6c) maken zij producten (o.a. inzake leveranciersmanagement) die niet NEN-7510 als basis/uitgangspunt kennen, maar een binnen de zorg nauwelijks gebruikt ENISA document. Voorts blijken veel van hun signaleringen rechtstreeks afkomstig te zijn van het NCSC. Mijn beeld is dan ook dat het een betere oplossing zou zijn om één CSIRT te hanteren, waarbij deze dan desgewenst specialisten per sector kan huisvesten. Alle informatiestromen (kwetsbaarheden, incidenten, e.a.) moeten ook via deze ene CSIRT lopen.
   b. Andere keuze voor inrichting toezicht; advies: één toezichthouder en Trias Politica
      Wat hiervoor gesteld is voor CSIRT geldt mutatis mutandis ook voor het toezicht. Een toezicht dat verdeeld is over teveel partijen, zal niet efficiënt kunnen werken en problemen krijgen met de bemensing. Zeker als je ziet dat deze toezichthouders ook nog eens zelf beveiligingsaudits, vulnerabilitycans en penetratietesten zouden moeten gaan uitvoeren. In de zorg heb ik te maken gehad met toezicht vanuit IGJ en de Autoriteit Persoonsgegevens op het gebied van informatiebeveiliging. Beide waren niet of nauwelijks in staat om de aard en complexiteit van informatiebeveiliging in de volle omvang aan te pakken, laat staan dat ze zelf in staat zijn tot genoemde scans en testen.
      Voorstel is dan ook om – net als bij CSIRT – maar één toezichthoudende autoriteit op het gebied van informatie- en netwerkbeveiliging te hanteren. IGJ en AP zouden hun bevoegdheden op het gebied van informatiebeveiliging aan deze toezichthouder moeten overlaten. Hierbij zou de toezichthouder een getrapte benadering gehanteerd moeten worden. Dit is dat de onder de NIS2 richtlijn vallende entiteiten aantoonbaar voldoen aan gestelde beveiligingsnormen. Aantoonbaar via een certificering of rapportage van een onafhankelijke IT-auditor (NOREA). De naleving kan dan in eerste instantie gericht worden op organisaties die niet beschikken over een dergelijke certificering of rapportage. Organisaties die hierover wel beschikken kunnen steekproefsgewijs of naar aanleiding van concrete incidenten onderzocht worden.
      Dit pleit ervoor om ook het toezicht zoveel mogelijk in één centrale organisatie onder te brengen. M.i. de enige mogelijkheid om een basis aan kennis en ervaring binnen te halen. Voorts dienen deze organisaties dan voldoende budget te hebben om vanuit de markt partijen in te huren voor gedetailleerde en complexe audits en scans.
   c. Voldoende mandaat om echt in te grijpen? Gaat er ook ingegrepen worden?
      Sinds 2018 ben ik na de invoering van de AVG betrokken geweest bij het afsluiten van vele

(verwerkers)overeenkomsten met leveranciers inclusief het maken van afspraken over informatiebeveiliging. Hierbij is gebleken dat je als middelgrote organisatie vrijwel machteloos staat tegen grote (buitenlandse) leveranciers. In diverse gevallen is het mogelijk gebleken om door samenwerking onder de vlag van de NVZ toch nog tot afspraken te komen. Dit lukte echter niet altijd zodat er risico's voor de informatiebeveiliging overbleven (m.n. remote toegang voor support door de leverancier). Bij een bekende zorgleverancier is zelfs geprobeerd dit aan te kaarten bij de AP. Inmiddels hebben noch het Ministerie, noch de AP en noch de ACM op dit punt thuisgegeven. Organisaties hebben duidelijk behoefte aan een verantwoordelijke en/of toezichthouder die daadwerkelijk in durft te grijpen tegen leveranciers en daarmee de organisaties ondersteunt.

4. Onvoldoende aandacht voor de praktijk, praktische uitvoerbaarheid en kosten
   a. Onvoldoende aansluiting op gebruikelijke praktijken; zelfregulering
      In de MvT wordt slechts summier gewezen op het feit dat organisaties zelf als normenkader kiezen voor de ISO-27000 serie. Dit doet geen recht aan de praktijk. Mijn ervaring is dat de meeste leveranciers van IT- en netwerkdiensten dit niet alleen gekozen hebben als normnekader maar daar ook tegen gecertificeerd zijn (m.n. ISO-27001). Dit is breed geaccepteerd als 'hygiëne factor voor informatiebeveiliging'. Zo is het na de invoering van de AVG in 2018 een goed gebruik om voor de uitbesteding van de verwerking van persoonsgegevens zogenaamde verwerkersovereenkomsten af te sluiten. Deze kennen ook een verplichte beveiligingsparagraaf. Deze bestaat veelal uit een basis dat de verwerker moet beschikken over (o.a.) een ISO-27001 certificering en verplicht is deze te onderhouden, aangevuld met specifieke afspraken / verdiepingen over bepaalde maatregelen (zoals encryptie, 2FAMFA, e.d.).
      In diverse reacties en adviezen op de 10 maatregelen in de NIS2 is aangegeven dat deze een directe link hebben met ISO-27001 en dat een organisatie die voldoet aan ISO-27001 ook al grotendeels aan deze 10 maatregelen zal voldoen. Wat aanpassingen zullen o.a. nodig zijn om de incident(meld)processen te laten aansluiten op NIS2.
      Het wetsvoorstel was *de* gelegenheid geweest om in een appendix aan te geven welke aanpassingen naar de mening van de wetgever nodig zouden zijn op de basis ISO-27001/2 implementatie om tevens te voldoen aan NIS2. Een gemiste kans. Nu bestaat het risico dat iedere toezichthouder een eigen interpretatie zal hanteren. Een risico dat door het gebrek aan kennis (zie onder punt 2 hiervoor) zeer reëel te achten is.
   b. Certificering van auditors en hackers/pentesters
      Nederland kent een hoog niveau van IT-audit via de NOREA. Ook bestaan er breed erkende certificeringen voor (ethical) hackers en penetratietesters. Het is jammer dat in het voorstel niet direct hierop wordt aangesloten.
   c. Goede beveiliging helaas geen garantie
      Als ik kijk welke grootschalige incidenten er in de afgelopen jaren in mijn omgeving hebben plaatsgevonden, dan zijn met name ook organisaties getroffen die hun beveiliging op orde hadden: certificering tegen of aantoonbaar voldoen aan NEN-7510, patch- en vulnerability management op orde, recente pentest zonder ernstige bevindingen. In deze gevallen ging het om zero-day exploits in producten van grote leveranciers (Log4j, Juniper/Pulse secure, Ivanti).
      Het feit dat de term zero-day geen enkele keer voorkomt in de Memorie van Toelichting lijkt een indicatie dat hierover onvoldoende is nagedacht.
   d. Het tegengestelde bereiken van wat beoogd wordt.
      De doelstelling van de wet is mede gericht op het waarborgen van de continuïteit van (de diensten van) de betrokken organisaties. In de teksten over het opleggen van boetes mis ik echter aandacht voor het effect van de hoogte van de boete op de continuïteit van de organisaties. De boetes die de AP in de zorg heeft opgelegd, hebben altijd gevolgen gehad voor de dienstverlening aan de patiënten. In het ergste geval wordt immers niet de entiteit gepakt maar de burger.

e. Afwijkend model ten aanzien van bestuurlijke verantwoordelijkheid
Het Nederlandse model voor bestuur en raad van commissarissen (toezicht) gaat doorgaans uit van een collegiaal model waarbij – naast basisvaardigheden – via individuele aandachtsgebieden tot een passend geheel wordt gekomen. Denk aan de combinatie van CEO, CIO, CFO, CISO, Manager HR, e.d.. In artikel 26 wordt een beeld geschetst dat alle leden moeten beschikken over diepgaande kennis van (de risico's) van informatiebeveiliging én de ontwikkelingen daarin. Als ik kijk naar mijn eigen opleidingen dan hebben die minimaal 1 jaar geduurd met daarna vele verdiepingen. Dat nog in een tijd dat ICT niet zo complex was. Nu volstaat dit enkel voor kennis op hoofdlijnen en zal ik mij niet wagen aan het werk van specialisten (zoals beheer firewall, SIEM, anti-virusoplossingen, e.d.). Het is m.i. niet reëel een dergelijk kennisniveau van het gehele bestuur te eisen. Voorts is een zo gedetailleerde kennis niet reëel: het gaat erom om de juiste vragen te kunnen stellen aan specialisten en de validiteit van de antwoorden te kunnen beoordelen. Er geldt immers nog altijd het gestelde onder letter c. hiervoor.

5. Diverse inconsistenties:
   a. Wel/niet de toevoeging 'van de NIS2-richtlijn' achter een verwijzing naar een artikel uit de richtlijn. Zie bijvoorbeeld onder definities: *als bedoeld in artikel 16* versus *genoemd in artikel 12 van de NIS2-richtlijn*
   b. Onderwerpen verwijzen via aanpassingen in andere wetten versus een onderwerp uitwerken in de Cyberbeveiligingswet. Ik ben gewend dat implementatie van aanpassingen op de c.q. benutting van de ruimte voor nationale afwijkingen in de AVG (GDPR) verlopen via de Uitvoeringswet AVG (UAVG), zo ook de verwerking van bijzondere gegevens (gezondheid, strafrecht, e.d.). Zeker is de zorg is het aantal wetten en regels dat erbij gehaald moet worden om over een beveiligings- of privacy issue een uitspraak te kunnen doen al bijna ondoenlijk. Als zaken die je in de UAVG verwacht, niet daar, maar op andere plaatsen staan, zoals hier in artikel 64a, dan wordt het helemaal niet meer te doen. Advies is om deze aanpassingen door te voeren via de UAVG.
   c. NEN-7510 versus ISO-27001: NEN-7510 wordt gezien als een voorbeeld van een sectorale norm, waar ISO-27001/2 wordt gezien als een eigen invulling van de organisatie. Los van de vraag of dit laatste klopt als hele sectoren (inclusief de grootste spelers zoals Google, Microsoft en Amazon) zich hieraan conformeren. De CISO's van de ziekenhuizen zijn van mening dat NEN-7510 zonder meer ingetrokken kan worden omdat ze geen toegevoegde zien ten opzichte van ISO-27001/2. Het lijkt eerder alsof andere partijen er belang bij hebben om voor eigen gewin deze NEN-norm te handhaven.
   [Deze weerstand is mede ingegeven door het feit dat de Autoriteit Persoonsgegevens een mogelijke (zorgspecifieke) maatregel uit NEN-7510 deel 2 tot hard norm heeft verheven, terwijl de ISO-27000 benadering is dat deze maatregelen op basis van risicoanalyse *kunnen* worden geselecteerd om invulling te geven uit de beoogde beveiligingsdoelstelling van NEN-7510 deel 1.]

6. Te vrijblijvende teksten in de Memorie van Toelichting
   Ik noem slechte twee voorbeelden:
   a. Meldproces: op pagina 25 van de MvT staat: Er *wordt naar gestreefd* deze dubbele meldplicht technisch zo in te richten dat het verspreiden van de benodigde informatie maar één handeling voor de entiteit vergt. Organisaties moeten in voorkomend geval ook nog aan andere instanties melden (in de zorg bijvoorbeeld aan IGJ en AP). Dit levert al een grote belasting op. Het is niet aanvaardbaar om in het kader van dit wetsvoorstel meer dan één melding te moeten doen.
   b. Beveiligingsscans: op pagina 33 van de MvT wordt onderkend dat deze een grote impact kunnen hebben op de (continuïteit van de) organisatie waartegen deze worden ingezet. De

praktijk is dan ook dat organisaties die ethical hackers en pentesters inhuren hierover altijd duidelijke afspraken maken; vanuit de kant van die hackers en pentesters ook om de aansprakelijkheid te beperken. De tekst rept echter van “indien nodig in samenwerking met de betrokken entiteit” en het in de rede dat mogelijke meer risicovolle beveiligingsscans die bijvoorbeeld de continuïteit van de dienstverlening kunnen raken pas na consultatie van de betreffende entiteit en indien nodig in samenwerking met de entiteit door de toezichthoudende instantie worden ingezet. Gegeven de risico’s voor de continuïteit zou het een verplichting moeten zijn dat risicovolle beveiligingsscans alleen na overleg en in samenwerking met de entiteit worden uitgevoerd.