Nederlandse Vereniging van Ziekenhuizen

Internetconsultatie Cyberbeveiligingswet

Datum

20 juni 2024

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 wetsvoorstel
Ingediend op 13 mei 2024, via de website Overheid.nl | Consultatie Cyberbeveiligingswet en de Wet Weerbaarheid Kritieke entiteiten.
Link naar consultatie Cyberbeveiligingswet:
www.internetconsultatie.nl/cyberbeveiligingswet
Link naar consultatie Wet weerbaarheid kritieke entiteiten:
www.internetconsultatie.nl/wetweerbaarheidkritiekeentiteiten

Inleiding

De Nederlandse Vereniging van Ziekenhuizen (NVZ) maakt graag van de mogelijkheid gebruik om te reageren op het concept van de Cyberbeveiligingswet en de CER.
Wij waarderen de mogelijkheid onze input te kunnen geven. De NVZ draagt graag bij aan een effectieve en evenwichtige wetgeving op het gebied van cyberbeveiliging voor de aangesloten instellingen.
In het algemeen ondersteunen wij het doel van de wet om de digitale weerbaarheid van kritieke sectoren te versterken en de bescherming van persoonsgegevens te waarborgen. Echter, wij hebben enkele specifieke aandachtspunten en aanbevelingen op de wetgeving zoals die nu voor ons ligt, of die invulling vragen in de AMvB.

Meldplicht

De NVZ pleit als eerste voor een evenwichtige benadering van meldplicht bij incidenten, waarbij duidelijke minimale grenswaarden zijn aangegeven. Zodat de administratieve last tot een minimum beperkt blijft voor onze leden en voor Z-CERT.
Om meer consistentie in meldingsvereisten te waarborgen, kunnen de volgende stappen worden overwogen. Geef duidelijk aan wat wordt verstaan onder significant. Zorg ervoor

dat dezelfde termen en definities, en periodes van meldingen worden gebruikt in alle relevante wetgeving en richtlijnen van zowel de Cyberwetgeving als de CER.
Dit minimaliseert verwarring en bevordert uniformiteit.

De naam van de wet geeft aanleiding om te denken dat de wet gericht is op cyberdreigingen, maar de meldplicht blijkt zoveel breder, gericht op de bereikbaarheid en beschikbaarheid van zorg. Dat maakt dat alle incidenten, die mogelijk ook zo weer zijn opgelost, en geen invloed hebben op de IT-infrastructuur van anderen, ook moeten worden gemeld.
Advies: Graag een duidelijke grenswaarden aangeven over wat wel en niet gemeld moet worden in relatie tot deze cyberbeveiligingswet in de AMvB met als belangrijkste doel het cyberveiliger maken van de vitale sector.

Eenmalig melden
Het kan niet zo zijn dat van instellingen wordt gevraagd om op meerdere plekken informatie over incidenten te moeten aanleveren. Het streven is er al om voor Z-CERT en IGJ samen via het op te richten portaal in te richten. De NVZ zou graag zien, dat als het een datalek zou betreffen, deze melding ook voor de AP inzichtelijk zou zijn in het portaal, of in ieder geval conform eenzelfde “informatiestandaard” wordt aangeleverd bij alle belanghebbende toezichthoudende partijen met hoogstens wat specifieke aanvullingen als het om bijzondere persoonsgegevens gaat.

Bewustwording en opleiding.
Investeringen in bewustwordingscampagnes en opleiding van medewerkers zijn cruciaal om cyberdreigingen te verminderen. VWS zou dit financieel moeten stimuleren en er ook voor moeten waken dat “zorggeld” niet naar commerciële partijen wegvloeit zonder relevante kennis van de zorg. Deze zelfde partijen zijn ook minder effectief in het verzorgen van de trainingen als trainingen die ontwikkeld kunnen worden, of in ieder geval de kaders en toetsing daarvoor worden bepaald, in samenwerking met Z-CERT en ECP (Informatieveiligheid in de Zorg) die de zorgsector echt goed kennen. Daarbij is het van belang dat er niet alleen aandacht is voor de trainingen van bestuurders, maar ook van het management, informatiebeveiligers en crisis coördinatoren. Het is van het grootste belang dat deze betrokkenen in basis dezelfde informatie en communicatielijn in de organisatie uitdragen. Dat gaat over het belang van een goed functionerend ISMS (NEN7510) en daarmee inzicht hebben in de risico’s en bijbehorende beheersmaatregelen. De gehele organisatie moet zich bewust zijn van de te nemen passende en evenredig technische, operationele en organisatorische maatregelen. Dit om de risico’s voor de beveiliging van de netwerken- en informatiesystemen te beheersen.

Handhaving
Sancties worden gegeven als het leed al is geschied. Is het niet veel belangrijker om in de wetgeving het belang van preventie te benadrukken door essentiële organisaties te verplichten om een minimaal percentage van de jaaromzet in te zetten voor cyberbeveiliging? Daarmee kan veel ellende mogelijk worden voorkomen, want echt voorkomen zal nooit lukken.
Indien de IGJ een boete moet opleggen dan graag “passende” sancties. In plaats van een bedrag van maximaal 10 miljoen euro op te leggen als boete voor deze sector, zou een meer gedifferentieerde aanpak kunnen worden overwogen in de AMvB.
De NVZ kiest liever voor een risico gebaseerde benadering daarin, waarbij het opleggen van te nemen beheersmaatregelen binnen een bepaalde termijn een veel effectievere sanctie is omdat dit de veiligheid in de keten daadwerkelijk verbeterd. Sancties kunnen worden afgestemd op de ernst van de inbreuk en de impact op de patiëntenzorg door de IGJ. Zorginstellingen met een hoger risico, zouden strengere maatregelen moeten nemen met mogelijk “verplichte” investeringen om incidenten in de toekomst te voorkomen.
Een verplichte investering in beveiligingsmaatregelen op basis van een uitgevoerde beveiligingsscan kan en zal op termijn effectiever zijn dan een hoog bedrag als boete opleggen. Het doel van de wet is om deze vitale sector veiliger te maken en te beschermen tegen cyberaanvallen. Dit zou de zorginstellingen dan dwingen om aantoonbaar de gerichte verbeteringen door te voeren.
De delegatiegrondslagen bieden VWS de mogelijkheid om met sectorspecifieke regels te komen zoals voor de drempelwaarden van de incidenten maar ook voor de te bepalen sancties, maar daar gebruik van als VWS.
Het is belangrijk dat de wetgeving evenwichtig is en rekening houdt met de specifieke uitdagingen waar de zorgsector voor staat, en dat is ook dat de kosten – baten in balans moeten zijn om patiëntenzorg te kunnen blijven bieden. Voor kleinere instellingen in de zorg is er tevens het verzoek om op basis van het beginsel van zorgvuldigheid oog te hebben voor de proportionaliteit in de wet, zowel op het gebied van de sancties als de audit en controlelast.

Artikel 23 lijkt minder concreet dan artikel 21 uit de Europese richtlijn. De NVZ pleit voor duidelijkere richtlijnen in de AMvB om de zorgplicht praktisch toepasbaar te maken voor zorginstellingen. Blijf bij de lijn die nu al wordt gevolgd, aantoonbaar voldoen aan de NEN 7510. Een risico gebaseerde aanpak is de basis van de NEN 7510, maar zou dat ook moeten zijn voor de Cyberbeveiligingswet en de CER. Art. 23 lid 1 refereert naar de risico's maar dit is erg algemeen opgesteld. NIS2 geeft veel handvatten over deze risico's en de strekking van de invulling van de risico gebaseerde aanpak. In de huidige wet, zoals die nu voorligt, wordt deze risico gebaseerde aanpak onvoldoende en onvolledig weergegeven. Het advies is om tevens een duidelijke relatie te leggen met de risico gestuurde aanpak van de NEN 7510.

Artikel 26 (governance) spreekt over bestuur en elk lid van het bestuur. De Europese richtlijn noemt echter bestuursorganen wat een bredere interpretatie (RvB, MSB, MT en RvT) mogelijk maakt. Alle leden van de RvB moeten het hetzelfde kennisniveau hebben ten aanzien het managen van een crisissituatie bij een cyberincident en van het risicomanagement op het gebied van informatiebeveiliging. De bestuurder die informatiebeveiliging in zijn of haar portefeuille heeft zal moeten kunnen voldoen aan de eisen ten aanzien van kennis en vaardigheden zoals genoemd in artikel 26, lid 2 a t/m c, vanaf het moment dat hij/zij deze portefeuille beheert, en niet pas vanaf 2 jaar na aanstelling. Hij/zij zal in de besluitvorming binnen de RvB, waarbij ook de directie van het MSB aanwezig is, moeten onderbouwen waarom bepaalde beheersmaatregelen moeten worden genomen of welke rest-risico's door de RvB kunnen worden geaccepteerd. Een realistisch vereist kennisniveau bevordert het gevoel van eigenaarschap, niet alleen bij de RvB, maar ook bij het MSB en de RvT en de betrokken directeuren en managers.

De NVZ heeft de voorkeur om zo min mogelijk uitzonderingen aan te wijzen binnen haar leden als belangrijke entiteit, zodat ook zo min mogelijk op (één van) hen, door de openbaarheid van die aanwijzing, alle aandacht wordt gevestigd. Dat kan onaanvaardbare risico's met zich mee brengen voor de totale sector.

Tot slot is het advies om in de AMvB duidelijk te zijn over wie in de lead is bij incidenten waarbij naast de zorg, andere vitale entiteiten betrokken zijn die onder een ander ministerie vallen, denk aan energie, water of infrastructuur. Wat is dan de rol van de Veiligheidsregio's, is de NCSC dan in de lead?

Samengevat zijn dit de belangrijke punten:

- Een evenwichtige benadering van de meldplicht bij incidenten, met duidelijke minimale drempelwaarden en voorbeelden.
- Consistentie in meldingsvereisten bij de Cyberbeveiligingswet en de CER.
- Het vermijden van meerdere meldingspunten voor incidenten (Z-CERT, IGJ en AP).
- Het mogelijk maken van een opleiding voor RvB, en direct betrokkenen, om cyberdreigingen te verminderen met ECP en Z-CERT, de partijen in de zorg.
- Het belang onderschrijven van het hebben van een realistisch vereist kennisniveau voor alle leden van de RvB.
- Het benadrukken van het belang van preventie in de wetgeving.
- Het overwegen van een meer gedifferentieerde aanpak voor sancties (geen max 10 miljoen voor de zorg!).
- Het gebruik van een risico gebaseerde aanpak voor de Cyberbeveiligingswet en de CER conform de NEN 7510.
- Het hebben van duidelijkere richtlijnen in de AMvB om de zorgplicht praktisch toepasbaar te maken voor zorginstellingen.

Nederlandse
Vereniging van
Ziekenhuizen

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 deze belangrijke wet op het gebied van informatiebeveiliging.

Veronique Esman, directeur
NVZ - Nederlandse Vereniging van Ziekenhuizen