Geachte heer/mevrouw,

Namens de Nederlandse Federatie van Universitaire Medische Centra (NFU) geven wij een reactie op het concept van het Cyberbeveiligingsbesluit (hierna: Cbb) en de daarbij behorende nota van toelichting. Als NFU zullen we daarbij algemene en specifieke aandachtspunten naar voren brengen.

Algemeen:

In deze publieke consultatie is naast het Cbb een gezamenlijke ministeriële regeling vanuit de ministeries van EZ, KGG, LVVN en IenW ter consultatie aangeboden. De zorgsector heeft het vermoeden dat hiermee de ministeriële regeling vanuit VWS niet publiek ter consultatie zal worden aangeboden. Door als VWS niet mee te doen met de gezamenlijke regeling bestaat de kans op ongelijkheid ten aanzien van het publiek consulteren van ministeriele regelingen onder de Cyberbeveiligingswet (hierna: Cbw). We roepen de minister van VWS op om alsnog de toekomstige sectorale ministeriele regeling onder de Cbb publiekelijk te consulteren. Verder verzoeken we het coördinerende ministerie J&V om zorg te dragen voor gelijke behandeling van de sectoren vallende onder de Cbw t.a.v. het wel/niet publiek consulteren van lagere regelgevingen.

Omdat een concept ministeriele regeling voor de zorgsector nog ontbreekt is het onduidelijk wat de parameters zijn om onder de Cbw/Cbb te voldoen aan de meldplicht. Na afstemming met de diverse brancheorganisaties binnen zorg willen we VWS verzoeken om zoveel mogelijk in te zetten op aansluiting bij bestaande incidentprocessen en daar gehanteerde en bekende parameters. Een ministeriele regeling die mogelijk niet aansluit op de praktijksituatie in de zorg zal het nut en effectiviteit van de wet verlagen en werkt voornamelijk lastenverzwarend.

Lastenverzwaringen zijn binnen zorgsector niet onbekend en we zien eveneens een toenemende regeldruk voortkomen uit de Cbw/Cbb. Zo wordt onder de Cbb gevraagd om extra bewijslasten bij de registratie en opvolging van meldingen en signaleringen. Onzeker is hoe breed deze extra bewijslasten zijn en wat de overheid specifiek vraagt aan bewijs van een entiteit.

Tot slot zijn er in het Cbb specifieke benamingen van beleidsdocumenten opgenomen. Deze specifieke benamingen sluiten niet aan bij best practices binnen de zorg en bestaande normen zoals de NEN7510. Betekent dit dat nieuw/bestaand beleid moet worden aangepast aan de gehanteerde benamingen uit de Cbb?

Specifiek:

In de nota van toelichting Cbb wordt op pagina 3 gesproken over een eenmalige kostenpost betreffende de aanschaf van soft- en hardware. De NFU vraagt zich af sinds wanneer soft- en hardware als eenmalige kostenposten worden gezien. Software is in de meeste gevallen licentie gedreven en hardware moet periodiek worden vervangen / onderhouden. Dat zijn geen eenmalige kosten maar periodieke kosten die blijven terugkomen. Daarnaast zien we op pagina 3 onder tabel 1 in de nota van toelichting een aantal uren (2.177) geprojecteerd ten aanzien van de implementatie van zorgplicht onder artikel 21 Cbw. Onduidelijk is hoe dit aantal uren tot stand gekomen en waar deze specifiek uit bestaan.

Op pagina 4 en 5 van de nota van toelichting wordt de paragraaf ‘panel MKB’ besproken. De NFU vraagt zich af waarom deze paragraaf is opgenomen in de nota van toelichting op de Cbb. Onduidelijk is wat de bedoeling is van deze opname en welke conclusies hieruit kunnen worden getrokken. De paragraaf komt over als een preferente consultatiereactie vanuit het MKB met een weergave/verslag van een panelbijeenkomst. Welke conclusies kunnen er worden verbonden aan de in de nota opgenomen opvattingen onder de paragraaf ‘panel MKB’?

In de nota van toelichting pagina 8 op de Cbb wordt in de laatste alinea van artikel 6 gesproken over PDCA systematiek/ISMS. Voorbeelden worden gegeven zoals de ISO 27000-reeks of het Cyber Security Management System (CSMS) op basis van EIC 62443. Waarom is in de toelichting niet expliciet de zorg specifieke NEN7510 als voorbeeld voor een ISMS/PDCA opgenomen. Met name omdat op de landingspagina van de consultatie wel gesproken wordt over het normenkader NEN7510 maar dit nergens in de geconsulteerde stukken terugkomt.

Op pagina 9 van de nota van toelichting Cbb wordt het volgende beschreven:

> *'(…) Risico's met betrekking tot de netwerk- en informatiesystemen kunnen daarnaast niet los gezien worden van alle andere risico's waar de entiteit aan bloot gesteld wordt. Daarom behoort het beheersen van de risico's met betrekking tot de netwerk- en informatiesystemen een onderdeel van het bredere risicobeheerproces van de entiteit te zijn.'*

Voorgaande werkwijze t.a.v. risicomanagement wordt door de NFU onderschreven. Het is echter niet gepast om via de nota van toelichting op de Cbb de reikwijdte van de NIS2/Cbw te vergroten tot het bredere risicobeheerproces van een entiteit. Hiermee ontstaat scope creep t.o.v. de oorspronkelijke Europese tekst en de Nederlandse omzetting.

Op pagina 14 in de nota van toelichting Cbb onder artikel 17 (attenderingen, adviezen en informatie) wordt geschreven over het schriftelijk vastleggen van beoordelingen t.a.v. ontvangen kwetsbaarheden of cyberdreigingen. Dagelijks ontvangen de UMC's grote hoeveelheden meldingen, adviezen over kwetsbaarheden en updates/patches vanuit bijvoorbeeld softwareleveranciers. Kan worden verhelderd of het aantoonbaar uitvoeren van reguliere patchrondes, (bijv. patch tuesday) waarbij leveranciers vele kwetsbaarheden oplossen, voldoende zijn als dergelijk bewijslast. Of dient ieder bericht/melding apart voorzien te worden van een beoordeling met bijbehorende schriftelijk bewijslast? Afhankelijk van de duiding kan voorgaande verplichting namelijk leiden tot extra bureaucratische handelingen t.a.v. het vastleggen van schriftelijke bewijslast.

Op pagina 15 in de nota van toelichting Cbb onder artikel 21 eerste lid (eisen aan training) worden specifieke (technische) onderwerpen voor een training genoemd. Volgens de NFU zou deze invulling niet zo specifiek en technisch van aard moeten zijn. De specifieke invulling van de training zou moeten afhangen van de organisatie en diens inrichting en security-bemensing. De focus van een bestuurderstraining zou daarbij voornamelijk gericht moeten zijn op de omgang met risico's en een aantoonbare betrokkenheid bij de afweging van risico's.

Tot slot wordt op pagina 16 nota van toelichting Cbb onder artikel 24, tweede lid het volgende t.a.v. evaluaties geschreven:

> *(…) bedoelde criteria ten minste elke vier jaar moeten worden geëvalueerd door de betrokken vakminister. Met het evalueren kan worden bewerkstelligd dat de criteria actueel blijven en aansluiten op de gevaren en dreigingen die voor een sector relevant zijn. Denk daarbij bijvoorbeeld aan zeer snelle technologische ontwikkelingen.*

Het snel en tijdig kunnen evalueren van criteria wordt door de NFU onderschreven. Als NFU verzoeken we om, na inwerkingtreding van de volledige Cbw, de eerste evaluatie na bijvoorbeeld 1 jaar te laten plaatsvinden. Dit verzoek doen we zodat tijdig kan worden bepaald of de criteria voor significante incidenten passend zijn en werkbaar zijn voor de sector.

Namens de NFU / UMC's van Nederland,

mr. Sander Vols

Chief Information Security Officer (CISO), Radboudumc