Datum : Vrijdag 28 juni 2024

Onderwerp : Reactie VZVZ op de concept Cyberbeveiligingswet

VZVZ, entiteit in de zorgsector

VZVZ is een vereniging van koepelorganisaties in de zorg en heeft als doel om elektronische gegevensuitwisseling tot stand te brengen tussen zorgaanbieders onderling en met patiënten. VZVZ heeft als kerndoelstelling het ten behoeve van de leden realiseren van elektronische uitwisseling van medische gegevens in de zorg. Onze ambitie is te bewerkstelligen dat de juiste informatie, veilig en op het juiste moment toegankelijk is voor de juiste mensen.

VZVZ doet dat op verschillende manieren: door partijen in het veld bijeen te brengen, zodat wat zij aan (technische) functionaliteiten tot stand willen brengen, daadwerkelijk gerealiseerd wordt (netwerkcoördinerend). Door het bieden van expertise met betrekking tot elektronische gegevensuitwisseling als kennis- en expertisecentrum en door functionaliteiten te realiseren, te beheren en door te ontwikkelen, die voldoen aan alle eisen van interoperabiliteit. VZVZ is daarbij beheerder van afsprakenstelsels en generieke voorzieningen.
VZVZ heeft geen commercieel oogmerk en is geen ICT-leverancier. Onze missie is om een bijdrage te leveren aan het duurzaam informatiestelsel van de zorg, zodat gegevensuitwisseling op een doelmatige en kosteneffectieve manier kan plaatsvinden.

Wij signaleren een aantal conflicten in de NIS2-richtlijn en in de Nederlandse implementatiewet daarvan, de Cyberbeveiligingswet (Cbw).

Indeling qua sector, toezicht en ondersteuning
Zorgaanbieders die voldoen aan de criteria uit de Cbw zijn verplicht om zich via de toezichthouder Inspectie Gezondheidszorg en Jeugd (IGJ) en Z-CERT te laten controleren en ondersteunen. VZVZ lijkt onder de Cbw niet als een organisatie in de gezondheidszorgsector te worden aangemerkt, maar valt mogelijk wel onder één van de andere sectoren die raken aan de digitale dienstverlening. Dat zou met zich meebrengen dat niet de IGJ, maar de Rijksinspectie Digitale Infrastructuur (RDI) mogelijk de toezichthouder van VZVZ zal worden en dat VZVZ moet aansluiten bij zowel het NCSC als CERT. VZVZ is echter momenteel al meerdere jaren deelnemer van Z-CERT.

Niet commercieel
In tegenstelling tot andere digitale dienstverleners is VZVZ geen commerciële partij. VZVZ biedt de bestaande centrale infrastructuur (het Landelijk Schakelpunt (LSP)) en diensten voor elektronische gegevensuitwisseling en ontwikkelt die als een oplossing voor zorgaanbieders die veilig en gestandaardiseerd hiermee willen samenwerken, ook met de patiënten. Het uitgangspunt hierbij is dat zorgaanbieders op basis van vrijwilligheid beslissen of zij gebruik maken van de aangeboden infrastructuur en diensten. De infrastructuur is neutraal, non-concurrentieel en gebaseerd op open standaarden.

VZVZ levert uitsluitend op verzoek van de koepelorganisaties/zorgaanbieders diensten en expertise ten bate van de zorgsector voor complexe problemen op het gebied van

gegevensuitwisseling die niet door de markt op te lossen zijn. Of diensten waarvoor er door commerciële partijen geen sluitende businesscase te maken is.

VZVZ is dus een centrale partij in de zorgsector, opgericht door en uitsluitend werkend voor zorgaanbieders en patiënten. Het ligt daarom het meest voor de hand om VZVZ aan te merken als een 'entiteit in de gezondheidszorgsector'. Het is logisch om onze meldplicht bij de toezichthouder zorg te laten vallen, omdat zij juist de expertise hebben en verbinding leggen ten behoeve van de zorg. We willen voorkomen dat er informatie achter blijft die voor onze leden, de zorgaanbieders, cruciaal is in geval van een ernstige cybercalamiteit. Indien VZVZ wordt aangemerkt als een entiteit in één van de andere sectoren die betrekking hebben op digitale dienstverlening, dan treedt een heel ander mechanisme in werking, waarvan wij denken dat dat veel risico's met zich meebrengt. In dit kader is het belangrijk dat VZVZ aangemerkt of aangewezen wordt als een 'entiteit in de sector gezondheidszorg'. VZVZ heeft als entiteit een dusdanig sterke connectie met de sector gezondheidszorg, dat wij een aanwijzing legitiem achten.

Wij signaleren de volgende mogelijke conflicten en risico's voor de informatie-uitwisseling, de verschillende toezichthouders en CERT-dienstverleners.

1. Dubbele meldplicht

VZVZ levert verschillende diensten voor de uitwisseling van medische gegevens tussen zorgaanbieders en tussen zorginstellingen en burgers. VZVZ kan daarmee goed bepalen wat de impact is voor de zorgaanbieders bij een incident. VZVZ staat als ketenregisseur bij de gegevensuitwisseling ook voortdurend in contact met de beheerpartijen die de zorginformatiesystemen beheren voor zorgaanbieders. Het is daarom logisch dat VZVZ zich meldt bij de beoogde toezichthouder voor de zorg: de IGJ. Daarnaast is VZVZ een belangrijke organisatie voor de beschikbaarheid en uitwisseling van medische gegevens van zorgaanbieders die aangesloten zijn bij Z-CERT.

Echter, het wordt verwarrend (en risicovol!) als een incident zowel binnen de sector gezondheidszorg als binnen één van de andere sectoren valt. Dit kan zelfs leiden tot een dubbele meldplicht bij instanties. Wij geven hiervan twee voorbeelden:

a. Via VZVZ worden ook medische gegevens uitgewisseld door partijen die onder het ministerie van Volksgezondheid Welzijn en Sport vallen. Dit betreft bijvoorbeeld het RIVM met het rijksvaccinatieprogramma. Zij gebruiken het LSP voor de gegevensuitwisseling tussen JGZ-instellingen. Het RIVM is een agentschap en moet melden en rapporteren bij het ministerie van Binnenlandse Zaken en Klimaat, JGZ is een zorgaanbieder of overheid (GGD) en moet bij een incident melden bij de IGJ.

b. Wanneer VZVZ voor bepaalde diensten, zoals Mitz en ZORG-ID, valt onder een sector die raakt aan de digitale dienstverlening, dan ontstaat daarmee mogelijk een meld- en zorgplicht bij de RDI. Het risico bestaat dan dat VZVZ opeens een dubbele meldplicht heeft bij incidenten, bijvoorbeeld indien het ook een incident in de gezondheidszorgsector betreft. Het risico is tevens, dat een incident bij de verkeerde toezichthouder wordt gemeld.

2. **Verantwoordelijkheid en jurisdictie**
   Het is van belang om nu vast te stellen wie er straks verantwoordelijk is voor de melding en het beheer van een incident.
   Indien er geen duidelijke keuze wordt gemaakt, dan vrezen wij dat VZVZ en zorgaanbieders per keer gaan bepalen welke aspecten van een incident onder de verantwoordelijkheid van de RDI vallen en welke aspecten onder de verantwoordelijkheid van de IGJ vallen.

3. **Europese uitwisseling**
   De keuze is ook van groot belang in het kader van gegevensuitwisseling op Europees niveau op basis van de EHDS. Voor het uitwisselen van medische gegevens tussen Europese lidstaten sluit het CIBG als Nationaal Koppelpunt (NCPeH-NL) aan op het LSP. De situatie die daarmee ontstaat is dat de zorgaanbieders onder de Cbw vallen (afhankelijk van grootte en omzet) en dat het NCPeH-NL onder de verantwoordelijkheid van het CIBG valt. Ook hier ontstaat dus een tegenstrijdigheid.

4. **Informatiedeling, samenwerking, en coördinatie**
   Het is van belang dat de toezichthouders borgen dat het melden van incidenten die betrekking hebben op de informatie-uitwisseling in de zorg, eenduidig geregeld wordt. Daarbij is het in ons belang, dat wij zicht houden op incidenten en/of informatie daarover van leveranciers die ook digitale diensten verlenen voor de zorg en aangesloten zijn op onze diensten en uitwisselingsplatformen.
   Overigens hebben deze leveranciers van zorginformatiesystemen (ook) te maken met dit dilemma: zij zijn een digitale dienstverlener die hun diensten verlenen voor de zorg. Zij hebben plichten met een andere toezichthouder dan voor de zorg. Voor enkele dienstverleners (bijvoorbeeld VECOZO) geldt dat zij ook samenwerken met Z-CERT. Het zou logischer zijn om ICT-dienstverleners te kunnen verbinden aan een sector.

5. **Verschillende focus en expertise**
   RDI en IGJ hebben verschillende expertisegebieden en focuspunten. Dit kan leiden tot verschillende benaderingen bij het beoordelen van en reageren op incidenten. Om deze conflicten aan te pakken, is het belangrijk dat er duidelijke richtlijnen en samenwerkingsmechanismen zijn tussen de betrokken partijen. Het kan ook nodig zijn om de meldingsprocedures en de verantwoordelijkheden te verduidelijken, zowel voor ICT-dienstverleners als voor zorgaanbieders, om zo een soepele samenwerking te bevorderen en de cybersecurity in de zorgsector te verbeteren.

6. **Verzamelwet gegevensverwerking VWS II.a**
Met het wetsvoorstel Verzamelwet gegevensverwerking VWS II.a wordt de toezichtmogelijkheid van de IGJ in het kader van de Wabvpz uitgebreid.

VZVZ is op grond van artikel 8 lid 2 Wabvpz bevoegd tot het verwerken van het BSN van cliënten en op basis van het Besluit elektronische gegevensverwerking door zorgaanbieders verplicht om te voldoen aan de NEN7510, NEN7512 en NEN7513. Dat betekent dat VZVZ in het kader van de Wabvpz onder toezicht van de IGJ valt. Daar waar we onder de Cyberbeveiligingswet mogelijk niet onder toezicht van de IGJ staan. Deze verschillende regimes dragen niet bij aan een eenduidig toezicht.

Samenvattend

Wij verzoeken om VZVZ, in het kader van de Cbw aan te merken of aan te wijzen als een ‘entiteit in de sector gezondheidszorg’. VZVZ heeft als entiteit een dusdanig sterke connectie met de sector gezondheidszorg, dat wij een aanwijzing legitiem achten. Daarmee wordt de problematiek voorkomen zoals die hierboven omschreven is.

Indien dat geen optie is, dan verzoeken wij om te onderzoeken hoe de overlap tussen de toezichthoudende instanties vermeden kan worden en vragen wij om een goede borging van de samenwerking/informatie-uitwisseling tussen de toezichthoudende instanties.
Bevorder tevens dat RDI en IGJ zoveel mogelijk dezelfde benadering hanteren bij het beoordelen van en reageren op incidenten.

Opmerkingen per artikel

- **Artikel 26**: NIS2 vereist dat bestuursleden moeten beschikken over (technische) kennis en vaardigheden op het gebied van cyberbeveiliging. Bestuurders moeten ook een training certificaat kunnen overhandigen. Moet dit ook gelden voor de RvB leden? Het is begrijpelijk dat het bestuur niet zomaar blind securityzaken moet aftekenen of risico's accepteren zonder een goed begrip te hebben van de implicaties. Echter, het is logischer om dit bij enkele bestuursleden deze vereisten toe te wijzen die de verantwoordelijkheid dragen voor cyberbeveiliging, met de voorwaarde dat zij samenwerken met deskundige medewerkers die aan hen rapporteren.

- **Artikel 31** Het vrijgeven van dit soort informatie, ook onder de wetgeving openbaarheid bestuur, kan ook risico's voor andere entiteiten met zich meebrengen. Het voortgangs-/eindverslag moet straks gedeeld worden met twee instanties (CSIRT en bevoegde autoriteit). Dit bevat een schat aan gevoelige informatie. Hierdoor worden deze twee overheidsinstanties een centrale bron van zeer gevoelige informatie die aantrekkelijk kan zijn voor een kwaadwillende. Dit brengt risico's met zich mee. Hoe wordt zorggedragen dat juiste beveiligingsmaatregelen worden getroffen (b.v. versleuteling van gegevens in transit en rust, strikte toegangscontrole, detectie en monitoring)?

- **Artikel 39** CSIRT kan besluiten in overleg om het publiek te informeren over incident. Wordt daarbij een afweging gemaakt wat de impact is van deze openbaarmaking door de overheidsinstantie? Specifiek voor partijen die indirect geraakt kunnen worden, doordat informatie nu publieke beschikbaar is. In onze digitale samenleving zijn veel zaken van elkaar afhankelijk die zeker niet altijd volledig inzichtelijk zijn en ook niet voor partijen die niet onder de NIS2 vallen. Juist door het samenbrengen van deze kwetsbaarheden en afhankelijkheden worden de CSIRT's ook een bron voor andere partijen. Hoe wordt dit gezien en wat is de afweging die hier gemaakt wordt?