Position Paper Cyberveiligheid en informatiebeveiliging

Samen vormen de gemeentelijke gezondheidsdiensten (GGD'en) en Geneeskundige Hulpverleningsorganisaties in de Regio (GHOR'en) de basis voor de publieke gezondheidszorg in Nederland. Medewerkers van GGD'en en GHOR's zetten zich dagelijks in voor onder meer de bestrijding van infectieziekten, het verlenen van geneeskundige zorg bij rampen en crises, de ondersteuning van jonge ouders en jeugdigen, en het bevorderen van een veilige en gezonde leefomgeving. Data spelen hierin een onmisbare rol. Zonder data is er géén publieke gezondheidszorg. Tegelijkertijd zijn juist deze data doelwit van hackers en kwaadwillende derden. Dit stelt hoge eisen aan organisaties en aan de politiek. In deze position paper zet GGD GHOR Nederland uiteen wat dit vraagt.

De vaste Kamercommissie Digitale Zaken stelt in haar uitnodiging voor het rondetafelgesprek '*cyberveiligheid en informatiebeveiliging*' (d.d. 23 april jl.) de centrale vraag hoe de informatiebeveiliging van publieke en private organisaties kan worden verbeterd. Voorafgaand aan dit gesprek wil GGD GHOR Nederland bij de Kamercommissie het belang benadrukken van gezamenlijke en domeinoverstijgende investeringen in randvoorwaarden. Deze investeringen zijn nodig om te komen tot een cultuur waarin informatiebeveiliging en gegevensbescherming structureel zijn verankerd in het handelen van zowel veldpartijen als overheid.

Cultuur als basis

In reactie op de vragen van leden van de vaste Kamercommissie met betrekking tot 'preventie' en het voorkomen van incidenten, benadrukken wij dat cultuur daarbij wat ons betreft de basis vormt. Het is essentieel dat niet alleen binnen organisaties, maar ook binnen samenwerkingsverbanden en ketens, een cultuur ontstaat waarin informatiebeveiliging en gegevensbescherming *by design* en *by default* zijn geborgd en geprioriteerd. Binnen zo'n cultuur worden deze onderwerpen niet gezien als een last, maar als randvoorwaardelijk. Dit maakt het mogelijk om kansen en kwetsbaarheden op een veilige manier te signaleren, bespreekbaar te maken en op te volgen.
Dit vraagt om een doorlopende en domeinoverstijgende benadering, waarin samenwerking tussen partijen, meer dan nu, centraal staat om de benodigde randvoorwaarden te realiseren. Zonder uitputtend te willen zijn, ziet GGD GHOR Nederland hierbij de volgende kansen:

1. Maak het naleven van verplichtingen makkelijk(er) en duidelijk(er).
2. Investeer in kennis, innovatie en samenwerking.
3. Houd rekening met uitvoeringskosten, ook bij bezuinigingen

Ad 1. Maak naleven verplichtingen makkelijk(er) en duidelijk(er)

In de afgelopen jaren zijn verschillende wettelijke kaders tot stand gekomen en in werking getreden. Daarbij gaat het onder meer om de AVG en de AI Act, maar ook om de EHDS, NIS2, de bijbehorende Cyberbeveiligingswet en andere (lidstatelijke) verplichtingen en normenkaders. Hoewel niet al deze kaders direct zien op informatiebeveiliging en gegevensbescherming, vloeien hieruit vaak wél verplichtingen voor organisaties voort.
Het voldoen aan al deze verplichtingen brengt aanzienlijke uitvoerlasten met zich mee. Vaak zijn meerdere specialistische functies nodig, terwijl deze expertise schaars is op de arbeidsmarkt. Regelmatig worden daarom externe consultants ingeschakeld om complexe en diverse wettelijke kaders te vertalen naar de praktijk. Het risico is dat zowel medewerkers als bestuurders hierdoor het overzicht verliezen en afhaken, terwijl juist iedereen betrokken en aangehaakt moet zijn om informatie en gegevens effectief te beveiligen. Tegelijkertijd leidt dit tot hoge kosten. Dit bemoeilijkt het ontstaan van de gewenste cultuur én de naleving van regels op alle organisatieniveaus, mede in relatie tot passende financiering (zie ad 3).

Daarnaast is het van belang dat bestaande normenkaders daadwerkelijk het beoogde effect hebben binnen de gehele keten. Voor organisaties moet duidelijk zijn wat er van hen verwacht wordt, en er moet vertrouwen zijn dat alle partijen aan dezelfde normen voldoen. Eenheid van taal en handelen is daarbij cruciaal.

Brancheafspraken kunnen bijdragen aan een stimulans om informatiebeveiliging en gegevensbescherming aantoonbaar en uniform op orde te brengen.

Ad 2. Investeer in kennis, innovatie en samenwerking
De vraag welke maatregelen nodig zijn om persoonsgegevens en bedrijfsgevoelige informatie adequaat te beschermen, is niet eenduidig te beantwoorden. Wat vandaag toereikend is, kan morgen achterhaald zijn. De snelle technologische ontwikkelingen versterken dit beeld: zij bieden kansen, maar brengen ook nieuwe dreigingen met zich mee. Voor individuele organisaties is het een grote uitdaging om deze dreigingen zelfstandig het hoofd te bieden. Daarom is het van belang om blijvend te investeren in kennis, innovatie en samenwerking, zowel binnen domeinen als domeinoverstijgend. Alleen door gezamenlijk op te trekken kunnen partijen data veilig houden.

Ad 3. Houd rekening met uitvoeringskosten, ook bij bezuinigingen
Het is een open deur, maar wel de realiteit: informatiebeveiliging en gegevensbescherming kosten geld. Organisaties kunnen middelen slechts één keer uitgeven. Het is daarom belangrijk dat investeringen worden gedaan in maatregelen die daadwerkelijk effect sorteren, mede gelet op het grote aantal verplichtingen die op organisaties afkomt (zie ad 1). Tegelijkertijd dient er bij het alloceren van financiële middelen in de basis rekening gehouden worden met de kosten die gemoeid zijn met passende informatiebeveiliging en gegevensbescherming. Het mag niet zo zijn dat dit sluitposten zijn op een begroting: we doen het, als er geld over is. Omgekeerd geldt dit eveneens. Bezuinigingen raken namelijk ook direct het budget dat beschikbaar is voor informatiebeveiliging en gegevensbescherming. Dit geldt ook als de dienst waarop bezuinigd wordt niet langer bestaat. Zo moet een medisch dossier op grond van wetgeving vaak nog minimaal twintig jaar worden bewaard, en ook dan moeten er voldoende financiële middelen zijn om deze gegevens te beschermen. Hier dienen bewindspersonen, politici en bestuurders zich bewust van te zijn.