

## Vragen gesteld door de leden der Kamer, met de daarop door de regering gegeven antwoorden

### 2308

Vragen van het lid **Peters** (CDA) aan de Minister van Volksgezondheid, Welzijn en Sport over *het datalek bij Jeugdzorg waardoor dossiers van duizenden kwetsbare kinderen zijn gelekt* (ingezonden 12 april 2019).

Antwoord van Minister **De Jonge** (Volksgezondheid, Welzijn en Sport) (ontvangen 16 april 2019).

Vraag 1 en 2

Kunt u bevestigen dat dat door een fout van Bureau Jeugdzorg Utrecht in totaal 3278 dossiers van 2702 kinderen zijn gelekt?<sup>1</sup>

Waarom is de oude website van Jeugdzorg Utrecht niet beveiligd afgesloten nadat deze offline is gehaald?

Antwoord 1 en 2

Datalekken zoals deze laten zien dat aandacht voor informatieveiligheid in de zorgsector steeds belangrijker wordt. Het datalek bij Samen Veilig Midden-Nederland is ontstaan door het gebruik van oude e-mailadressen met een oude domeinnaam. Deze domeinnaam was vanaf december 2017 niet meer bij Samen Veilig Midden-Nederland in beheer. Naar nu blijkt zijn de consequenties hiervan onvoldoende ingeschat en afgedekt. Samen Veilig Midden-Nederland heeft mij laten weten dat zij de oude domeinnaam weer hebben overgenomen en dat daarmee het lek gedicht is. Samen Veilig Midden-Nederland heeft mij gemeld direct na geïnformeerd te zijn over het datalek een onderzoek te zijn gestart om uit te zoeken hoe dit heeft kunnen gebeuren.

Vraag 3 en 4

Is het gebruikelijk dat binnen de jeugdzorg dossiers van patiënten onbeveiligd en geautomatiseerd doorgestuurd worden naar e-mailadressen van werknemers?

Deelt u de mening dat het niet zo kan zijn dat zorginstellingen patiëntendossiers onbeveiligd en zonder authenticatie worden rondgestuurd? Zo nee, waarom niet? Zo ja, op welke wijze denkt u te kunnen waarborgen dat dit in het vervolg wel goed wordt gedaan?

<sup>1</sup> RTL-Nieuws, «Groot datalek bij Jeugdzorg: dossiers duizenden kwetsbare kinderen gelekt», 10 april 2019

#### Antwoord 3 en 4

Ik deel de mening dat alle zorginstellingen passende maatregelen moeten nemen om patiëntdossiers en communicatie over patiënten maximaal te beveiligen. Ze moeten zorgen dat binnen hun organisaties goed met persoonsgegevens wordt omgegaan om datalekken zoals deze te voorkomen maar ook om weerbaar te zijn tegen bijvoorbeeld cyberaanvallen. Daarbij hoort onder anderen het gebruik van beveiligde e-mail voor het uitwisselen van persoonsgegevens. Alle zorg- en jeugdhulpinstellingen zouden daarom gebruik moeten maken van beveiligde e-mail verbindingen, waarvoor ook een NEN<sup>2</sup>-norm beschikbaar komt.

#### Vraag 5 en 6

Klopt het dat Bureau Jeugdzorg Utrecht niet voldeed aan de concrete normen ten aanzien van informatieveiligheid zoals door Z-CERT geformuleerd? Bent u van mening dat deelname aan Z-CERT door (jeugd)zorgaanbieders verplicht gesteld moet worden? Zo nee, waarom niet?

Welke verplichtingen hebben (jeugd)zorginstellingen voor wat het security-beleid betreft? Welke standaardnormen zijn hieraan verbonden waar in ieder geval aan voldaan moeten worden?

#### Antwoord 5 en 6

Zorginstellingen moeten onder meer voldoen aan de AVG. Ook de Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg stelt eisen aan informatieveiligheid voor het zorgveld. Deze eisen zijn neergelegd in normen ontwikkeld door het Nederlands Normalisatie-instituut (NEN). Het Computer Emergency Response Team voor de Zorg (Z-CERT) ontwikkelt geen normen waaraan zorginstellingen dienen te voldoen. Z-CERT is wel belast met monitoring, preventie en reparatie van ICT-incidenten in de zorg. Bij datalekken zoals deze kunnen aangesloten zorginstellingen rekenen op de hulp van Z-CERT. Deze organisatie fungeert ook als «brandweer» bij informatieveiligheidsincidenten in de zorg. Alle zorg- en jeugdhulpinstellingen zouden wat mij betreft aangesloten moeten zijn bij een organisatie als Z-CERT. Zoals toegezegd in reactie op de motie Ellemeet (TK 270529, nr 179) zal VWS in 2019 het verplichtstellen van de deelname van zorg- en jeugdhulpinstellingen aan Z-CERT onderzoeken.

#### Vraag 7 en 8

Wat is uw reactie op de bewering van de klokkenluiders dat er nog tientallen soortgelijke zorgorganisaties zijn waarvan de oude domeinnaam is verlopen, en die door kwaadwillenden zijn over te nemen of reeds zijn overgenomen? Bent u bereid te inventariseren welke websites dit betreft om hier zo spoedig mogelijk actie op te zetten om deze beveiligd af te (laten) sluiten?

#### Antwoord 7 en 8

Ik heb Z-CERT gevraagd om passende actie te ondernemen. Z-CERT meldt mij dat er inderdaad domeinnamen circuleren die eerder door zorginstellingen zijn gebruikt en daarna zijn vrijgegeven. Op mijn verzoek heeft Z-CERT deze domeinnamen zelf geregistreerd zodat deze niet meer voor anderen beschikbaar zijn.

#### Vraag 9

Zijn alle betrokken personen waarvan de dossiers gelekt zijn inmiddels ingelicht over dit datalek?

#### Antwoord 9

Samen Veilig Midden-Nederland heeft mij gemeld dat zij niet weten welke dossiers precies gelekt zijn, dit is door de klokkenluiders en RTL niet gedeeld. Samen Veilig Midden-Nederland heeft mij laten weten direct alle cliënten te hebben geïnformeerd en ook een speciale telefoonlijn geopend te hebben voor vragen van bezorgde burgers.

---

<sup>2</sup> NEN begeleidt en stimuleert de ontwikkeling van normen. Daarnaast beheert en publiceert NEN de voor Nederland geldende normen waaronder NTA 7516 voor veilige mail.

Vraag 10

Op welke wijze wordt dit datalek van Bureau Jeugdzorg Utrecht gedicht en op welke wijze wilt u er op inzetten dat dit soort fouten in de toekomst niet meer worden gemaakt?

Antwoord 10

Samen Veilig Midden-Nederland heeft mij laten weten direct nadat ze op de hoogte werden gesteld van het datalek een crisisteam te hebben gevormd en een Functionaris Gegevensbescherming te hebben aangesteld. De oude domeinnaam is direct weer overgenomen waardoor het lek inmiddels gedicht is. De instelling is een onderzoek gestart om uit te zoeken hoe dit heeft kunnen gebeuren. Ook is er direct melding gemaakt bij de Autoriteit Persoonsgegevens. De beveiliging van medische gegevens valt onder de verantwoordelijkheid van de zorginstellingen zelf. De Autoriteit Persoonsgegevens ziet hierop toe.