Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2019–2020

27 529 Informatie- en Communicatietechnologie (ICT) in de Zorg

Nr. 193 **BRIEF VAN DE MINISTER VOOR MEDISCHE ZORG**

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 8 oktober 2019

In mijn brief van juli jl. heb ik u geïnformeerd over de stappen die ik zet in het nemen van regie op digitale gegevensuitwisseling en heb ik u een aparte brief toegezegd na de zomer over «Informatiebeveiliging in de zorg».[1] Met deze brief, die ik mede namens de Minister van VWS verstuur, voldoe ik aan die toezegging. Tevens geef ik de gevraagde reactie op de berichten dat medische scans van 25.000 personen onbeveiligd publiek te benaderen zijn, zoals gevraagd door het Kamerlid Van den Berg naar aanleiding van vragen van het Kamerlid Ploumen.[2]

Kernboodschap en samenvatting

In deze brief meld ik u aan de hand van de voortgang op de acties die ik de afgelopen periode heb ontplooid, hoe ik in lijn met de regie op de elektronische gegevensuitwisseling, ook blijvende aandacht en regie heb genomen op het onderwerp informatieveiligheid. Het goed regelen van informatieveiligheid is onlosmakelijk verbonden met verdergaande digitalisering en verdient daarom aandacht, van mij, maar gezien de primaire verantwoordelijkheid voor informatieveiligheid bij de sector, ook van de sector zelf.
In de brief vermeld ik de ontwikkelingen met betrekking tot Z-CERT, het cybersecuritycentrum voor de zorg. Het aantal deelnemende zorginstellingen aan Z-CERT is sinds vorig jaar verdubbeld. Ik constateer dat Z-CERT tijdig betrokken was bij het datalek van de medische scans en snel en adequaat heeft gehandeld. In reactie op de motie van het Kamerlid Ellemeet Z-CERT[3] om te verkennen of deelname aan Z-CERT verplicht kan worden, is nodig dat duidelijk wordt welke type instellingen en sectoren precies onder die eventuele verplichting zouden moeten vallen en welke typen instellingen en sectoren de meeste risico lopen. Sectoren en ketens

[1] Kamerstuk 27 529, nr. 189
[2] Handelingen II 2019/20, nr. 3, Regeling van werkzaamheden
[3] Kamerstuk 27 529, nr. 177

kst-27529-193
ISSN 0921 - 7371
's-Gravenhage 2019

die de meeste risico's hebben, hebben immers het meeste baat bij een spoedige aansluiting. Ik wil samen met Z-CERT tot een dergelijke risicogestuurde aanpak komen, want of het nu een verplichting is of niet: een beheerst tempo van aansluiting is nodig om de continuïteit en kwaliteit van de dienstverlening van Z-CERT gelijke tred te laten houden met het tempo van aansluiting.

Voor de aansluiting van de jeugdhulpsector bij Z-CERT heb ik naar aanleiding van de motie van de leden Hijink en Raemakers[4] Z-CERT gevraagd samen met de jeugdhulpsector een eerste verkenning uit te voeren. Daaruit blijkt dat de hulpvraag van de jeugdhulpinstellingen niet aansluit op de huidige dienstverlening van Z-CERT. Om inzicht te krijgen in wat dan wel nodig is en wat dat vraagt van de jeugdhulpsector zelf, laat ik op dit moment pentesten uitvoeren op ICT-systemen in de jeugdhulp. Het onderzoek naar de publieke rol van Z-CERT loopt. Ik verwacht daarvan in de eerste helft van 2020 de resultaten.
In deze brief ga ik verder kort in op de Nederlandse Technische Afspraak (NTA) 7516 voor veilige email die in mei van dit jaar beschikbaar is gekomen. Ik geef de actuele stand van zaken van het Actieplan Bewustwording dat door het zorgveld ontwikkeld is. Ik vermeld de belangrijkste resultaten van het onderzoek naar opslag van medische data in Google Cloud en ik ga kort in op het rijksbrede wetenschappelijk onderzoekstraject naar cybersecurity van de Minister van OCW waar ik op aangesloten ben. Tenslotte licht ik toe dat vanwege het succes van de AVG Helpdesk ik in samenwerking met het Informatieberaad heb besloten die Helpdesk in ieder geval tot medio 2020 in stand te houden en de website tenminste tot eind 2020 in de lucht te laten blijven.

Informatieveiligheid in de zorg

Voor het leveren van goede zorg is het belangrijk dat zorgprofessionals de beschikking hebben over de juiste informatie, op het juiste moment en op de juiste plek. Digitalisering van dossiervoering en gegevensuitwisseling is hiervoor nodig en moet worden versneld. Op verzoek van het zorgveld en uw Kamer heb ik hierop meer regie genomen en bereid ik de benodigde wetgeving voor.[5] In april en juli van dit jaar heb ik u over de stappen die ik daarvoor neem geïnformeerd[6]. Ook met betrekking tot de inzet van data voor de gezondheid van ons allen ben ik bezig stappen te zetten. Ik heb u in november 2018[7] de actielijnen op dit terrein gepresenteerd en zal u aan het einde van dit jaar over de voortgang informeren. Informatieveiligheid is een belangrijke randvoorwaarde om bovenstaande ontwikkelingen waar te maken. Medische informatie is immers persoonlijke informatie en daar moet zorgvuldig mee omgegaan worden.

In mijn beleid op informatieveiligheid in de zorg onderscheid ik vier lijnen:
- *Bewust worden* van informatieveiligheid door de kennis erover te verhogen,
- *Beveiligen* van systemen met passende wet- en regelgeving en certificering,
- *Bewaken* van de naleving van de veiligheidsregels en monitoring van (cyber)kwetsbaar-heden om de weerbaarheid te vergroten en alertheid te verhogen,
- *Blussen* van (cyber)incidenten door de juiste instanties in staat te stellen cyberincidenten snel te bestrijden en de schade zoveel mogelijk te beperken.

---

[4] Kamerstuk 31 839, nr. 676
[5] Kamerstuk 27 529, nr. 166
[6] Kamerstuk 27 529, nrs. 183 en 189
[7] Kamerstuk 27 529, nr. 164

Van blussen naar een breed informatieveiligheidsbeleid

Z-CERT

Ik beschouw Z-CERT als het cybersecuritycentrum voor de zorg. In de eerste jaren na oprichting van Z-CERT is door deze organisatie met name invulling gegeven aan het *«blussen»* bij incidenten. Een goed voorbeeld daarvan is het recente optreden van Z-CERT bij het datalek waarin de medische scans van 25.000 personen waren in te zien. Het betrof drie systemen in Nederland en één op Curaçao. Voor publicatie van berichten in de pers hierover was Z-CERT hiervan al op de hoogte gebracht en een onderzoek gestart. Uit het onderzoek van Z-CERT bleek dat door de betrokken systeemeigenaren in Nederland al maatregelen waren getroffen zodat de scans al bij het onderzoek van Z-CERT niet meer in te zien waren. Voor het systeem in Curaçao heeft Z-CERT opgeschaald naar het National Cyber Security Center (NCSC), onderdeel van het Ministerie van Justitie en Veiligheid dat lands- en sectorbreed aan digitale veiligheid werkt. Het NCSC heeft het incident verder afgehandeld.

De komende periode zullen ook *«bewust worden, beveiligen en bewaken»* steeds meer verweven raken en onderdeel worden van de reguliere dienstverlening van Z-CERT. Z-CERT zal daarmee dienstverlening verzorgen op alle vier de lijnen die ik onderscheid in mijn beleid ten aanzien van informatieveiligheid in de zorg.

Dat Z-CERT aan belang blijft toenemen blijkt ook uit het aantal aangesloten zorginstellingen dat is verdubbeld ten opzichte van vorig jaar. Inmiddels zijn alle ziekenhuizen (academisch, topklinisch en algemeen) aangesloten. In totaal heeft Z-CERT heeft op dit moment circa 120 deelnemers. Dit waren vorig jaar nog circa 60 deelnemers.

In reactie op de motie van het Kamerlid Ellemeet Z-CERT[8] om te verkennen of deelname aan Z-CERT verplicht kan worden, is nodig dat duidelijk wordt welke type instellingen en sectoren precies onder die eventuele verplichting zouden moeten vallen en welke typen instellingen en sectoren de meeste risico lopen. Sectoren en ketens die de meeste risico's hebben, hebben immers het meeste baat bij een spoedige aansluiting. Voor ZZP'ers in de zorg is aansluiting bij Z-CERT wellicht minder opportuun. Ik wil samen met Z-CERT tot een dergelijke risicogestuurde aanpak komen, want of het nu een verplichting is of niet: een beheerst tempo van aansluiting is nodig om de continuïteit en kwaliteit van de dienstverlening van Z-CERT gelijke tred te laten houden met het tempo van aansluiting.

Voor de aansluiting van de jeugdhulpsector heb ik naar aanleiding van de motie van de leden Hijink en Raemakers[9] Z-CERT gevraagd samen met de jeugdhulpsector een eerste verkenning uit te voeren. Z-CERT heeft met Jeugdzorg Nederland en een aantal gecertificeerde instellingen gesproken om te bezien wat de wensen en behoeften zijn van de jeugdhulpsector voor het verbeteren van de informatieveiligheid. Daaruit blijkt dat de hulpvraag van de jeugdhulpinstellingen

niet aansluit op de huidige dienstverlening van Z-CERT. De dienstverlening van Z-CERT richt zich momenteel primair op de cure sector (ziekenhuizen, GGZ-instellingen en categorale instellingen) terwijl de behoefte van jeugdhulpinstellingen meer individueel van aard is. Jeugdhulpinstellingen hebben hun IT vaak uitbesteed aan externe

[8] Kamerstuk 27 529, nr. 177
[9] Kamerstuk 31 839, nr. 676

ICT-leveranciers die zelf de informatiebeveiliging regelen. Binnen de jeugdhulpinstellingen zelf is weinig gespecialiseerde, technische informatieveiligheidskennis aanwezig. De dienstverlening van Z-CERT is technisch van aard, terwijl de behoefte van jeugdhulpinstellingen functioneel organisatorisch van aard is. Zo monitort Z-CERT operational alerts en kwetsbaarheden, controleert periodiek of domeinnamen op «zwarte lijsten staan» van virussen, wormen en botnets en adviseert over aanpak en oplossing van cyberincidenten. De behoefte van jeugdhulpinstellingen ligt met name op risicomanagement, het verhogen van cyberbewustwording van medewerkers, het ontwikkelen van concrete uitwerkingen op basis van de NEN-norm 7510 en het doorlichten van de IT-omgeving binnen de jeugdhulpsector.

Ik vind het belangrijk dat snel duidelijk wordt wat precies nodig is voor Z-CERT en van de jeugdhulpsector zelf, zodat vanuit het Ministerie van VWS waar nodig kan worden ondersteund. Ik laat daarom zoals door de leden Hijink en Raemakers in hun motie[10] verzocht, pentesten uitvoeren op de ICT systemen in de jeugdhulpsector. Deze worden door een extern bureau uitgevoerd bij zes jeugdhulpaanbieders en gecertificeerde instellingen. De opdrachtnemer zal in samenwerking met Jeugdzorg Nederland, een rapport opstellen met een samenvatting, een schets met globale gevolgtrekkingen voor de sector en een advies over het verhogen van het informatiebeveiligingsniveau binnen de sector. De Minister van VWS zal u begin 2020 informeren over de leerpunten die uit deze testen voor de jeugdzorg en mogelijk het brede zorgveld zijn gekomen. Aan de hand van de pentest resultaten zal ik in de loop van 2020 nadere besluiten nemen over de wenselijkheid en tempo van aansluiting van jeugdhulpinstellingen bij Z-CERT.

Het onderzoek naar de publieke rol van Z-CERT loopt. Aan de hand van interviews en gesprekken met stakeholders wordt een grove schets van huidige en mogelijke toekomstige taken en scenario's gegeven. Ik verwacht daarvan in de eerste helft van 2020 de resultaten.

Bewustwording

Actieplan bewustwording

Aanvankelijk had een aantal koepels[11] het initiatief genomen voor een actieplan om de veiligheid van patiëntgegevens te verhogen. Sinds eind 2018 is de vereniging Brancheorganisaties Zorg (BOZ) actief op dit onderwerp. Door middel van e-learning en campagnes zal bijgedragen worden aan het verhogen van de bewustwording om veilig om te gaan met informatie. Ik zal dit initiatief vanuit de zorgsector van harte ondersteunen.

Beveiligen

Veilige mail

In mei van dit jaar is de Nederlandse Technische Afspraak (NTA) 7516 beschikbaar gekomen, dit is een veldnorm die kaders stelt voor veilig e-mailen van medische persoonsgegevens in de zorg. De NTA 7516 is in opdracht van het Informatieberaad Zorg door NEN opgesteld in nauwe samenwerking tussen mijn ministerie en groot aantal IT-leveranciers van veilige mail producten en organisaties in het veld. Daarmee zorgen we dat

[10] Kamerstuk 31 839, nr. 676
[11] NVZ, NFU, ZKN en GGZ Nederland

de leveranciers veilige en interoperable mailproducten leveren. Zorginstellingen ondersteunen we met communicatie bij het invoeren van de norm.

Opslag van medische data in Google Cloud

Bij het *beveiligen* van medische gegevens is door een aantal zorginstellingen gekozen voor het opslaan van medische data in de cloud. Naar aanleiding van de berichtgeving in het AD van 30 maart jl. over de opslag van medische data in de Google Cloud, heb ik een onafhankelijk advies gevraagd over de wenselijkheid van de opslag van medische data bij cloudproviders met vestigingslocaties in Nederland, de EU, de Verenigde Staten en overige landen. Dit advies vindt u in de bijlage[12]. De Autoriteit Persoonsgegevens (AP) liet mij weten een verkennend onderzoek te gaan doen naar eventuele overtredingen van de AVG door het betreffende bedrijf. Inmiddels is duidelijk dat de AP op basis van de gesprekken met en verstrekte informatie door het betreffende bedrijf, geen aanleiding ziet tot het instellen van een nader controlerend onderzoek.

Uit het onderzoek dat ik heb laten verrichten, is naar voren gekomen dat het wenselijk is om gebruik te maken van een cloudprovider met een vestiging, vertegenwoordiging of opslagcapaciteit binnen de Europese Unie. Op deze cloudproviders is immers de AVG van toepassing. Hiermee worden de data beschermd tegen onrechtmatig gebruik door de cloudprovider en kan naleving van de AVG effectief worden afgedwongen. Ik zal de zorginstellingen hierop wijzen en ga ervan uit dat zij voldoende maatregelen treffen in bijvoorbeeld de aanbesteding om de data alsnog goed te beschermen. Hiermee wil ik aanvullende wet- en regelgeving voor zorgaanbieders voorkomen.

De onderzoekers adviseren daarnaast om het versleutelen van de informatie vóór deze in de cloud geplaatst wordt, waardoor er sprake is van een dubbele versleuteling. Ik zal het veld hierop wijzen zodat zij afspraken kunnen maken over de toepassing van deze technische maatregelen.

Beveiligen en bewaken

Zorg als vitale sector

Met betrekking tot het aanwijzen van de zorg als vitale sector zoals bedoeld in de Wet beveiliging netwerk- en informatiesystemen (Wbni), verken ik op dit moment of het nodig is een herbeoordeling te doen op het besluit de zorg niet als vitale sector aan te merken.

Ongeacht de uitkomst hiervan vind ik het van belang dat de zorg aansluit bij het door de Minister van Justitie en Veiligheid in te richten Landelijk Dekkende Stelsel voor uitwisseling van informatie over digitale dreigingen binnen de vitale sectoren. In het kader van het versterken van dit stelsel zal door de Ministerie van Justitie en Veiligheid dit jaar worden beoordeeld of Z-CERT kan worden aangewezen als computercrisisteam.

Onderzoek en ondersteuning

Rijksbreed onderzoek

Hoewel de zorgsector haar eigen uitdagingen heeft, zijn veel vraagstukken niet uniek. Ik sluit daarom aan bij het grootschalige wetenschappelijk

[12] Raadpleegbaar via www.tweedekamer.nl

onderzoektraject dat door de Minister van Onderwijs, Cultuur en Wetenschap is ingezet naar Rijksbrede cybersecurity waar de zorg één van de sectoren is die wordt onderzocht.

AVG Helpdesk

Ik faciliteer zorginstellingen met informatie over het borgen van privacy en bij het interpreteren van de AVG. Daarom is door mij samen met meer dan 20 koepelorganisaties, in mei 2018 de AVG Helpdesk voor Zorg, Welzijn en Sport opgericht. Gehoord hebbende de blijvende behoefte van het veld, heb ik in samenwerking met het Informatieberaad besloten de AVG Helpdesk in ieder geval tot medio 2020 mede in stand te houden. De website zal tenminste tot eind 2020 in de lucht blijven.

Tot slot

Het naar een hoger plan tillen van informatieveiligheid binnen de zorgsector blijft de komende jaren één van mijn speerpunten. Op nationaal niveau zoek ik actief samenwerking met het NCSC en de andere departementen. Op Europees niveau draag ik mijn steentje bij aan gezamenlijke beleidsontwikkeling in de aanpak van cybersecurity, aangezien cyberdreigingen vrijwel per definitie een internationale component hebben. Het goed regelen van informatieveiligheid is onlosmakelijk verbonden met verdergaande digitalisering.

De Minister voor Medische Zorg,
B.J. Bruins