Risicogestuurde aanpak voor aansluiten instellingen bij Z-Cert

9 oktober 2019

De bewindsman geeft in de Kamerbrief een overzicht van acties die hij de afgelopen periode heeft ontplooid op het gebied van informatiebeveiliging en gegevensuitwisseling in de zorg. Bruins benadrukt dat hij – in lijn met de regie op de elektronische gegevensuitwisseling, ook blijvende aandacht en regie heeft genomen op het verwante onderwerp informatieveiligheid. De primaire verantwoordelijkheid hiervoor ligt echter nog steeds bij zorgaanbieders zelf, benadrukt Bruins.

Verdubbeling aansluiting bij Z-CERT

Het aantal deelnemende zorginstellingen aan Z-CERT is sinds vorig jaar verdubbeld, stelt Bruins. Hij constateert dat Z-CERT tijdig betrokken was bij een datalek van medische scans eerder dit jaar en snel en adequaat heeft gehandeld. Voordat er een verplichting tot aansluiting bij Z-CERT komt, zoals Tweede Kamerlid Corinne Ellemeet (GroenLinks) in een motie heeft gevraagd, moet duidelijk wordt welke type instellingen en sectoren precies onder die eventuele verplichting moeten vallen en welke typen instellingen en sectoren de meeste risico lopen.

Sectoren en ketens die de meeste risico’s hebben, hebben volgens Bruins het meeste baat bij een spoedige aansluiting. dat vergt een risicogestuurde aanpak, 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.’

Z-CERT en jeugdzorg

Voor de aansluiting van de jeugdhulpsector bij Z-CERT heeft Bruins naar aanleiding van een andere motie (Hijink en Raemakers) aan Z-CERT gevraagd om samen met de jeugdhulpsector een verkenning uit te voeren naar de mogelijkheden van aansluiting. De hulpvraag van jeugdhulpinstellingen blijkt echter niet aan te sluiten op de huidige dienstverlening van Z-CERT.

- Zo richt de dienstverlening van Z-CERT zich momenteel primair op de cure sector (ziekenhuizen, GGZ, categorale instellingen) terwijl de behoefte van jeugdhulpinstellingen meer individueel van aard is.
- Verder hebben jeugdhulpinstellingen hun IT vaak uitbesteed aan externe ICT-leveranciers die zelf de informatiebeveiliging regelen. Binnen de instellingen 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.

Om inzicht te krijgen in wat dan wel nodig is en wat dat vraagt van de jeugdhulpsector zelf, laat Bruins momenteel pentesten (penetratietesten) uitvoeren op ICT-systemen in de jeugdhulp. Het onderzoek naar de publieke rol van Z-CERT loopt. Bruins verwacht daarvan in de eerste helft van 2020 de resultaten.

NTA, bewustwording

In de Kamerbrief gaat Bruins verder nog kort in op de Nederlandse Technische Afspraak (NTA) 7516 voor veilige e-mail die in mei van dit jaar beschikbaar is gekomen. Ook schetst hij de actuele stand van zaken van het Actieplan Bewustwording dat door het zorgveld ontwikkeld is, vermeldt hij de belangrijkste resultaten van het onderzoek naar opslag van medische data in Google Cloud en gaat hij kort in op het rijksbrede wetenschappelijk onderzoekstraject naar cybersecurity van de minister van OCW waar VWS op aangesloten is.

Tot slot blijkt volgens Bruins de AVG Helpdesk (waar zorgpartijen met vragen over de impact van de AVG op hun processen terecht kunnen) zo succesvol te zijn dat hij in samenwerking met het Informatieberaad Zorg heeft besloten deze helpdesk in ieder geval tot medio 2020 in stand te houden en de website tenminste tot eind 2020 in de lucht te laten blijven.

Medische data in de cloud

Voor wat betreft de twee onderzoeken naar de opslag van medische data voor kwaliteitsdoelen in Google Cloud, schrijft Bruins dat de toezichthouder Autoriteit Persoonsgegevens inmiddels besloten heeft dat verder onderzoek niet nodig is.

Uit het eigen onafhankelijk onderzoek dat Bruins liet verrichten, kwam naar voren dat het wenselijk is om gebruik te maken van een cloudprovider met een vestiging, vertegenwoordiging of opslagcapaciteit binnen de Europese Unie (zoals het Google Cloud datacentrum in de Groningse Eemshaven). Op deze cloudproviders is namelijk de AVG van toepassing. Zo worden 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. Bruins: Ik zal het veld hierop wijzen zodat zij afspraken kunnen maken over de toepassing van deze technische maatregelen.

In het eerstvolgende nummer van ICT&health, dat in de derde week van oktober verschijnt, wordt uitgebreid ingegaan op het werk van Z-CERT.