Ministerie van Volksgezondheid,
Welzijn en Sport

> Retouradres Postbus 20350 2500 EJ Den Haag

De Voorzitter van de Tweede Kamer
der Staten-Generaal
Postbus 20017
2500 EA DEN HAAG

Bezoekadres:
Parnassusplein 5
2511 VX Den Haag
T 070 340 79 11
F 070 340 78 34
www.rijksoverheid.nl

Ons kenmerk
1366703-178223-DICIO

Bijlagen
-

Uw kenmerk
2018Z10608

Correspondentie uitsluitend richten aan het retouradres met vermelding van de datum en het kenmerk van deze brief.

Datum 2 juli 2018
Betreft Commissiebrief Tweede Kamer inzake waarom ziekenhuizen en andere zorgaanbieders volgens de memorie van de toelichting van de Cybersecuritywet niet aangewezen worden als essentiële diensten en toezegging rapporteren voortgang Actieplan informatiebeveiliging

Geachte voorzitter,

Aanleiding voor deze brief is het verzoek van de vaste commissie voor Volksgezondheid, Welzijn en Sport van 6 juni om een nadere toelichting waarom ziekenhuizen en andere zorgaanbieders volgens de memorie van toelichting van de Cybersecuritywet niet aangewezen worden als essentiële dienst (Regels ter implementatie van richtlijn EU 2016/1148 Cybersecuritywet, nu genaamd Wet beveiliging netwerk- en informatiesystemen (Wbni) (34883). In deze brief geef ik de gevraagde nadere toelichting. Verder ga ik in op de voortgang van het Actieplan informatieveiligheid. Hiermee geef ik invulling aan de toezegging aan de Tweede Kamer in de brief van 20 juni 2017[1], waarin ik onder meer uiteen heb gezet dat de zorgsector haar eigen maatregelen neemt om de informatieveiligheid te verhogen. Een onderdeel daarvan is het Actieplan van zorgkoepels ter verhoging van de bewustwording van informatieveiligheid.

Geen aanwijzing van aanbieders van essentiële diensten in de zorg

De Wbni strekt ter uitvoering van de Europese NIB-richtlijn. Het doel van deze richtlijn is om, ter ondersteuning van het functioneren van onze samenleving en economie, eenheid en samenhang te brengen in Europees beleid voor netwerk- en informatiebeveiliging, door de digitale paraatheid te vergroten en de gevolgen van cyberincidenten te verkleinen. In bijlage II van de NIB-richtlijn wordt de gezondheidszorg genoemd als sector met potentiële aanbieders van essentiële diensten (AED's), met als deelsector zorginstellingen. Het is vervolgens aan de lidstaten zelf te bepalen of en welk deel van de zorgsector tot de scope van de richtlijn behoort. Voor de implementatie van de NIB-richtlijn worden Rijksbreed de criteria voor vitale infrastructuur gebruikt om te bepalen of er AED's zijn. Omdat we in Nederland graag willen zorgen voor samenhang tussen de categorieën 'essentiële diensten' en 'vitale processen', komt dit erop neer dat als een proces

[1] https://www.tweedekamer.nl/kamerstukken/brieven_regering/detail?id=2017Z08640&did=2017D18113

als vitaal wordt aangemerkt, dit dan ook als een dienst van essentieel belang in de zin van de NIB-richtlijn wordt aangemerkt.

In 2015 heeft de toenmalige minister van het ministerie van Justitie en Veiligheid een herijking doen plaatsvinden van de vitale processen in het kader van de nationale veiligheid[2], zoals gerapporteerd aan uw Kamer in de voortgangsbrief nationale veiligheid d.d. 12 mei 2015. Het benoemen van vitale processen doet de Rijksoverheid om maatregelen te kunnen treffen die het risico op ernstige crises verkleinen en om in geval van een crisis sneller prioriteiten te kunnen stellen voor de respons op de crisis. Het doel van de herijking was een betere selectie te maken aan de hand van strengere criteria. Een proces in de samenleving is vitaal als uitval leidt tot:

- meer dan 5 miljard euro schade of 1.0 % daling reëel inkomen
- meer dan 1.000 doden, ernstig gewonden of chronisch zieken
- meer dan 100.000 personen ondervinden emotionele problemen of ernstig maatschappelijke overlevingsproblemen

Wij zijn destijds tot de conclusie gekomen dat er geen situaties zijn waarin uitval van ICT-systemen of -structuren in de zorg deze gevolgen zullen hebben. In Nederland is er namelijk geen centrale vitale technische infrastructuur voor de gehele zorg die bij uitval dergelijke gevolgen heeft voor landsbrede zorg. De zorg en de zorginfrastructuur in Nederland zijn niet centraal georganiseerd, maar decentraal en de instellingen zijn zelf verantwoordelijk voor de veiligheid van informatievoorziening en gegevensuitwisseling. Bij uitval van een deel van de zorg kan deze zorg in veel gevallen worden overgenomen door andere zorgaanbieders. Daarom heeft het ministerie van VWS geen processen in de zorg als vitaal geïdentificeerd en zijn er dus geen AED's aangewezen.

De continue beschikbaarheid en betrouwbaarheid van informatievoorziening en gegevensuitwisseling in de zorg is echter van groot belang voor de patiëntveiligheid. Wij hebben ons daarom met de zorgsector wel gericht op andere maatregelen om de veiligheid van de technische infrastructuur in de zorg te verhogen, zoals mijn ambtsvoorganger vorig jaar bij eerder genoemde brief van 20 juni 2017 aan uw Kamer heeft gemeld. Wij hebben specifieke normen voor informatieveiligheid in de zorg vastgesteld: De NEN-normen 7510, 7512 en 7513. Verder heeft de sector haar eigen sectorale CERT (Computer Emergency Response Team) voor de Zorg (Z-CERT) in het leven geroepen. Z-CERT draagt zorg voor specifieke monitoring, preventie en reparatie van informatieveiligheidsinbreuken in het zorgveld en medische apparatuur. Sinds 24 januari 2018 is Z-CERT officieel van start gegaan. Verder hebben wij samen met de koepels NVZ, NFU, ZKN en GGZ Nederland een Actieplan opgezet voor de verhoging van de veiligheid van patiëntgegevens.

[2] Kamerbrief Ministerie van Justitie en Veiligheid, voortgangsbrief nationale veiligheid, 12 mei 2015

Voortgang Actieplan Informatieveiligheid

Het doel van het Actieplan Informatiebeveiliging[3], is om de informatieveiligheid en privacybescherming binnen de zorg structureel op een hoger niveau te brengen. De koepels willen de initiatieven die zij zelf reeds ontplooien met elkaar delen, op een hoger plan zetten en beschikbaar stellen aan andere koepels en zorginstellingen. Hierbij wordt ingezet op zowel cultuur, structuur als de compliance ten aanzien van wetgeving.

De cultuur in het zorgdomein is inherent ingericht op patiëntveiligheid en privacy. Door de toenemende ICT ontwikkeling en inbreuken op de privacy is daarom meer aandacht voor informatiebeveiliging noodzakelijk. Om het onderwerp ook bij zorgverleners onder de aandacht te brengen is in oktober 2017 'De maand van de informatieveiligheid'[4] gelanceerd. Door een communicatiecampagne is hierin veel aandacht gegeven aan informatieveilig werken door zorgverleners. Dit is met diverse instrumenten ondersteund, zoals: een serious game, kaartspellen, posters, folder, checklist cybersecurity en toolkit informatiebeveiliging. Voorbereidingen voor een nieuwe campagne in 2018 zijn intussen gestart.

Koepels van zorgaanbieders bieden een structuur voor onderlinge kennisdeling en geven aandacht aan goede praktijkvoorbeelden. Netwerken van security officers en functionarissen gegevensbescherming worden gefaciliteerd met als doel ervaringen en aanpak met elkaar te delen en intervisie te bevorderen. Z-CERT speelt een coördinerende rol als het gaat om de technische uitdagingen rondom informatiebeveiliging, waar de technische afdelingen bij zorgaanbieders en leveranciers te maken krijgen.

Veel aandacht is de afgelopen periode gegaan naar compliance met de Algemene Verordening Gegevensbescherming (AVG). Koepels van zorgaanbieders hebben, naast het organiseren van bijeenkomsten, communicatiemateriaal en sectorspecifieke hulpmiddelen, ook gezamenlijk instrumenten gerealiseerd. Een mooi voorbeeld hiervan is het model verwerkerovereenkomst van de Brancheorganisaties Zorg (BoZ), die inmiddels ook door zorgaanbieders buiten de tweedelijns zorg wordt gebruikt. Verder hebben we samen met de koepels een gezamenlijke AVG Helpdesk[5] ingericht voor het beantwoorden van vragen. Op de speciaal ingerichte website staan antwoorden op veelgestelde vragen die met de Autoriteit Persoonsgegevens zijn afgestemd. Op deze manier krijgen zorgaanbieders praktische privacygerelateerde vragen beantwoord en kunnen ze goede voorbeelden en instrumenten vinden die door de deelnemende partijen zijn ontwikkeld.

Z-CERT is door de opstellers van het Actieplan aangewezen als projectleider voor de uitvoering van de acties in het Actieplan. Z-CERT heeft de activiteiten rondom het Actieplan verder uitgewerkt en de eerste resultaten worden in het najaar van

[3] https://www.tweedekamer.nl/downloads/document?id=4f67b7ed-30de-4875-aeb1-3561083c2936&title=Actieplan%3A%20Informatiebeveiliging%20in%20de%20medisch-specialistische%20zorg%20en%20geestelijke%20gezondheidszorg.pdf
[4] www.zorgzekeren.nl
[5] https://www.avghelpdeskzorg.nl/

2018 verwacht. Zo zal er een een portaal opgezet worden waar producten, expertise en ervaringen centraal kunnen worden gedeeld.

Ons kenmerk
1366703-178223-DICIO

Z-CERT werkt verder aan haar eigen expertiseverdieping en uitbreiding van serviceverlening. Z-CERT breidt haar producten en dienstverlening verder uit in afstemming met zorgaanbieders, zorg-IT leveranciers, Zorg CERTs uit andere landen en het Nationaal Cyber Security Centrum. Zo wordt de gebundelde kennis van de zorgaanbieders en de specialistische kennis van Z-CERT ingezet voor het behoud van een (informatie)veilige zorg.

Hoogachtend,

de minister voor Medische Zorg,
en Sport,

Bruno Bruins