Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2023–2024

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

30 821 **Nationale Veiligheid**

Nr. 311 **BRIEF VAN DE MINISTER VAN VOLKSGEZONDHEID, WELZIJN EN SPORT**

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 12 december 2023

De processen en diensten die samen de vitale infrastructuur vormen zijn het fundament waarop de Nederlandse samenleving draait. Elektriciteit, toegang tot internet, drinkwater en betalingsverkeer zijn hier voorbeelden van. Uitval, verstoring of manipulatie van dergelijke processen of diensten kan grote gevolgen hebben voor het functioneren van de Nederlandse economie en maatschappij en in het uiterste geval een bedreiging vormen voor de nationale veiligheid. Daarom werken overheden, bedrijven, organisaties, inlichtingen- en veiligheidsdiensten voortdurend samen aan het beschermen van de weerbaarheid van onze vitale infrastructuur.

De zorg vormde tot nu toe geen onderdeel van de Nederlandse vitale infrastructuur. Met deze brief informeer ik u, mede namens de Minister voor Langdurige Zorg en Sport, de Staatssecretaris van Volksgezondheid, Welzijn en Sport en de Minister van Justitie en Veiligheid, over de vitaal verklaring van (delen van) de zorgsector. Ik doe dit binnen de kaders van de implementatie van de Europese Critical Entities Resilience[1] richtlijn (CER) en van de herziene richtlijn Network- and Information Security[2] (NIS2). Dit om de fysieke en digitale weerbaarheid van het zorgstelsel te verhogen en daarmee stappen te maken om alle instellingen en organisaties in de zorg op een digitaal veiliger niveau te brengen.

De Minister van Justitie en Veiligheid voert de regie op de implementatie van de richtlijnen als coördinerend bewindspersoon voor de bescherming van de vitale infrastructuur. De vakdepartementen beoordelen welke processen vitaal zijn binnen hun systeemverantwoordelijkheid en stellen algemene kaders en sectorale beleid, wet- en regelgeving vast. Ik ben daarin verantwoordelijk voor de zorgsector. Deze brief sluit aan op de

[1] CER EUR-Lex – 52020PC0829 – EN – EUR-Lex (europa.eu).
[2] NIS2 https://eur-lex.europa.eu/legal-content/NL/TXT/?uri=OJ:L:2022:333:TOC.

kst-27529-311
ISSN 0921 - 7371
's-Gravenhage 2023

brief[3] over de versterkte aanpak bescherming vitale infrastructuur van de Minister van Justitie en Veiligheid van 17 mei 2023.

Waar staan we nu?

Digitale weerbaarheid – NIS2 in de zorg

Burgers en zorgverleners worden in bijna alle aspecten van zorg ondersteund door data en digitale toepassingen. Digitalisering in de zorg vervult een wezenlijke rol en dient veilig te gebeuren. Daarbij is het uitgangspunt dat digitale infrastructuren te allen tijde overeind dienen te blijven om de continuïteit en kwaliteit van zorg te waarborgen.

In Nederland is de huidige NIS1-richtlijn sinds 2018 geïmplementeerd in de Wet beveiliging netwerk- en informatiesystemen (Wbni). Deze wet streeft ernaar de digitale weerbaarheid van Nederland, en in het bijzonder van vitale aanbieders, de Rijksoverheid en digitale dienstverleners, te waarborgen. Op dit moment zijn er geen aanbieders in de zorgsector aangewezen.

De herziene NIS2-richtlijn heeft tot doel om de digitale weerbaarheid van essentiële en belangrijke entiteiten binnen de EU naar een hoger gemeenschappelijk niveau te brengen en moet nog worden geïmplementeerd. De sector zorg valt onder de reikwijdte van de NIS2-richtlijn, waarmee o.a. zorgaanbieders, farmaceutische fabrikanten en medische hulpmiddel producenten rechten en plichten krijgen ten aanzien van de beveiliging van hun organisatie. Bij de Stichting Koninklijk Nederlands Normalisatie Instituut (NEN) zijn alle nationale normen over de informatiebeveiliging in de zorg vastgelegd. De bestaande NEN-normen over informatiebeveiliging in de zorg, waaronder de NEN 7510, bieden een uitgangspunt als normenkader.

Fysieke weerbaarheid – CER in de zorg

De CER-richtlijn is een nieuwe richtlijn die richt zich op de fysieke weerbaarheid van kritieke entiteiten en diensten in een aantal sectoren, waaronder de zorgsector. Het gaat hierbij om entiteiten die diensten verlenen die van essentieel belang zijn voor de instandhouding van vitale en maatschappelijke activiteiten. De richtlijn richt zich op een aantal sectoren waaronder de gezondheidszorg, waarbinnen bedrijven en organisaties door lidstaten kunnen worden aangewezen als kritieke entiteit.

Vitaal in de zorg

De Nederlandse zorg was tot op heden geen onderdeel van de vitale infrastructuur in Nederland. De voormalig Minister van VWS heeft, mede op verzoek van de Tweede Kamer, in 2021 besloten opnieuw te beoordelen of de zorg in Nederland onderdeel zou moeten worden van de vitale infrastructuur. Ik heb deze herbeoordeling gebaseerd op scenario's met *maximale* uitval: een overstroming en een digitale verstoring. Op basis van deze herbeoordeling, merk ik nog nader te bepalen onderdelen van de zorg als vitaal aan.

Waar gaan we naartoe?

De komende tijd wordt door het kabinet gewerkt aan de totstandkoming van wetsvoorstellen ter implementatie van de NIS2- en CER-richtlijnen. De

[3] Kamerstukken II 2022/2023, 30 821, nr. 182.

conceptwetgeving zal volgend jaar in consultatie worden gebracht, zodat bedrijven en organisaties er kennis van kunnen nemen en hierop kunnen reageren. Op dat moment kan meer duidelijkheid geboden worden over de concrete vertaling in nationale wetgeving (bijvoorbeeld welke entiteiten in de zorg wel of niet onder de richtlijnen gaan vallen), zodat iedereen zich kan voorbereiden. De komende periode wordt uitgewerkt hoe de wettelijk kaders voor de verplichtingen uit de richtlijn nader vormgegeven kunnen worden. Om ervoor te zorgen dat er passende beveiligingsmaatregelen genomen worden, krijgen bedrijven en organisaties (entiteiten) die onder de wetgeving gaan vallen, te maken met wettelijke verplichtingen.

Digitale weerbaarheid – NIS2 in de zorg

De NIS2-richtlijn zal naar verwachting gaan gelden voor maximaal 2000 organisaties die actief zijn in de Nederlandse zorgsector zoals zorgaanbieders, EU-referentielaboratoria, entiteiten die farmaceutische producten of medische hulpmiddelen vervaardigen. Deze organisaties dienen verplicht preventieve maatregelen te nemen tegen cyberincidenten (zorgplicht), grootschalige incidenten te melden (meldplicht) en bij ernstige bedreigingen van hun netwerk de ontvangers van hun diensten te informeren over mogelijke gevolgen (informatieplicht). Aanvullend verplicht de NIS2-richtlijn dat deze organisaties zich registeren (registratieplicht) en aan de verplichtingen dienen te voldoen vanaf de inwerkingtreding. Dit betekent onder meer dat ziekenhuizen, laboratoria en andere zorginstellingen bij het ingaan van de implementatiewet hun netwerk- en informatiebeveiliging op orde moeten hebben overeenkomstig de eisen zoals gesteld in de NIS2.

De NIS2-richtlijn maakt onderscheid tussen belangrijke en essentiële entiteiten onder meer de entiteiten die actief zijn in de sector zorg. Entiteiten met meer dan 50 fte en/of 10 miljoen euro omzet worden geclassificeerd als belangrijk. Entiteiten met meer dan 250 fte en/of 50 miljoen euro omzet die actief zijn in de gezondheidszorg worden geclassificeerd als essentieel.

Het onderscheid tussen belangrijke of essentiële entiteit heeft te maken met hoe de toezichthouder zal toezien en zal handhaven evenals de maatregelen die de toezichthouder in dat kader kan treffen.

Naast plichten krijgen essentiële en belangrijke entiteiten ook rechten. Zo kunnen ze aanspraak maken op dienstverlening van een Computer Security Incident Response Team. Op dit moment voert Z-CERT vergelijkbare taken uit voor partijen in de zorgsector. De taken van het Computer Security Incident Response Team voor de verschillende sectoren[4] onder de NIS2-richtlijn zullen worden geregeld in de implementatiewet en de bijbehorende lagere regelgeving.

Fysieke weerbaarheid – CER in de zorg

De richtlijn zal er door het voorschrijven van geharmoniseerde minimumvoorschriften voor zorgen dat aanbieders van essentiële diensten hun weerbaarheid verhogen dan wel op peil houden. De richtlijn schrijft voor dat kritieke entiteiten onder meer op basis van een risicobeoordeling, weerbaarheidsverhogende maatregelen moeten nemen. Afhankelijk van de risicobeoordeling van de nog aan te wijzen entiteiten zullen de

[4] Kamerstuk 26 643, nr. 1058 inzake de integratie Digital Trust Center (DTC, CSIRT DSP en NLCS). En bijlage 1 CISRT stelsel- een beleidskader voor het inrichten van het stelsel met nationale en sectorale CSIRT's in Nederland.

maatregelen in de Nederlandse wetgeving worden uitgewerkt op basis van passend en evenredigheid. De komende periode zal ik in nauw overleg met de Minister van Justitie en Veiligheid en het zorgveld de implementatie van de CER-richtlijn en wat dit betekent voor betrokken zorgpartijen verder uitwerken. Daarnaast wordt nagegaan hoe de informatie over fysieke dreigingen en risico's beter kan worden gedeeld in de zorg.

Ik zal het komende half jaar criteria opstellen die bepalen welke entiteiten in de (gezondheids-)zorg worden aangewezen als kritieke entiteit en aan de verplichtingen van de CER-richtlijn moeten voldoen. Eén van de criteria, zoals genoemd in de richtlijn, stelt dat een incident aanzienlijk verstorende effecten moet hebben. Dit betekent dat het gaat om een selectie van (een beperkt aantal) entiteiten met een unieke functie of voorziening in de zorg in Nederland die noodzakelijk is. Dergelijke elementen dienen gezamenlijk en integraal te worden afgewogen, waarbij ook de geografische spreiding een rol kan spelen. Hierover zal ik uw Kamer informeren.

De criteria (zoals het aanmerken van incidenten die meldplichtig zijn) voor de aangewezen entiteiten zal worden afgestemd met de Inspectie voor de Gezondheidszorg en Jeugd (IGJ), die als toezichthouder op de kwaliteit en veiligheid ook toeziet op de informatiebeveiliging van de zorg.

Vitaal in de zorg

De volgende stap binnen de vitaalbeoordeling van de zorg is om een beperkt aantal vitale processen in kaart te brengen en vitale aanbieders aan te merken. Ik zal hiervoor de criteria van de CER-richtlijn gebruiken. Alleen organisaties die een wezenlijke verantwoordelijkheid hebben bij het ongestoord verlopen van vitale processen zijn «vitale aanbieders». Vitale aanbieders zijn primair verantwoordelijk voor de continuïteit, integriteit en vertrouwelijkheid van het proces en de informatie die wordt gebruikt binnen het proces. Het is voor hen belangrijk te weten welke verantwoordelijkheden, rechten en plichten ze als vitale aanbieder hebben. Ik zal deze de komende tijd, samen met betrokken partijen, in kaart brengen.

De vitaalverklaring van de zorg zal pas *concreet* consequenties hebben, wanneer zorgaanbieders worden aangemerkt als vitale aanbieder en aangewezen zijn als kritieke entiteit (onder de nog te bepalen criteria op basis van de CER-richtlijn). In overleg met de zorgsector en de Minister van Justitie en Veiligheid zal ik nagaan hoe de sector kan worden ondersteund in dit proces en hoe de sector helder geïnformeerd kan worden.

Toezeggingen en moties

Met deze brief doe ik een aantal toezeggingen en moties af. Hiermee geef ik invulling aan de motie van het lid van den Berg van 11 maart 2020[5], aan de motie van de leden Van den Hil en Tielen van 14 september 2022[6] en aan de motie van het lid van den Berg van 14 september 2022 (Kamerstuk 35 925 XVI, nr. 180)[7]. Bij het Hoofdlijnendebat van 8 maart 2022 heeft de Kamer mij gevraagd om in de vitaalbeoordeling ook aandacht te besteden aan de risico's van cybercrime voor ziekenhuizen. In de vitaalbeoordeling is gekeken naar de effecten van de uitval van digitale systemen. Via deze

[5] Kamerstukken II 2019/2020, 30 821, nr. 103.
[6] Kamerstukken II 2021/2022, 35 824, nr. 41.
[7] Kamerstukken II 2021/22, 35 824, nr. 30.

brief geef ik invulling aan deze toezegging. De wettelijke maatregelen van de richtlijn van de NIS2 zullen de beveiliging van digitale systemen in onder meer de zorgsector versterken.

Hoe houd ik uw Kamer en betrokken zorgpartijen op de hoogte?

Over de precieze inhoud van de implementatiewetgeving en bijbehorende keuzes zal uw Kamer bij de parlementaire behandeling van de wetsvoorstellen worden geïnformeerd door de Minister van Justitie en Veiligheid. De financiële gevolgen van de implementatie van de CER- en NIS2-richtlijn worden de komende tijd nader in kaart gebracht, waaronder ook voor de zorgsector.

Ik zal uw Kamer volgend jaar informeren over de voortgang van mijn beleid inzake het robuuster maken van de fysieke en digitale weerbaarheid van de zorgsector.

Met de omzetting van de CER- en NIS2-richtlijn in nationale wetgeving zullen voor de nog nader aan te wijzen bedrijven en organisaties binnen bepaalde sectoren, waaronder de zorg, verplichtingen gaan gelden. Hierover zal voor zorgpartijen informatie beschikbaar komen op www.gegevensuitwisselingindezorg.nl/weerbaarheid.

De Minister van Volksgezondheid, Welzijn en Sport,
E.J. Kuipers