RAPPORT

Onderzoek naar de prioriteitstelling en aansluitbaarheid van zorgsectoren bij Z-CERT

Dit rapport sluit aan bij het 4B-informatiebeveiligingsbeleid:

Bewust worden, beschermen, bewaken en blussen.

Uitgevoerd door:
ICTU samen met Z-CERT

In opdracht van:
Ministerie van Volksgezondheid, Welzijn en Sport (VWS)

Datum:
December 2020

Voorwoord

Eén ding dat de coronacrisis ons in 2020 heeft geleerd, is dat de zorgsector maatschappelijk cruciaal is. In de hitte van de crisis leek het er even op dat de zorgcapaciteit in Nederland onvoldoende zou zijn. De maatschappelijke gevolgen van de crisis waren überhaupt al ernstig, maar zouden zonder voldoende zorgcapaciteit nog ernstiger zijn geweest. Nóg veel ernstiger zou het geweest zijn als tijdens de crisis zorginstellingen digitaal gesaboteerd zouden worden. Dan zou de al beperkte zorgcapaciteit nog verder verminderen. Gelukkig is het niet zover gekomen.

Toch hangt de mogelijkheid van digitale sabotage van zorginstellingen als 'het zwaard van Damocles' boven de zorgsector. Slachtoffer worden van een ransomware aanval (zoals de Universiteit van Maastricht in 2019 overkwam) kan ervoor zorgen dat ook bij zorginstellingen digitale systemen onbruikbaar worden. Met of zonder crisis, we kunnen het ons niet permitteren dat patiëntveiligheid in gevaar komt door cyberproblemen en/of ICT-storingen.

Daarom benadruk ik graag het belang van Z-CERT. Als informatie- en coördinatiecentrum voor digitale veiligheid kan het cyberdreigingen in kaart brengen en zorginstellingen ondersteunen bij het verbeteren van hun digitale veiligheid. Niet alle zorginstellingen kunnen al ten volle gebruikmaken van de diensten van Z-CERT. Zorginstellingen dienen eerst tijd te krijgen hun digitale veiligheid optimaal op orde te brengen. Intussen groeit Z-CERT in de rol die zij toebedeeld heeft gekregen.

Een beheerste groei van Z-CERT is daarom gebaat bij een gefaseerde aansluitstrategie. Ik kan me daarom ook goed vinden in de resultaten van dit onderzoek naar deze strategie. Het is mooi om te zien dat de onderzoekers nauw hebben samengewerkt met het werkveld om te bepalen welke groepen zorginstellingen voorrang zouden moeten krijgen bij het aansluiten op Z-CERT. En ook voor wie nog ruimte nodig is om eerst hun digitale veiligheid verder op orde te brengen.

Dr. Marcel Spruit, Lector Cybersecurity Haagse Hogeschool

INHOUDSOPGAVE

SAMENVATTING

DOELSTELLING VAN DE OPDRACHT

Dit rapport bevat de uitkomsten van een onderzoek gedaan door ICTU in samenwerking met Z-CERT in opdracht van het ministerie van Volksgezondheid Welzijn en Sport (VWS) naar de prioriteitstelling en volgorde waarmee zorgsectoren beheerst kunnen aansluiten bij Z-CERT. De opdracht komt mede voort uit de motie Ellemeet en Kamervragen[1] inzake het aansluiten van alle zorginstellingen op Z-CERT. Het rapport geeft ook aanbevelingen voor een nadere invulling van het reeds in gang gezette "4B- informatiebeveiligingsbeleid" van VWS (bewust worden, beschermen, bewaken en blussen). Het rapport is primair bedoeld voor beleidsmakers bij VWS en koepel- en brancheorganisaties in de zorg.

Voor de invulling van de opdracht hebben we gekozen voor een risico-gebaseerde aanpak en het maken van een business impact analyse (BIA). We hebben enerzijds gekeken naar de mate van impact die cyberdreigingen kunnen hebben op de bedrijfsvoering van de zorginstellingen in specifieke sectoren. Anderzijds naar in hoeverre de zorginstellingen in staat zijn om direct bij Z-CERT aan te sluiten.

De analyse is een momentopname en het is nodig om deze periodiek te evalueren en waar nodig bij te stellen. Zodat de volgorde van aansluiten, indien nodig, aangepast kan worden.

AANDACHT NODIG VOOR CYBERCRIME IN DE ZORG

Medische informatiesystemen zijn vandaag de dag niet meer weg te denken uit zorginstellingen. Naast de vele kansen en mogelijkheden die deze systemen bieden, loopt de zorgsector steeds meer risico op het gebied van informatiebeveiliging en cybersecurity. Dreigingen van statelijke actoren en cybercriminelen hebben inmiddels een permanent karakter gekregen en richten zich onder andere op zorginstellingen. Omdat er steeds meer digitale systemen beschikbaar komen en een groeiende afhankelijkheid van technologie en informatievoorziening bestaat, hebben cyberaanvallers ook meer om aan te vallen; er is een groter digitaal aanvalsoppervlak ontstaan. Kortom, er is voldoende aandacht nodig voor het terugdringen van het effect van cyberrisico's en het weerbaarder maken van de zorgsector.

Z-CERT ALS EXPERTISECENTRUM VOOR DE ZORG

Om zorginstellingen op dit gebied te ondersteunen en van advies te voorzien is in 2018 Z-CERT opgericht. Inmiddels zijn vrijwel alle ziekenhuizen en bijna alle GGZ-instellingen op Z-CERT aangesloten. Het streven van Z-CERT is om het aantal zorginstellingen gefaseerd aan te laten sluiten en om de dienstverlening uit te breiden naar de hele zorgsector.

IMPACTANALYSE CYBERDREIGINGEN OP DE BEDRIJFSVOERING

De volgende zorgsectoren zijn meegenomen in de scope van dit onderzoek:

- Ambulancezorg.
- Farmaceutische zorg.
- Geboortezorg.
- Gehandicaptenzorg.
- Huisartsenzorg.
- Jeugdzorg.
- Paramedische zorg.
- Publieke gezondheid.

1 www.tweedekamer.nl/kamerstukken/detail?id=2019Z03467&did=2019D07420 (motie Ellemeet verplichte deelname Z-CERT)

- Revalidatiezorg.
- Tandheelkundige zorg.
- Verpleging, verzorging en thuiszorg.

Voor iedere sector is een risicoprofiel opgesteld en een BIA uitgevoerd. Die zijn vervolgens gevalideerd bij de desbetreffende achterban.

Bij vijf sectoren is gebleken dat ICT falen door cyberincidenten een relatief hoge impact heeft op de beschikbaarheid, integriteit en vertrouwelijkheid van de informatievoorziening en hiermee op de continuïteit van de zorgverlening. Deze vijf sectoren kennen daarmee een hogere prioriteit om aangesloten te worden bij Z-CERT. Dit zijn, in willekeurige volgorde:

A. Jeugdzorg (gecertificeerde jeugdzorginstellingen).
B. Publieke gezondheidszorg (Gemeentelijke Gezondheidsdiensten en GHOR).
C. Huisartsenzorg (huisartsenposten en huisartspraktijken).
D. Farmaceutische zorg (apotheken).
E. Ambulancezorg (ambulancediensten).

MATE VAN AANSLUITBAARHEID

Om vervolgens te kunnen beoordelen in hoeverre zorginstellingen uit de verschillende sectoren in staat zijn om direct bij Z-CERT aan te sluiten, hebben we gekeken naar de onderstaande criteria:

- Aansluitvermogen: de mate waarin kennis en capaciteit aanwezig is om met de producten en diensten van Z-CERT aan de slag te gaan.
- Bereidheid: de mate waarin de organisatie de meerwaarde ziet van de dienstverlening van Z-CERT en daarvoor bestuurlijk commitment en de financiële middelen beschikbaar wil stellen.
- Uitbesteding: de mate van uitbesteding van IT-diensten aan leveranciers en de afhankelijkheid daarvan en de mate van aandacht bij zorginstellingen voor cybersecurity.

Uit de analyse blijkt dat grotere zorginstellingen vaak zodanig zijn georganiseerd dat de kans groter is dat ze kunnen voldoen aan de aansluitcriteria van Z-CERT. Zij kunnen direct aangesloten worden bij Z-CERT, rekening houdend met de geprioriteerde volgorde en de dienstverleningscapaciteit van Z-CERT.

Voor kleinere zorginstellingen ligt dit anders. Huisartsenpraktijken en apotheken bijvoorbeeld zijn vanwege hun omvang en organisatiegraad niet rechtstreeks aan te sluiten op Z-CERT. Hiervoor dient Z-CERT samen met VWS en relevante organisaties een alternatieve aanpak te onderzoeken en te ontwikkelen.

AANBEVELINGEN INFORMATIEBEVEILINGSBELEID VWS

Aanvullend op ons advies met betrekking tot de prioriteitstelling en aansluitvolgorde geven we aanbevelingen mee voor het verder invullen van het reeds in gang gezette “4B-informatiebeveiligingsbeleid”. Deze zijn gericht op VWS, Z-CERT, het zorgveld en patiënten/zorgconsumenten. Centraal hierin staan kennisdeling en samenwerking, doorontwikkeling van het instrument van de risico-gestuurde aanpak en monitoring van de zorgsector in relatie tot cybersecurity risico’s en de aansluiting op Z-CERT.

Hoofstuk 1 Opdrachtformulering

Dit rapport bevat de uitkomsten van een onderzoek gedaan door ICTU in samenwerking met Z-CERT in opdracht van het ministerie van Volksgezondheid, Welzijn en Sport (VWS) naar de prioriteitstelling en volgorde waarmee zorgsectoren beheerst kunnen aansluiten bij Z-CERT. Het rapport is primair bedoeld voor beleidsmakers bij VWS en koepel- en brancheorganisaties in de zorg.

Na het lezen van dit hoofdstuk bent u op de hoogte van:

- De context van de opdracht.
- De doelstelling en scope van de opdracht.
- De gevolgde aanpak.
- De uitgevoerde werkzaamheden.

1.1 CONTEXT VAN DE OPDRACHT

1.1.1 Digitale dreiging neemt toe in de zorgsector

Medische informatiesystemen zijn vandaag de dag niet meer weg te denken uit zorginstellingen. Technologische ontwikkelingen volgen elkaar in rap tempo op en bieden steeds meer mogelijkheden. Voorbeelden hiervan zijn:

- Breder gebruik van elektronische cliënt- of patiëntdossiers (ECD of EPD).
- Intensievere uitwisseling van medische gegevens in de keten.
- Toenemende inzet van eHealth- en domoticatoepassingen.
- Toenemend gebruik van medische apparatuur en *wearables*/sensoren voor diagnose en behandeling.
- Toenemende inzet van mogelijkheden voor data-analyse en artificiële intelligentie.

Naast de vele kansen en mogelijkheden die de inzet van medische informatiesystemen biedt, loopt de sector steeds meer risico op het gebied van informatiebeveiliging en cybersecurity. In het meest recente Cybersecuritybeeld Nederland (CSBN2020)[2] van het Nationaal Cyber Security Centrum (NCSC) wordt geconstateerd dat de digitale dreiging de afgelopen jaren onverminderd is toegenomen. Dreigingen van statelijke actoren en cybercriminelen hebben inmiddels een permanent karakter gekregen en richten zich onder andere op zorginstellingen. Sinds de start van de COVID-19 pandemie zijn er aanwijzingen dat actoren de situatie misbruiken om gerichte cyberaanvallen uit te voeren op bijvoorbeeld ziekenhuizen, farmaceuten, onderzoekscentra en fabrikanten van medische IT of medische hulpmiddelen. Om Nederlandse organisaties gedurende de COVID-19 pandemie bij digitale dreigingen en incidenten zo goed mogelijk bij te staan, is onlangs een tijdelijke spoedwet tot stand gebracht[3].

Omdat er steeds meer digitale systemen beschikbaar komen en een groeiende afhankelijkheid van technologie en informatievoorziening bestaat, hebben cyberaanvallers meer om aan te vallen; er is een groter digitaal aanvalsoppervlak ontstaan. Kwaadwillenden maken hier dankbaar gebruik van. Dit speelt niet alleen bij de zorginstellingen zelf, maar ook bij alle toeleveranciers (de zogenaamde *supplychain*).

Cyberdreigingen en -aanvallen hebben directe impact op de fysieke wereld. Ze kunnen het werk van zorgmedewerkers belemmeren en de zorg aan patiënten in gevaar brengen.

2 Cybersecuritybeeld Nederland 2020 (CSBN 2020), zoals vastgesteld door de NCTV op 29 juni 2020

3 Tweede Verzamelspoedwet Covid-19 - Memorie van toelichting, nummer 35 497

Hierbij valt te denken aan het lekken van vertrouwelijke (patiënten)informatie of het verstrekken van verkeerde medicatie door onjuiste of niet beschikbare dossiers. Ook kunnen ze schade toebrengen aan het imago en de financiële positie van zorginstellingen.

Kortom, er is voldoende aandacht nodig voor het terugdringen van het effect van cyberrisico's en het weerbaarder maken van de zorgsector.

1.1.2 Z-CERT – cybersecuritycentrum voor de Nederlandse zorgsector

Om zorginstellingen op dit gebied te ondersteunen en van advies te voorzien is in 2018 Z-CERT opgericht. Dit is een Computer Emergency Response Team (CERT) voor de Nederlandse zorgsector, dat (financieel) ondersteund wordt door VWS. Z-CERT is onafhankelijk en verzamelt en analyseert informatie over cybersecurity en deelt de uitkomsten met de deelnemende zorginstellingen.

Inmiddels zijn vrijwel alle ziekenhuizen en bijna alle GGZ-instellingen op Z-CERT aangesloten. Begin 2021 komen daar nog meer GGZ-instellingen bij. Het streven van Z-CERT is om het aantal zorginstellingen gefaseerd aan te laten sluiten en om de dienstverlening uit te breiden naar de hele zorgsector.

Mede naar aanleiding van een aantal incidenten (datalekken) zijn de afgelopen periode verschillende vragen door de Tweede Kamer gesteld over (verplichte) deelname aan Z-CERT[4]. VWS heeft naar aanleiding hiervan opdracht gegeven aan ICTU om samen met Z-CERT te inventariseren met welke volgorde en prioriteit zorgsectoren beheerst bij Z-CERT kunnen worden aangesloten.

1.2 DOELSTELLING EN SCOPE VAN DE OPDRACHT

1.2.1 Doelstelling van de opdracht

ICTU en Z-CERT hebben de volgende specifieke taak op zich genomen:

"Voer een globale risicoanalyse uit met als resultaat een risicoprofiel per zorgsector. Dit profiel omvat zowel een visuele weergave van de risico's per zorgsector als een tekstuele onderbouwing hiervan in termen van beschikbaarheid, integriteit en vertrouwelijkheid[5]. Het resultaat dient hierbij de volgende doelen:

1. *Input geven om te komen tot een weloverwogen strategie met welke volgorde en prioriteit de verschillende type zorgaanbieders bij Z-CERT kunnen worden aangesloten (en hiermee input te geven voor de verschillende moties).*
2. *Input geven voor de beleidsvorming door het ministerie van VWS passend bij het gehanteerde 4B beleid (bewustwording, beschermen, bewaken en blussen)."*

4 Voorbeelden moties en kamerbrieven:
www.tweedekamer.nl/kamerstukken/detail?id=2019Z03467&did=2019D07420 (motie Ellemeet verplichte deelname Z-CERT)
www.parlementairemonitor.nl/9353000/1/j9vvij5epmj1ey0/vkznqnrue7zr (motie Raijmakers aansluiten jeugdzorg op Z-CERT)
www.rijksoverheid.nl/documenten/kamerstukken/2019/10/08/kamerbrief-over-informatieveiligheid-en-privacy-in-de-zorg

5 Beschikbaarheid, integriteit en vertrouwelijkheid zijn gangbare termen binnen het vakgebied cybersecurity en informatiebeveiliging

1.2.2 Scope van de opdracht

De Nederlandse gezondheidszorg is op verschillende manieren in te delen. Voor deze opdracht hanteren we de onderverdeling in tweedelijns- en eerstelijnszorg, zie hieronder.

Tweedelijnszorg

- Ziekenhuiszorg (ziekenhuizen):
  - Universitair.
  - Topklinisch.
  - Algemeen.
  - Private klinieken en gespecialiseerde centra.
- Revalidatiezorg (revalidatiecentra).
- Geestelijke gezondheidszorg (GGZ).
- Jeugdzorg (jeugdzorginstellingen):
  - Jeugdbescherming en Jeugdreclassering.
  - Jeugdhulp en pleegzorg.
- Publieke gezondheidszorg (GGD-instellingen) en de Geneeskundige Hulpverleningsorganisatie in de Regio (GHOR).
- Verpleging en verzorging (verpleeg- en verzorgingshuizen) en thuiszorg (thuiszorginstellingen), samengevoegd tot VVT.
- Gehandicaptenzorg (gehandicaptenzorg instellingen).
- Ambulancezorg (ambulancediensten).

Eerstelijnszorg

- (Spoedeisende) huisartsenzorg (huisartsenpraktijken en huisartsenposten).
- (Spoedeisende) farmaceutische zorg (openbare apotheken en dienstapotheken), exclusief fabrikanten en groothandels.
- Tandzorg (tandartspraktijken).
- Geboortezorg (praktijken voor kraamzorg en kraamverpleging).
- Paramedische zorg (praktijken voor fysiotherapie, logopedie, ergotherapie, podotherapie, etc.).

De ziekenhuizen (met uitzondering van de klinieken en gespecialiseerde centra zoals voor dialyse en radiotherapie) en GGZ- instellingen vallen buiten de scope van de opdracht omdat zij al zijn aangesloten bij Z-CERT of binnenkort worden aangesloten.

Binnen de scope van de opdracht hoort het maken van een business impact analyse (BIA) op basis waarvan de risicoprofielen zijn vastgesteld. Het inschatten van kwetsbaarheden en de kans op dreigingen en de impact daarvan maken geen onderdeel van deze opdracht. Ook het selecteren en realiseren van mitigerende maatregelen valt buiten de scope. Wel doen we in hoofdstuk 5 aanbevelingen voor vervolgactiviteiten die aansluiten bij het informatiebeveiligingsbeleid van VWS.

1.2.3 Aanpak van de opdracht en leeswijzer

Op basis van het doel en de scope van de opdracht hebben we een BIA uitgevoerd. Per zorgsector en per groep van (medische) informatiesystemen hebben we op basis van deskresearch en aanwezige kennis een risicoprofiel opgesteld en de impact geïnventariseerd. Het gaat hierbij om het niet-beschikbaar of niet-integer zijn van de informatie die met de systemen wordt verwerkt en/of het niet vertrouwelijk verwerken ervan. De profielen zijn vervolgens gevalideerd bij de desbetreffende achterban. De BIA is een eerste stap in de risicomanagementmethode IRAM2. Een nadere toelichting op deze methode staat in bijlage A. De risicoprofielen staan in bijlage B. De resultaten van de analyse leest u in hoofdstuk 2 en bijlage C.

De uitkomsten van het onderzoek naar in hoeverre zorginstellingen uit de verschillende sectoren in staat zijn om direct bij Z-CERT aan te sluiten (aansluitbaarheid) vindt u in hoofdstuk 3. Ook de criteria die we hiervoor hebben gehanteerd, leest u daarin terug.

In hoofdstuk 4 staat de conclusie van ons onderzoek in de vorm van een globale aansluitstrategie.

Tot slot doen we in hoofdstuk 5 aanbevelingen voor vervolgactiviteiten die aansluiten bij het informatiebeveiligingsbeleid van VWS.

In bijlage D vindt u een visualisatie van het speelveld zorg in relatie tot de aansluitbaarheid bij Z-CERT.

Bijlage E bevat achtergrondinformatie over cybersecurity in Nederland voor wie zich meer wil verdiepen in de context van aansluiten bij Z-CERT.

Onze bevindingen hebben we inhoudelijk afgestemd met vertegenwoordigers van koepelorganisaties en zorginstellingen. Wij zijn hen zeer erkentelijk voor hun bijdrage! Hieronder vindt u een overzicht van alle betrokken organisaties:

- Actiz.
- Ambulancezorg Nederland (AZN).
- CMIO Netwerk Eerste Lijn.
- GGD GHOR Nederland.
- InEen.
- Jeugdzorg Nederland.
- Koninklijk Nederlands Genootschap voor Fysiotherapie (KNGF).
- Koninklijke Nederlandse Maatschappij ter bevordering der Pharmacie.
- Koninklijke Nederlandse Organisatie van Verloskundigen.
- Landelijke Huisartsen Vereniging (LHV).
- NedAIS.
- Nederlands Huisartsen Genootschap (NHG).
- Revalidatie Nederland.
- Stichting Portaal Patiëntveiligheid.
- Vereniging Gehandicaptenzorg Nederland (VGN).
- Zorgthuisnl.

1.2.4 Contact

Voor inhoudelijke vragen of opmerkingen kunt u contact opnemen met André den Breejen (projectleider bij ICTU) via Andre.denBreejen@ictu.nl.

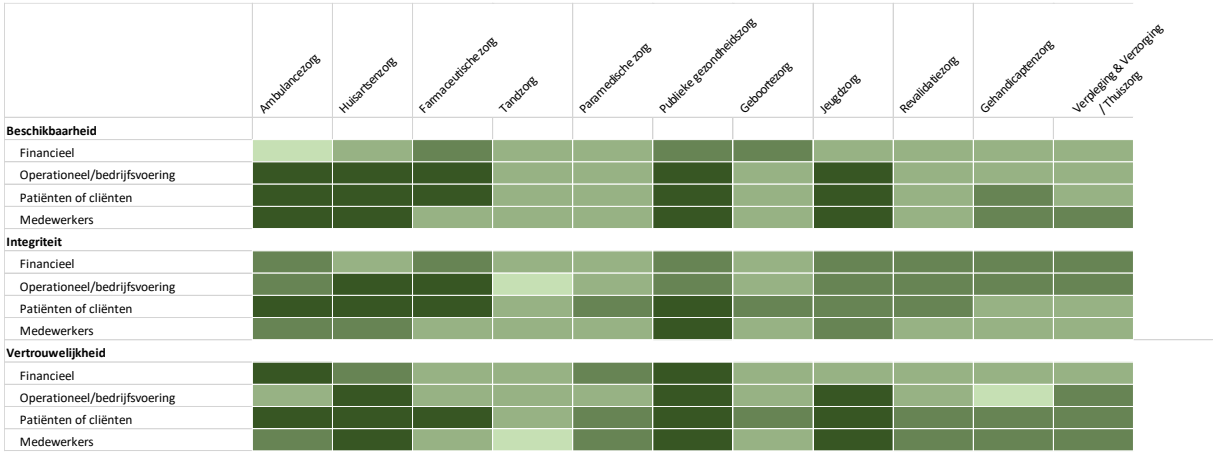
Hoewel de auteurs van dit rapport rekening hebben gehouden met de digitale toegankelijkheid van dit document, zijn niet alle tabellen en grafieken digitoegankelijk gemaakt. Heeft u hier vragen over, neem dan ook contact op met André den Breejen.

Hoofdstuk 2 Impactanalyse zorgsectoren

In dit hoofdstuk worden de resultaten van de BIA gedeeld en toegelicht. We hebben gekozen voor een visuele weergave hiervan in de vorm van een *heatmap*. Hiermee ziet u in één oogopslag de impact: hoe donkerder de kleur, hoe hoger de impact. Per kwaliteitsaspect (beschikbaarheid, integriteit, vertrouwelijkheid) en daarbinnen per onderwerp (financieel, operationeel/bedrijfsvoering, patiënten/cliënten, medewerkers) is de maximale waarde opgenomen (mogelijke scores waren een, twee, drie of vier).

Volledigheidshalve wordt opgemerkt dat de impact niets zegt over de mate waarin deze sectoren aan kunnen sluiten bij de huidige organisatie en dienstverlening van Z-CERT. Ook zegt het niets over de behoefte die ze hebben aan de dienstverlening van Z-CERT. Tenslotte is het goed om te beseffen dat het karakter van de zorg per instelling verschilt en dat de relevantie van de informatievoorziening daarmee samenhangt.

De heatmap vindt u hieronder. Meer informatie over de resultaten van de BIA per sector staat in bijlage C.



Figuur 1: Decoratieve afbeelding heatmap zorgsectoren

2.1 SECTOREN MET EEN HOGERE IMPACT

Uit de heatmap blijkt dat vijf sectoren een relatief hoge impact kennen op de beschikbaarheid, integriteit en vertrouwelijkheid van de informatievoorziening en hiermee samenhangend op de continuïteit van de zorgverlening. Deze vijf sectoren kennen daarmee een hogere prioriteit om aangesloten te worden bij Z-CERT. Dit zijn, in willekeurige volgorde:

A. Jeugdzorg (gecertificeerde jeugdzorginstellingen).
B. Publieke gezondheidszorg (Gemeentelijke Gezondheidsdiensten en GHOR).
C. Huisartsenzorg (huisartsenposten en huisartspraktijken).
D. Farmaceutische zorg (apotheken).
E. Ambulancezorg (ambulancediensten).

Hieronder staat per sector een samenvattende toelichting op de resultaten van de impactanalyse.

A. Jeugdzorg

- Uit de BIA blijkt dat er voor jeugdzorginstellingen (en bovenal voor gecertificeerde instellingen die jeugdbescherming en jeugdreclassering leveren) sprake is van een

zeer hoge impact op het imago, de continuïteit, de financiën van de instellingen en voorts op de kwaliteit van de zorg en veiligheid van cliënten en medewerkers van de instelling.
- Jeugdzorginstellingen leveren zorg aan een (zeer) kwetsbare doelgroep. Vanwege de aard van de zorg wordt (zeer) privacygevoelige informatie van kinderen en hun directe leefomgeving verwerkt. Voor gecertificeerde instellingen geldt bovendien dat deze privacygevoelige informatie ook wordt uitgewisseld in de veiligheidsketen[6]. Juist vanwege dit privacygevoelige karakter van de informatie krijgen incidenten, zoals datalekken, vaak landelijke (media)aandacht.
- De informatie die door de (grotere) instellingen wordt gebruikt is (vrijwel) volledig gedigitaliseerd, waardoor een directe afhankelijkheid bestaat naar de beschikbaarheid van de zorgsystemen. Voor gecertificeerde instellingen geldt dat de informatie in een landelijk systeem wordt verwerkt en uitval van dit systeem heeft een grote impact op deze instellingen.

B. Publieke gezondheidszorg

- Uit de BIA komt naar voren dat voor de GGD'en, en met name de afdelingen Jeugdgezondheidszorg, Infectieziektebestrijding, Openbare GGZ en de GHOR, sprake is van een (zeer) hoge impact op het imago, de continuïteit en de financiën van de instelling. Daarnaast is er sprake van hoge impact op de betrouwbaarheid van de zorgverlening en het moraal/vertrouwen van cliënten en medewerkers van de instelling.
- Met het uitbreken van COVID-19 en de daaraan gekoppelde landelijk afgekondigde maatregelen is een grote druk ontstaan op de GGD'en. Voor het aanvragen, plannen en uitvoeren van testen (inclusief het beschikbaar stellen van de uitslag) wordt veel samengewerkt met private partijen en vrijwilligers op regionaal en landelijk niveau. Hetzelfde geldt voor bron- en contactonderzoek. Binnen Infectieziektebestrijding (waarbij COVID-19 zeer actueel is) wordt voor grote groepen Nederlanders privacygevoelige informatie verwerkt en met publieke en private organisaties uitgewisseld. De informatie is volledig gedigitaliseerd waarbij gebruik wordt gemaakt van lokale en landelijke systemen. Uitval hiervan heeft niet alleen een zeer grote impact op de afdeling, maar ook op de werkprocessen rondom testen en bron- en contactonderzoek.
- Binnen Jeugdgezondheidszorg en de Openbare GGZ is sprake van kwetsbare doelgroepen, met veelal sociaal- maatschappelijke en financiële problematiek. Daar wordt (zeer) privacygevoelige informatie verwerkt, al dan niet met ketenpartners. Ook hier geldt dat door het privacygevoelige karakter van de informatie, incidenten landelijke (media)aandacht trekken.
- Voor de GHOR geldt dat, ten tijde van rampen en crisissen, een directe afhankelijkheid bestaat naar de beschikbaarheid van systemen om tussen de betrokken partijen (waaronder gemeenten, ziekenhuizen, brandweer, politie en ambulancediensten) informatie uit te wisselen.

C. (Spoedeisende) huisartsenzorg

- Uit de BIA komt naar voren dat voor huisartspraktijken en -posten sprake is van een (zeer) hoge impact op het imago, de continuïteit en financiën van de instelling en daarnaast op de kwaliteit en veiligheid voor patiënten en medewerkers van de praktijken en posten.

6 In 2007 is de invoer van netwerksamenwerking (kenmerken: (parallel, informatie gemeenschappelijk delen, het kind centraal stellen) aanbevolen in een verkenning van de mogelijkheden voor de toepassing van e-overheid rond 'Het Kind Centraal" (opdrachtgever Directie Innovatie en Informatiebeleid Openbare Sector, BZK).

- Huisartsen leveren zorg voor een breed en gevarieerd spectrum aan klachten. Vanwege de aard van de huisartsenzorg wordt (zeer) privacygevoelige informatie verwerkt. Bovendien geldt dat informatie wordt uitgewisseld in verschillende ketens waaronder met ziekenhuizen en veel verschillende zorgaanbieders in de 1e en 2e lijn.
- De informatie die wordt verwerkt is (vrijwel) volledig gedigitaliseerd. De belangrijkste systemen die worden gebruikt zijn huisartsinformatiesystemen, huisartsenpost-informatiesystemen en keteninformatiesystemen. Afhankelijkheid van het functioneren van deze systemen is hoog.

D. Farmaceutische zorg

- Uit de BIA komt naar voren dat voor apotheken sprake is van een (mogelijk zeer) hoge impact op patiëntveiligheid en medicatieveiligheid alsook op de continuïteit en financiën.
- De apotheken leveren zorg aan alle Nederlanders waarbij medicatievoorschriften herleidbaar zijn tot soms (zeer) privacygevoelige informatie. Bovendien geldt dat informatie wordt uitgewisseld in verschillende ketens (met name, maar niet alleen, met de huisartsen).
- De informatie die wordt verwerkt is (vrijwel) volledig gedigitaliseerd. De belangrijkste systemen die worden gebruikt zijn apotheekinformatiesystemen (inclusief elektronisch voorschrijven). Uitval van deze systemen heeft een grote impact op zowel de logistieke processen van de apotheken als de farmaceutische zorgverlening (medicatieveiligheid).

E. Ambulancezorg

- Uit de BIA komt naar voren dat voor ambulancediensten sprake is van een (zeer) hoge impact op het imago, de continuïteit en financiën van de instelling. En daarnaast op de kwaliteit en veiligheid voor patiënten en medewerkers die aanwezig zijn op de ambulance.
- Ambulancediensten zijn direct afhankelijk van de beschikbaarheid van de communicatiesystemen die op de meldkamers worden gebruikt zoals 112, C2000 en het Geïntegreerd Meldkamer Systeem (GMS). Deze systemen worden beheerd door de Nationale Politie, maken onderdeel uit van de vitale infrastructuur en vallen hierdoor onder het NCSC. Er bestaat een directe afhankelijkheid naar het landelijke systeem dat zorgdraagt voor de doorgifte van gegevens van meldkamer naar voertuigen. Dit systeem wordt beheerd via de koepelorganisatie.
- De informatie die door de ambulancediensten wordt verwerkt, is voor wat betreft de logistieke aansturing van de ambulance volledig gedigitaliseerd. Het verwerken van patiëntinformatie op de ambulance en het uitwisselen hiervan met de spoedeisende hulp wordt grotendeels gedigitaliseerd (EPD). Uitval van deze systemen heeft een grote impact op zowel de logistieke processen van de ambulancezorg als de zorgverlening (de ambulance kan bijvoorbeeld niet of niet tijdig op de juiste bestemming komen).

2.2 SECTOREN MET EEN LAGERE IMPACT

Uit de heatmap kan worden opgemaakt dat cyberincidenten op onderstaande sectoren een lagere impact hebben dan de sectoren die hiervoor aan de orde zijn gekomen:

- Revalidatiezorg.
- Verpleging & verzorging en Thuiszorg (VVT).
- Gehandicaptenzorg.
- Paramedische zorg.

- Kraamzorg.
- Tandzorg.

De belangrijkste kenmerken van zorginstellingen in deze sectoren zijn:

- Zorgaanbieders zijn in mindere mate afhankelijk van de beschikbaarheid van digitale informatiesystemen om zorg te kunnen leveren en informatie wordt veelal in een 'kleinere' keten gedeeld.
- De informatie die door zorgaanbieders wordt verwerkt, kent veelal een 'beperkte' scope (informatie heeft bijvoorbeeld alleen betrekking op één specifiek lichaamsonderdeel of één klachtbeeld).
- De informatie is minder bijzonder privacygevoelig ten opzichte van de overige in beeld gebrachte sectoren.

Hoofdstuk 3 Aansluitbaarheid zorgsectoren

Dit hoofdstuk beschrijft kort de dienstverlening van Z-CERT en de factoren die van invloed zijn om een zorgsector hierop aan te kunnen sluiten. Vervolgens geven we inzicht in welke zorginstellingen uit de verschillende sectoren in staat zijn om direct of op een later moment bij Z-CERT aan te sluiten.

3.1 DIENSTVERLENING Z-CERT

Z-CERT is in 2018 opgericht als onafhankelijke stichting om zorginstellingen te ondersteunen en van advies te voorzien op het gebied van cybersecurity. Het is een Computer Emergency Response Team (CERT) voor de Nederlandse zorgsector dat (financieel) ondersteund wordt door VWS.

Z-CERT is gestart met het leveren van basis CERT-diensten aan ziekenhuizen en GGZ-instellingen. Inmiddels zijn vrijwel alle ziekenhuizen en bijna alle GGZ-instellingen op Z-CERT aangesloten. Begin 2021 komen daar nog meer GGZ-instellingen bij. Het streven van Z-CERT is om het aantal zorginstellingen gefaseerd aan te laten sluiten en om de dienstverlening uit te breiden naar de hele zorgsector.

Op dit moment biedt Z-CERT de volgende producten en diensten:

- Z-CERT en verzamelt en analyseert informatie over cybersecurity. De uitkomsten deelt Z-CERT met de deelnemende zorginstellingen via actuele berichtgeving en verdiepende publicaties.
- Als een instelling wordt getroffen door een cyberincident of als Z-CERT constateert dat het IP- adres van een instelling op ‘blacklists’ voorkomt, dan biedt Z-CERT advies en technische ondersteuning over het oplossen van het probleem om de schade zoveel mogelijk te beperken.
- Z-CERT kan mogelijke kwetsbaarheden afhandelen die in systemen van instellingen door derden worden ontdekt.
- Security professionals kunnen informatie over cybersecurity uitwisselen op het besloten online platform van Z-CERT.
- Indien sprake is van dreigingen, incidenten of kwetsbaarheden die sector-overstijgend zijn, dan heeft Z-CERT de rol van regievoerder en coördineert ze de informatievoorziening naar zorginstellingen. Dit in overleg en afstemming met haar partners zoals het NCSC, VWS en andere CERT’s.
- Het kan voorkomen dat Z-CERT informatie over kwetsbaarheden bij een niet-deelnemende zorginstelling ontdekt of daarop wordt geattendeerd. Z-CERT neemt contact op met de betreffende instelling en biedt advies en ondersteuning om gevolgschade zoveel mogelijk te beperken.
- Een recent voorbeeld van een nieuwe dienst is het ZorgDetectieNetwerk (ZDN). Hiermee wordt dreigingsinformatie uitgewisseld.

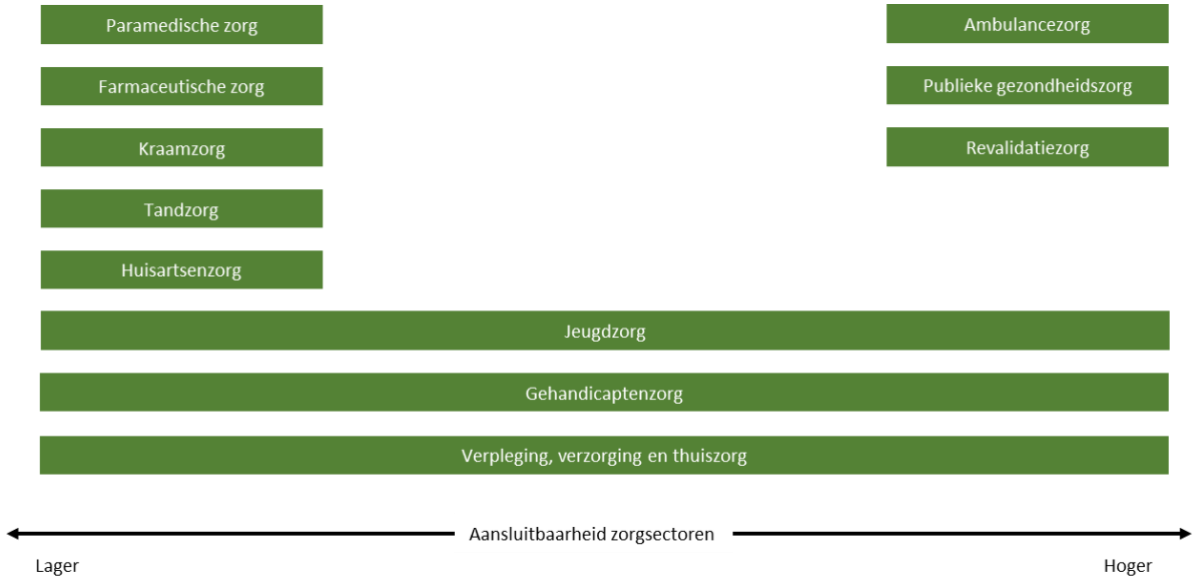
3.2 AANSLUITBAARHEID BIJ Z-CERT

De huidige dienstverlening van Z-CERT is gebaseerd op de behoeften van ziekenhuizen en GGZ- instellingen. Om te kunnen bepalen in hoeverre zorginstellingen uit de andere sectoren in staat zijn om direct bij Z-CERT aan te sluiten, hebben we gekeken naar de onderstaande criteria:

- Aansluitvermogen: de mate waarin bij een organisatie kennis en capaciteit aanwezig is om met de producten en diensten van Z-CERT aan de slag te gaan.

- Bereidheid: de mate waarin de organisatie de directe meerwaarde ziet van de dienstverlening van Z-CERT en daarvoor bestuurlijk commitment en de financiële middelen beschikbaar wil stellen.
- Uitbesteding: de mate van uitbesteding van IT-diensten aan leveranciers en de afhankelijkheid daarvan en de mate van aandacht bij zorginstellingen voor cybersecurity.

De uitkomsten van dit onderzoek staan in onderstaande figuur.



Figuur 2: Aansluitbaarheid zorgsectoren bij huidige organisatie en dienstverlening Z-CERT.

Figuur 2 geeft drie categorieën weer met betrekking tot de mate van aansluitbaarheid:

- Categorie 1: Sectoren die een grote variatie kennen in lage en hoge aansluitbaarheid:
  - Jeugdzorg.
  - Gehandicaptenzorg.
  - Verpleging, verzorging en thuiszorg.
- Categorie 2: Sectoren met een lagere aansluitbaarheid:
  - Paramedische zorg.
  - Farmaceutische zorg.
  - Kraamzorg.
  - Tandzorg.
  - Huisartsenzorg.
- Categorie 3: Sectoren met een hogere aansluitbaarheid:
  - Ambulancezorg.
  - Publieke gezondheidszorg.
  - Revalidatiezorg.

Uit de bijbehorende analyse blijkt dat grotere zorginstellingen vaak zodanig zijn georganiseerd dat de kans groter is dat ze kunnen voldoen aan de aansluitcriteria van Z-CERT. Zij zouden direct aangesloten kunnen worden, rekening houdend met de geprioriteerde volgorde en de dienstverleningscapaciteit van Z-CERT.

Voor kleinere zorginstellingen ligt dit anders. Huisartsenpraktijken en apotheken bijvoorbeeld zijn vanwege hun omvang en organisatiegraad niet rechtstreeks aan te sluiten. Beredeneerd vanuit de criteria kan in het algemeen worden gesteld dat kleinere instellingen veelal:

- Over minder financiële middelen beschikken om de vergoeding te kunnen betalen of geen direct meerwaarde in de dienstverlening van Z-CERT zien.
- Geen aparte IT- afdeling of aparte functionaris hebben die verantwoordelijk is voor informatiebeveiliging en/of cybersecurity.
- IT en/of IT-security hebben uitbesteed en leunen op de IT-leverancier(s).
- Geen behoefte hebben aan technische dienstverlening maar aan concrete en praktisch toepasbare informatie.

Daarom dient mede samen met Z-CERT een alternatieve aanpak onderzocht en ontwikkeld te worden. Deze is gericht op het vergroten van de aansluitbaarheid van kleinere zorgaanbieders met een hoge impact en het daarmee samenhangende risico op uitval van de zorgverlening.

Hoofdstuk 4 Globale aansluitstrategie

Dit hoofdstuk bevat de optelsom van de impactanalyse en de aansluitbaarheid in de vorm van een globale aansluitstrategie. Hierbij gaat het niet alleen om prioritering op basis van risico's, maar ook om wat haalbaar is voor Z-CERT en wat snel tot resultaat kan leiden.

4.1 AANSLUITSTRATEGIE PER SECTOR

De onderstaande sectoren komen met prioriteit in aanmerking voor aansluiting op Z-CERT in 2021-2022.

A. Jeugdzorg (gecertificeerde jeugdzorginstellingen).
B. Publieke gezondheidszorg (Gemeentelijke Gezondheidsdiensten en GHOR).
C. Huisartsenzorg (huisartsenposten en huisartspraktijken).
D. Farmaceutische zorg (apotheken).
E. Ambulancezorg (ambulancediensten).

Voor bovenstaande sectoren hebben we een opsomming gemaakt van onderwerpen die in de planvorming voor de aansluiting verder kunnen worden opgepakt door VWS, branche- en koepelorganisaties en Z-CERT. Hierbij hebben we rekening gehouden met de aansluitbaarheid van zorginstellingen binnen deze sectoren.

A. Jeugdzorg

- Aansluiten bij initiatief/verkenning van Jeugdzorg Nederland voor informatiebeveiliging en Z-CERT laten participeren bij de ontwikkeling van een integrale aanpak voor informatiebeveiliging voor de jeugdzorg.
- Als eerste aansluitafspraken maken met de gecertificeerde instellingen die jeugdbescherming en jeugdreclassering bieden (15 leden). Vervolgens met de overige leden van Jeugdzorg Nederland (70 leden). Daarna kunnen kleine(re) aanbieders van Jeugdzorg aansluiten volgens de hierboven geschetste integrale aanpak.
- Ontwikkelen van dienstverlening Z-CERT samen met Jeugdzorg Nederland en een afvaardiging van medewerkers van gecertificeerde instellingen waar informatiebeveiliging/cybersecurity (al) op de agenda staat.

B. Publieke gezondheidszorg

- Plan ontwikkelen in samenwerking met de koepel GGD GHOR en een afvaardiging van GGD-instellingen om de GGD-instellingen aan te kunnen sluiten bij Z-CERT. In het plan wordt aandacht besteed aan de financiering, GGD- specifieke dienstverlening, de staat van informatiebeveiliging binnen de sector en de wijze van aansluiting bij Z-CERT.
- Voor het opdoen van ervaring binnen deze sector kan worden overwogen om een (grotere) GGD- instelling versneld aan te laten sluiten bij Z-CERT.

C. Huisartsenzorg

- Verkennen van de mogelijkheden om Z-CERT te laten participeren in het landelijk initiatief van stichting LEGIO (opgericht door NedHIS, koepel van HIS-gebruikersverenigingen en de eerstelijns- en huisartsorganisaties InEen, LHV en NHG.) De stichting wil een integere, veilige, betrouwbare en toekomstbestendige ICT binnen de eerstelijnszorg stimuleren en tot stand brengen, onder meer door het ontwikkelen

van een keurmerk voor leveranciers binnen de eerstelijnszorg. Z-CERT zou kunnen adviseren over de inhoud van het keurmerk (beveiligingseisen waar leveranciers aan moeten voldoen, bewaken consistentie en adviseren bij oplevering audits).
- Inventariseren van bestaande landelijke en regionale structuren en analyseren van de (on)mogelijkheden om deze in te zetten voor het leveren van diensten van Z-CERT.
- Ontwikkelen van een model en informatiediensten voor huisartspraktijken in samenwerking met de koepels en het CMIO-netwerk binnen de eerstelijnszorg. In het model komt de behoeftestelling naar voren voor welke diensten hiervoor moeten worden ontwikkeld, de wijze waarop de diensten kunnen worden aangeboden en de financiering hiervan.

D. Farmaceutische zorg

- In samenwerking met de koepel KNMP, overleg voeren over de mogelijkheden om de apothekers aan te kunnen sluiten bij Z-CERT en daartoe een plan ontwikkelen.
- Het verkennen van een mogelijke aanpak voor de farmaceutische deelsector vergelijkbaar met de aanpak voor huisartsenzorg.

E. Ambulancezorg

- Plan ontwikkelen in samenwerking met de koepel en het netwerk van security-professionals om de ambulancediensten aan te kunnen sluiten bij Z-CERT. In het plan wordt aandacht besteed aan de financiering, ambulance specifieke dienstverlening, de staat van informatiebeveiliging binnen de sector en aansluiting bij Z-CERT.

4.2 AANSLUITSTRATEGIE PER ZORGINSTELLING

Kijken we vervolgens naar de aansluitstrategie per zorginstelling, dan komen we tot de volgende aanbevelingen:

Grote instellingen

- Wanneer: direct aansluiten bij Z-CERT.
- Hoe: door samen met de brancheorganisatie en een afvaardiging van leden een plan te ontwikkelen dat gericht is op optimaal verloop van deze aansluiting. Binnen het plan wordt aandacht besteed aan de financiering, de wijze waarop aansluiting plaatsvindt en de staat van informatiebeveiliging binnen de sector.
- Richtdatum: na goedkeuring van het plan kan tot aansluiting bij Z-CERT worden overgegaan.
- Bovendien: eventueel kunnen sectorspecifieke diensten ontwikkeld worden. Hierbij kan onder meer gedacht worden aan dienstverlening voor leveranciers van (medische) informatiesystemen. Voorbeelden hiervan zijn het uitwisselen van informatie over incidenten en kwetsbaarheden van de gebruikte systemen en het aansluiten van de leverancier op het ZDN. Ook kan gedacht worden aan het opzetten en onderhouden van communities, waaraan medewerkers van zorgaanbieders deelnemen, die zich bezighouden met cybersecurity en/of informatiebeveiliging.

Kleine zorginstellingen

- Wanneer: niet direct aansluiten bij Z-CERT, maar via een nog uit te werken combinatie van landelijke en regionale structuren (zogenaamde informatieknooppunten) waarop informatie voor de zorginstellingen wordt aangeboden. Te denken valt aan koepels, kennis- en informatieplatforms zoals het ECP (platform voor de informatiesamenleving) en CIP (Centrum voor Informatiebeveiliging en

Privacybescherming), regionale organisaties (zoals RSO's) en organisaties die zich richten op de informatieveiligheid van ondernemers zoals het Digital Trust Center (DTC) van EZK.

- Hoe: Z-CERT fungeert als een landelijk knooppunt. De structuren kunnen hierbij worden ondersteund door een community-platform waarop zorgaanbieders informatie kunnen ophalen, (elkaar) vragen kunnen stellen en elkaar kunnen ontmoeten. Ook kunnen in samenwerking met bovengenoemde organisaties informatiediensten worden ontwikkeld met concrete en praktische adviezen, afgestemd op de behoeften van de zorgaanbieders uit de verschillende sectoren van de eerstelijns- en tweedelijnszorg.
- Bovendien: eventueel kan een alternatief financieringsmodel worden ontwikkeld rekening houdend met de financiële mogelijkheden van deze kleinere zorginstellingen. Tenslotte kan ook hier gedacht worden aan de eerdergenoemde dienstverlening voor leveranciers van (zorg)informatiesystemen.

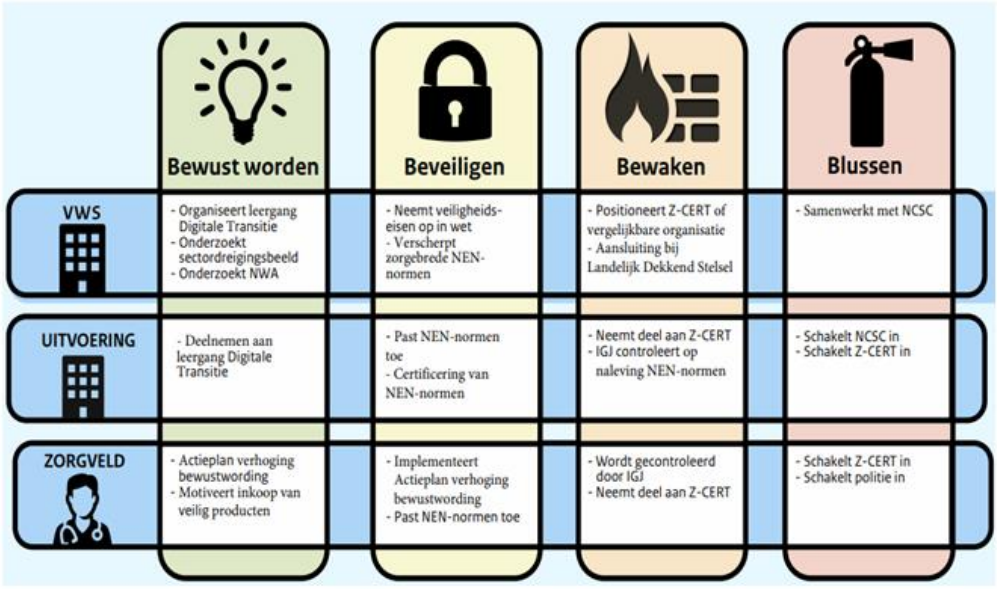
Naast het bewaken van status en voortgang van de voorgestelde activiteiten voor 2021 dienen in 2022 de risicoprofielen te worden geëvalueerd, rekening houdend met ontwikkelingen in de sector en (landelijke) dreigingsbeelden. Op basis van deze evaluatie kan een volgende groep van sectoren worden geprioriteerd voor aansluiting bij Z-CERT.

Hoofdstuk 5 Mogelijke vervolgstappen in kader van 4B-beleid

Dit hoofdstuk beschrijft hoe onze bevindingen aansluiten op het 4B-informatiebeveiligingsbeleid van VWS (bewust worden, beveiligen, bewaken en blussen). Op basis van een gap-analyse met de huidige stand van zaken, schetst dit hoofdstuk een aantal suggesties voor mogelijke vervolgstappen in dit beleid.

5.1 GERELATEERDE ACTIVITEITEN VWS

VWS voert een actief beleid op het bevorderen van de informatiebeveiliging binnen de zorg. Daarbij hebben uitvoeringsorganisaties (zoals CIBG, ZIN en NZA) en het zorgveld (private partijen zoals zorgaanbieders en zorgverzekeraars maar ook bijvoorbeeld VZVZ en natuurlijk de leveranciers) een duidelijke eigen verantwoordelijkheid. Dit terwijl VWS wél stelselverantwoordelijkheid draagt. VWS richt zich daarom met name op de kaderstelling en het stimuleren van zorgsectoren om op een hoger veiligheidsniveau te komen. Daarbij is de aanpak van VWS over de afgelopen jaren veranderd van reactief naar meer proactief beleid en van toezien en faciliteren naar meer regie nemen. Zo worden waar nodig aanvullende onderzoeken gedaan, zoals deze aansluitstrategie voor Z-CERT, en speelt VWS actief in op de actualiteit, zoals COVID-19 en de spoedwet WBNI waarvoor samengewerkt wordt met het NCSC. VWS rapporteert met regelmaat aan de Kamer over het geheel aan activiteiten passend binnen het 4B beleid.



Figuur 3. Decoratieve afbeelding van 4B-informatiebeveiligingsbeleid van VWS

Op het terrein van de normering wordt thans gewerkt aan de verdere inbedding van de reeds langer bestaande normen NEN 7510, met als subnormen NEN 7512 en NEN 7513 in de nieuwe wet elektronische gegevensuitwisseling zorg (Wegiz) en het toezicht daarop door de Inspectie Gezondheidszorg en Jeugd (IGJ). Dit mede omdat geconstateerd is dat de daadwerkelijke implementatie van deze normen in het zorgveld achterblijft. Recent is de NTA 7516 (Eisen voor veilige e-mail en chatapplicaties) vastgesteld en deze is thans in implementatiefase. Verder wordt overwogen om end-to-end encryptie en de aansluiting op Z-CERT mee te nemen in de NEN 7512.

Ook het zorgveld zelf zet op dit moment al aanzienlijke stappen, zoals de aansluiting op Z-CERT in tranches (eerst door ziekenhuizen en GGZ- instellingen). Deze stappen bevinden zich met name binnen de beleidslijnen Bewaken en Blussen. Daarnaast wordt door Brancheorganisaties Zorg (BoZ) in samenwerking met VWS gewerkt aan de uitvoering van het Actieplan Informatieveilig Gedrag, in het kader van Bewustwording.

5.2 SUGGESTIES VOOR VERVOLGACTIVITEITEN

Op basis van de huidige stand van zaken met betrekking tot het 4B beleid is een aantal aanvullende en flankerende maatregelen mogelijk om de in hoofdstuk 4 geschetste aansluitstrategie verder te versterken. Hierbij wordt aangesloten op het 4B model en ingegaan op de rol van VWS, Z-CERT en het zorgveld (koepels), in het besef dat Z-CERT zich met name richt op Bewaken en Blussen en de zorgsector privaat georganiseerd is. Zo komen wij tot de onderstaande suggesties.

Suggesties voor VWS

Bewust worden:

1. Periodieke herijking van de risico gestuurde aanpak.
   - Jaarlijks monitoren weerbaarheid en beveiligingsbeeld (FG/CISO, aansluiting Z-CERT).
   - Aandachtspunt: veiligheid om toe te passen (van leren, niet afrekenen, vertrouwelijk).
   - Ontwikkelen van cybersecuritybeeld voor de zorg zoals CSBN.
2. Ondersteunen koepels en leveranciers bij preventie, bewustwording en gedragsverandering.
3. Kennisdelen via de zorgbrede community Informatieberaad Zorg, en daarbinnen de expertise-community Informatieveiligheid & Privacy. Tevens samenwerking zoeken met andere platforms zoals het ECP en het CIP.
4. Ondersteunen bij activiteiten om IGJ voor te bereiden op nieuwe inspectietaken.
5. Financieringsmodel ontwerpen voor de aansluiting van (kleinere) zorgaanbieders.
6. Gesprek voeren met leveranciers t.b.v. aansluiten Z-CERT (mede in kader van de kostendiscussie).

Beveiligen

1. Monitoren Europese wet- en regelgeving en vertalen naar NL-normen.
2. Naar aanleiding van mogelijk benoemen van onderdelen van de zorg als vitale infrastructuur: dit zo nodig vertalen naar sectorspecifieke normen.
3. Keurmerk informatie-veilige producten op basis van security-by-design oprichten.

Bewaken

1. Verplichten tot melden cyberincidenten, vergelijkbaar met de procedure voor melden datalekken.

Suggesties voor Z-CERT

Beveiligen

1. Zich positioneren ten opzichte van andere CERT'S nationaal en internationaal, speelveld is in beweging.

Bewaken

1. Een signaalfunctie voeren richting nog niet/beperkt aangesloten sectoren (bijvoorbeeld via koepels en leveranciers).
2. Samenwerken met DTC voor kleine(re) zorgaanbieders en andere relevante partijen in de keten van zorgaanbieders.

Blussen

1. Noodhulp verlenen (art 16) voor niet bij Z-CERT aangesloten deelnemers.
2. Incidentrapportages leveren, ook voor niet-aangesloten deelnemers op basis van noodhulp.

3. Incidenten melden van niet bij Z-CERT aangesloten sectoren bij bijvoorbeeld Z-CERT/koepel/leverancier/politie.

Suggesties voor het zorgveld

Bewust worden

1. Actieplan opstellen bewustwording per prioritaire sector met de focus op oefenen (want incidenten blijven voor komen) in samenhang met andere crisisorganisaties.
2. Verbreden BOZ-pilots Informatieveilig gedrag.
3. Kennis over cybersecurity en weerbaarheid opnemen in studie/bijscholing (PE-punten).
4. Samenwerken met regionale organisaties en organisaties voor zorgondernemers, zie ook DTC van ministerie van Economische Zaken.
5. Ondersteunen koepels en leveranciers bij preventie en bewustwording.

Suggesties voor patiënten en zorgconsumenten

Bewust worden

1. Aansluiten op lopende initiatieven vanuit het ministerie van Binnenlandse Zaken (BZK).

Bijlage A Gehanteerde methodiek business impactanalyse (BIA)

In deze bijlage lichten we de gebruikte BIA-methodiek toe.

A1 DEFINITIE EN SCOPE INFORMATIEBEVEILIGING/CYBERSECURITY

Definitie informatiebeveiliging en cybersecurity

Informatiebeveiliging is voor deze opdracht gedefinieerd als een samenhangend stelsel van preventieve, detectieve, repressieve en correctieve maatregelen. Dit stelsel is gericht op het waarborgen van de betrouwbaarheid van informatie die wordt verwerkt door (medische) informatiesystemen waarmee zorgaanbieders in de onderkende sectoren werken.

Onder betrouwbaarheid wordt verstaan:

- Beschikbaarheid: mate waarin informatie op de juiste momenten beschikbaar moet zijn voor (zorg)medewerkers en/of systemen. Onder beschikbaarheid wordt tevens continuïteit verstaan en het heeft betrekking op de periode waarbinnen, in geval van een calamiteit, de oorspronkelijke situatie moet worden hersteld.
- Integriteit: mate waarin informatie juist, volledig en tijdig is geregistreerd en wordt verwerkt door het (medische) informatiesysteem.
- Vertrouwelijkheid: mate waarin toegang tot informatie beperkt is tot degenen of de systemen die daartoe bevoegd zijn. Indien sprake is van persoonlijke gegevens (van patiënten of medewerkers) wordt ook gesproken over privacygevoelige informatie.

Voor deze opdracht spreken wij van digitale informatie die door het (medische) informatiesysteem wordt verwerkt (raadplegen, uitwisselen, verwijderen, wijzigen, archiveren etc.), inclusief systemen waarmee informatie wordt uitgewisseld.

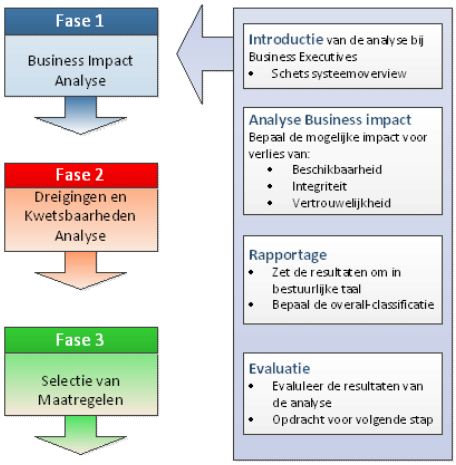
Cybersecurity heeft betrekking op de maatregelen voor het mitigeren van risico's die samenhangen met het internet zoals ransomware, malware, phishing en DDoS- aanvallen.

Uitgangspunten

Onderstaande soorten dreigingen zijn bij de BIA uitgesloten omdat deze dreigingen buiten de invloedssfeer van Z-CERT en de aanbieders vallen (dit is een indicatieve opsomming en heeft niet als doel om compleet te zijn):

- Stroomstoringen waardoor ICT- systemen, voor een bepaalde periode, niet beschikbaar zijn.
- Natuurrampen, zoals overstromingen en stormen waardoor instellingen niet bereikbaar zijn of afdelingen moeten sluiten,
- Rellen, opstanden, oorlog, atoomkernreacties waardoor gebouwen niet meer bruikbaar zijn of zorginstellingen de zorgvraag niet meer aankunnen.
- Virusuitbraken, epidemieën en pandemieën waardoor zorginstellingen geen (reguliere) zorg meer kunnen leveren.

Voor de risicoanalyse is gekozen voor de IRAM2- methodiek. Deze wordt vaak toegepast binnen de overheid (onderdeel van NORA) en de zorgsector. In het kader van deze opdracht is alleen fase 1 van deze methodiek van toepassing.



Figuur 4: Decoratieve afbeelding methodiek IRAM-2

A2 VRAGENLIJSTEN IMPACTANALYSE

In deze bijlage zijn de vragenlijsten opgenomen die voor het inventariseren van de impact zijn gebruikt. Het invullen van de vragenlijsten leidt tot een impactwaarde voor beschikbaarheid, integriteit en vertrouwelijkheid. Bij het onderdeel vertrouwelijkheid zijn eventuele gevolgen in relatie tot imagoschade meegenomen. Dit is terug te vinden bij de onderdelen financiën (directe gevolgen van), het onderdeel bedrijfsvoering (zoals continuïteit en bestuurbaarheid van de zorginstelling), de patiëntveiligheid en de medewerkers (vertrouwen). Steeds is uitgegaan van een worst-case scenario.

De vragenlijsten vindt u in het bij dit rapport behorende document “Aanvullende bijlagen bij Rapport Onderzoek naar de prioriteitstelling en aansluitbaarheid van zorgsectoren bij Z-CERT - december 2020”.

A3 GROEPERING (MEDISCHE) INFORMATIESYSTEMEN

Onderstaande indeling is gehanteerd voor het groeperen van de informatiesystemen die door de zorgaanbieders worden gebuikt en waarvoor de vragen zijn ingevuld:

- Sturing en verantwoording:
  - Systemen voor rapportage en managementinformatie.
  - Systemen voor populatiemanagement.

- Samenwerking:
  - Systemen die in de keten worden gebruikt om informatie over patiënten uit te kunnen wisselen.
  - Kennissystemen voor het opzoeken van informatie over onder meer ziektebeelden en behandelingen.
  - Systemen voor uitwisseling van gegevens met andere zorgaanbieders via regionale en landelijke koppelingen (zoals zorgdomein en LSP).

- Zorg:
    - Elektronisch patiëntdossier voor het registreren van onder meer persoonsgegevens, anamnese en allergieën, e-consulten, (lab)uitslagen, medicatie, verwijsbrieven, declaraties en persoonlijke aantekeningen.

- Zorgprocesondersteuning en logistiek:
    - Systemen voor het registreren van afspraken, het beheren van agenda's en maken van declaraties.
    - Systeem voor het plannen/roosteren van medewerkers, ruimten en patiënten.

- Bedrijfsondersteuning:
    - Financieel systeem.
    - Salaris- en personeelssysteem.
    - Facilitair systeem.
    - Communicatie, vaste en mobiele telefonie (inclusief apps zoals WhatsApp).
    - IT- infrastructuur: hardware en software die aanwezig is op de locatie(s) van de instelling om de applicaties te kunnen gebruiken (rekencentrum, servers, netwerk en pc's/laptops/tablets).

- Cliëntsystemen/portalen:
    - Praktijkwebsite: website met algemene informatie over de zorginstelling.
    - Patiëntportaal: website/portal voor patiënten voor onder meer het maken van afspraken, aanvragen (herhaal)medicatie, raadplegen medisch dossier en lab uitslagen.
    - E- health omgevingen: systemen waarmee, via internet, zorgverleners zorg op afstand kunnen leveren en patiënten zelf registraties en metingen kunnen uitvoeren.

Bijlage B Profiel zorgsectoren

In deze bijlage is een beschrijving opgenomen van de profielen van de onderkende sectoren. De profielen zijn volgens onderstaande structuur uitgewerkt. Bij de afstemming en validatie van de profielen met de achterban zijn voor de herkenbaarheid bepaalde accenten aangebracht (bepaalde onderwerpen zijn met meer/minder diepgang uitgewerkt).

De beschrijving van het profiel bestaat uit onderstaande onderwerpen:

- Typering zorgsector:
    - Beschrijving type zorg.
    - Kentallen.
    - Overzicht van koepelorganisaties, landelijke programma's en gebruikersverenigingen.

- Overzicht van de belangrijkste (medische) informatiesystemen en leveranciers die door de zorgaanbieder worden gebruikt.

- Overzicht van organisaties en andere zorgaanbieders waarmee patiëntgegevens worden uitgewisseld.

- Ontwikkelingen in de sector die van invloed kunnen zijn op het (toekomstige) profiel en de impact op cybersecurity.

De profielen vindt u in het bij dit rapport behorende document "Aanvullende bijlagen bij Rapport Onderzoek naar de prioriteitstelling en aansluitbaarheid van zorgsectoren bij Z-CERT - december 2020".

Bijlage C Resultaten BIA

In deze bijlage zijn de resultaten van de BIA van de onderkende sectoren opgenomen. De BIA bestaat uit een inventarisatie van de impact (financiën, continuïteit/ bedrijfsvoering, patiënt en medewerker) op een zorginstelling indien (1) de informatiesystemen niet beschikbaar zijn, (2) informatie die met de informatiesystemen wordt verwerkt niet-integer is en (3) informatie die met de informatiesystemen wordt verwerkt in verkeerde handen terechtkomt.

De resultaten bestaan uit een tabel met de scores voor de groepen informatiesystemen, voorzien van een toelichting. Deze vindt u in het bij dit rapport behorende document "Aanvullende bijlagen bij Rapport Onderzoek naar de prioriteitstelling en aansluitbaarheid van zorgsectoren bij Z-CERT - december 2020".

Bijlage D Visualisatie speelveld zorg in relatie tot aansluitbaarheid bij Z-CERT

Figuur 5: Decoratieve afbeelding visualisatie speelveld zorg

Bijlage E Achtergrondinformatie Cybersecurity in Nederland

In deze bijlage geven we achtergrondinformatie over cybersecurity in Nederland voor wie zich meer wil verdiepen in de context van aansluiten bij Z-CERT.

OVERHEIDSAMBITIES CYBERSECURITY

In Nederland zijn bedrijven en overheden in toenemende mate afhankelijk geworden van informatietechnologie ter ondersteuning van hun bedrijfsvoering. De COVID-19 crisis heeft deze groei versneld; een groot deel van de Nederlandse bevolking werkt nu op afstand, studeert op afstand en onderhoudt sociale contacten op afstand. De afhankelijkheid van (aanbieders van) digitale middelen is groter dan ooit. Analoge terugvalopties worden schaars of bestaan zelfs niet meer.

Deze toegenomen afhankelijkheid is ook van toepassing op de zorgsector. Medische informatiesystemen zijn vandaag de dag niet meer weg te denken uit zorginstellingen. Naast de vele kansen en mogelijkheden die de inzet van medische technologie biedt, kan het niet-betrouwbaar functioneren hiervan en/of het werken met niet-betrouwbare informatie (grote) consequenties hebben voor zowel patiënten als zorginstellingen. Het cybercrime risicoprofiel van de zorgsector en individuele zorginstellingen verandert dan ook voortdurend, bijvoorbeeld op het gebied van informatieveiligheid en privacy.

Dreigingen en incidenten komen ook vaker op de politiek-bestuurlijke agenda. Cybersecurity is een prioriteit van dit kabinet en vastgelegd in 2018 met de uitwerking van de Nederlandse Cybersecurity Agenda (NCSA)[7]. De strategische agenda omvat zeven ambities en is tot stand gekomen in nauwe samenwerking met partijen uit de publieke en private sector, de wetenschap en de samenleving.

Cybersecurity valt onder coördinatie van het ministerie van Justitie & Veiligheid, maar om de cybersecurity-ambities te realiseren zijn alle sectoren en ministeries aan zet. Met de Kamerbrief “Evaluatie Citrix problematiek” en de kabinetsreactie op het WRR-rapport “Voorbereiden op digitale ontwrichting”[8] onderschrijft het kabinet de hoofdaanbeveling van de Wetenschappelijke Raad voor het Regeringsbeleid (WRR) dat de voorbereiding op digitale incidenten een nadrukkelijk onderdeel moet zijn van ons nationaal veiligheidsbeleid.

Het voorkomen en bestrijden van cybercrime valt of staat met accurate, tijdige en begrijpelijke informatieverstrekking. Informatie over cybersecurity moet voor alle organisaties in Nederland op eenvoudige wijze toegankelijk zijn en reële handelingsperspectieven bieden.

Momenteel wordt door VWS in samenwerking met Z-CERT als volgt invulling gegeven aan de ambities:

- Z-CERT is begin 2020 door het NCSC aangewezen vanuit de WBNI[9] als sectorale CERT voor de zorg[10] binnen het Landelijk Dekkend Stelsel. Hierdoor kan het NCSC meer

7 www.ncsc.nl/onderwerpen/nederlandse-cyber-security-agenda/documenten/publicaties/2019/mei/01/nederlandse-cybersecurity-agenda

8 www.wrr.nl/publicaties/rapporten/2019/09/09/voorbereiden-op-digitale-ontwrichting

9 www.rijksoverheid.nl/documenten/rapporten/2018/09/01/wet-beveiliging-netwerk--en-informatiesystemen-wbni-voor-digitale-dienstverleners

10 www.rijksoverheid.nl/documenten/kamerstukken/2020/06/29/tk-beleidsreactie-csbn-2020-en-voortgangsrapportage-ncsa

dreigingsinformatie delen met Z-CERT. Dit heeft een belangrijke impuls gegeven aan de dienstverlening van Z-CERT wat ten goede komt aan de deelnemers.
- In de NCSA is het belang benadrukt van een adaptieve benadering van cybersecurity. Dit blijft noodzakelijk om in te kunnen spelen op de technologische en maatschappelijke ontwikkelingen en actuele dreigingen en risico's. De huidige COVID-19 crisis heeft bijvoorbeeld geleid tot spoedwetgeving om ziekenhuizen, farmaceuten en onderzoekscentra te kunnen ondersteunen bij cyberaanvallen. Hierin is Z-CERT als sectorale CERT het eerste aanspreekpunt voor de ziekenhuizen.
- De zorgsector voldeed eerder niet aan de criteria om in aanmerking te komen voor vitale infrastructuur. VWS voert momenteel een herbeoordeling uit over het wel- of niet vitaal verklaren van (onderdelen binnen) de zorg[11].

NATIONALE CRISISSTRUCTUUR

Niet alle incidenten kunnen worden voorkomen. Daarom is het belangrijk dat organisaties voldoende veerkrachtig zijn (ook wel cyberweerbaar genoemd). Organisaties moeten snel kunnen herstellen van een cybercrisis. Z-CERT helpt haar deelnemers om cyberincidenten in een vroeg stadium zelf onder controle te krijgen. Mocht een lokaal incident echter tot een organisatie- of sector overstijgende crisis uitgroeien, dan kan Z-CERT VWS ondersteunen in opschaling naar regionale of zelfs nationale crisisstructuren.

Voor situaties waarin de nationale veiligheid in het geding is (of kan zijn) en dus vitale belangen van de samenleving zodanig bedreigd worden dat er sprake is van (potentiële) maatschappelijke ontwrichting, zal de nationale crisisstructuur in werking treden. Deze is door het kabinet vastgelegd in het Instellingsbesluit Ministeriële Commissie Crisisbeheersing en het Nationaal Handboek Crisisbesluitvorming.

Het Nationaal Crisisplan Digitaal (NCP-Digitaal)[12] is een specifieke uitwerking voor de aanpak van een crisis met digitale elementen. Dit plan is een leidraad om inzicht en overzicht te creëren voor organisaties en betrokkenen die een rol spelen bij de beheersing van de maatschappelijke gevolgen en effecten van cyberincidenten. Het plan beschrijft de crisisaanpak op nationaal niveau en de samenwerking en aansluiting met betrokken publieke en private partners en netwerken op regionaal, nationaal en internationaal niveau. Centraal staat de gezamenlijke opgave om in het geval van een grootschalig incident of crisis de maatschappelijke ontwrichting te voorkomen of de effecten te beperken.

De zorgsector is via Z-CERT op meerdere vlakken aangehaakt bij deze nationale crisisstructuur. Z-CERT maakt onderdeel uit van de ICT Respons Board (IRB). Daarnaast zijn er directe lijnen met het Departementaal Crisis Centrum van VWS. Beiden zijn opgenomen in het NCP-Digitaal.

RELEVANTE ANDERE SECTORALE CERT'S

Het NCSC[13] is het informatieknooppunt en expertisecentrum voor cybersecurity in Nederland. Hier komen tactische en operationele kennis en expertise uit de publieke en private sectoren bij elkaar. Het NCSC heeft een directe relatie met de sectorale CERT's en voorziet hen van relevantie informatie. Bij dreigingssituaties heeft het NCSC een coördinerende rol. Het NCSC valt onder verantwoordelijkheid van de NCTV van het ministerie van J&V. In onderstaand overzicht staan de andere landelijke en sectorale CERT's in Nederland.

- Rijksoverheid (Vitaal): NCSC-versterking/uitbreiding LDS

11 www.rijksoverheid.nl/documenten/kamerstukken/2020/10/02/kamerbrief-over-vierde-brief-elektronische-gegevensuitwisseling-in-de-zorg

12 https://www.ncsc.nl/documenten/publicaties/2020/februari/21/nationaal-crisisplan-digitaal

13 https://www.nctv.nl/onderwerpen/nationaal-cyber-security-centrum

- Ondernemers (Private zorg): DTC-nadruk op Advies (zelfredzaamheid)
- Gemeentelijke zorgtaken: IBD-CERT taken en ondersteuning & adviesproducten
- Watersector: CERT-WM (expertise procesautomatisering)
- Universiteiten: SurfCERT - Academische Ziekenhuizen
- Nationale crisisstructuur (aanhaking bij DCC): NCTV/NCC
- Regionale crisisstructuur (veiligheidsregio's): VR-ISAC, verkenning naar een CERT (toekomstplannen)

Daarnaast zijn in diverse andere sectoren CERT's opgericht en zijn ook binnen multinationals CERT's actief. Hoewel in de basis alle CERT's een taak hebben op gebied van incident response, bestaan er in de praktijk (grote) verschillen in takenpakket/dienstverlening, doelgroep en organisatorische ophanging.

Voor Z-CERT is het intensiveren van samenwerking met andere CERT's aan te bevelen, waaronder informatie- en kennisdeling én afstemming over overlappende doelgroepen. Het NCSC werkt aan dit thema vanuit een voorstel voor een Landelijk Dekkend Stelsel (LDS) van cybersecurity samenwerkingsverbanden.

CYBERSECURITY IN BEWEGING

De cyberontwikkelingen in de zorgsector zijn gekoppeld aan het veranderende speelveld van cybersecurity in het algemeen. En daar moet Z-CERT continu op blijven inspelen door zich wendbaar op te stellen en te leren van toekomstige cybercrisissen en initiatieven van anderen rondom dit thema. Zo onderzoeken de Veiligheidsregio's vanuit reguliere regionale crisisbeheersing hun rol bij crisissen en bij het voorkomen hiervan[14]. Gemeenten verkennen vanuit een bestuurlijke agenda hun rol bij cyberincidenten in gemeentelijke context, zoals bij GGD'en. De NCTV werkt met een versterkingsprogramma 'Nederland Digitaal veilig' aan de actiepunten uit het NCSA. Daarnaast kijkt de NCTV vanuit haar coördinerende rol met een 'versterkingsprogramma vitale processen' onder andere naar cyberaspecten van nutsvoorzieningen, waarvan ook zorginstellingen afhankelijk zijn, zoals Internet Service Providers (ISP's), stroomvoorzieningen en communicatiediensten. Het ministerie van Economische Zaken (EZK)/het Digital Trust Center (DTC) onderzoekt hoe het optimaal bedrijven en organisaties kan ondersteunen bij digitaal ondernemen in een maatschappij waarin digitale dienstverlening een vlucht heeft genomen, zeker nu, ten tijde van de COVID-19 crisis.

14 Bestuurlijke agenda digitale ontwrichting Veiligheidsregio's.