CSIRT-STELSEL

Een beleidskader voor het herinrichten van het stelsel met een nationale en sectorale CSIRT's in Nederland

Petra Oldengarm

19 april 2023

Opdrachtgever

Stuurgroep voor de versterkte aanpak vitaal (VAV). Deze stuurgroep heeft als taak om bij het formuleren van de uitgangspunten voor een aanpassing van het vitaal stelsel en tijdens het implementatietraject sturing te geven aan dit traject en beleidskeuzes te maken met aandacht voor de samenhang tussen het huidige vitaal stelsel, de *Critical Entities Resilience* (CER) *directive* en de *Network and Information Security* (NIS2) *directive.* Elk departement dat bij het huidige vitaalbeleid of de implementatie van de CER of NIS2 betrokken is neemt deel aan deze stuurgroep. Bij specifieke onderwerpen schuift een afvaardiging vanuit de toezichthouders werkgroep en/of het NCSC aan.

Over de auteur

Petra Oldengarm is zelfstandig adviseur cybersecurityvraagstukken en adviseert in deze rol zowel de overheid als private organisaties over uiteenlopende strategische thema's. Ze is afgestudeerd in de technische informatica aan de Rijksuniversiteit Groningen. Daarna heeft ze ervaring opgedaan bij diverse werkgevers, zowel in de publieke als private sector. Gedurende meerdere jaren is ze actief in het domein van cybersecurity, waarvan sinds 2018 als zelfstandig adviseur. Naast haar advieswerkzaamheden is Petra Oldengarm (parttime) directeur van Cyberveilig Nederland en gastdocent aan de Universiteit Leiden. Ook is ze lid van de Raad van Toezicht van de Dutch Institute for Vulnerability Disclosure (DIVD).

INHOUDSOPGAVE

MANAGEMENT SAMENVATTING

In dit rapport worden de resultaten gepresenteerd van de CSIRT[1]-verkenning die heeft plaatsgevonden in de periode september 2022 tot en met maart 2023 en is gericht op de volgende hoofdvraag:

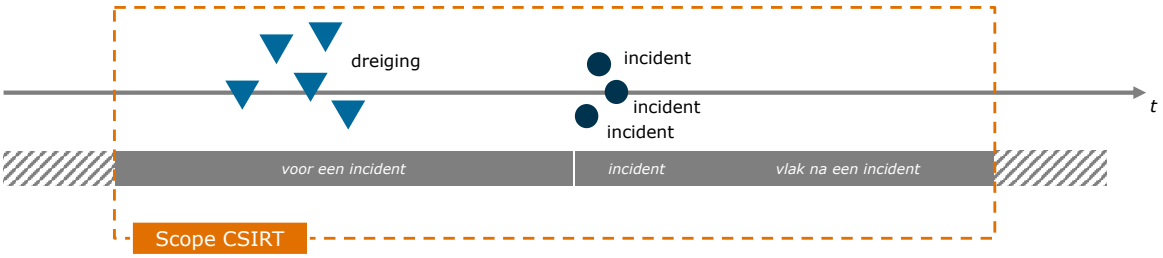
Hoe kan een beleidskader voor het herinrichten van het CSIRT-stelsel met een nationale en sectorale CSIRT's worden vormgegeven, rekening houdend met de impact van de NIS2 en sectorale cybersecurityrichtlijnen?

Er is in Nederland in de loop van de jaren een landschap ontstaan waarin verschillende sectorale en niet-sectorale CSIRT's actief zijn. Binnen deze verkenning, die uitgevoerd is door onafhankelijk adviseur Petra Oldengarm in opdracht van de stuurgroep van het programma Versterkte Aanpak Vitaal binnen de Rijksoverheid, ligt de **focus op de sectorale CSIRT's in Nederland** actief zijn. Daarvan is er op het moment van schrijven van dit rapport een zestal in Nederland actief: het **NCSC** en **CSIRT-DSP** (beiden in de Wbni opgenomen) en **CERT-WM**, **IBD**, **SURF-CERT** en **Z-CERT** (allen bij ministeriële regeling in het kader van de Wbni aangewezen).

De **term CSIRT** heeft in het kader van de Wbni/NIS een officiële definitie met daaraan verbonden eisen, maar daarbuiten niet. Buiten de definitie van de Wbni/NIS wordt een CSIRT gezien als een organisatie die zich **bezighoudt met cybersecurity-gerelateerde incidenten**, zowel in de **fase vooraf om ze te voorkomen**, als bij **ondersteuning als ze optreden** (zie Figuur 3). In de praktijk zien CSIRT's hun taak vaak (wat) breder dan de periode vlak rondom cyberincidenten. Het is vanzelfsprekend geen probleem dat CSIRT-organisaties ook andere taken op zich nemen. In dit rapport wordt primair de focus gelegd op de

[1] CSIRT = Computer Security Incident Response Team, equivalent met de term CERT die Computer Emergency Reponse Team betekent, maar waarvan het gebruik beperkt mogelijk is als gevolg van een handelsmerk van Carnegie Mellon University

kerntaken van een CSIRT die binnen de scope van Figuur 3 vallen en de eisen waaraan CSIRT's voor deze taken moeten voldoen. Er is daarbij gekeken naar de rol van een **nationale CSIRT** en de rol van **sectorale CSIRT's**.



Figuur 1 – Scope van een CSIRT

Uit de gevoerde verkenningsgesprekken met vertegenwoordigers van de huidige sectorale CSIRT's en de betrokken vakdepartementen komt het volgende beeld naar voren:

1. **Bestaande sectorale CSIRT's** voegen **waarde** toe aan het landschap
2. Er **ontbreekt overzicht en samenhang** in het CSIRT-landschap
3. **Nieuwe wetgeving vergroot de eisen** aan het CSIRT-landschap
4. De **governance-inrichting** van het huidige landschap **bemoeilijkt** het **beleggen** van **wettelijke taken**

In de komende periode ontstaan er diverse **nieuwe wettelijke taken** op het gebied van ondersteuning door sectorale CSIRT's, met name vanuit de Security of Network and Information Systems Directive (**NIS2**)[2], maar ook vanuit **nieuwe sectorale cybersecurityrichtlijnen** die nog in ontwikkeling zijn.

De **NIS2** voegt **nieuwe wettelijke taken** toe van **operationele aard** op de gebieden monitoring, analyse, het doen van meldingen en ondersteuning bij incident response. Ook zijn er **regie en coördinatietaken** gedefinieerd die bijvoorbeeld gaan over het instrumentarium voor informatiedeling en het bevorderen van standaardisatie. Daarnaast worden er **eisen** gesteld, zowel **aan de lidstaten** voor bijvoorbeeld het aanwijzen van CSIRT's en het zorgdragen van middelen als **aan de sectorale CSIRT's** zelf, voor wat betreft de inrichting van processen en systemen en de kwaliteit van dienstverlening. De **NIS2** wordt **van toepassing op een grote groep met belangrijke en essentiële entiteiten**. Hoewel op dit moment nog niet duidelijk is hoe groot die groep is (**mogelijk** wellicht **meer dan 11.000** entiteiten), is wel duidelijk dat er veel nieuwe entiteiten zijn waarvoor wettelijke eisen gaan gelden en die een beroep kunnen doen op een sectorale CSIRT. Voor sommige sectoren is er nog geen sectorale CSIRT aangewezen en bij sommige bestaande sectorale CSIRT's wordt de doelgroep substantieel groter. De aangewezen CSIRT's zullen in oktober 2024 aan de eisen uit de NIS2 moeten voldoen en de verplichte taken moeten kunnen uitvoeren.

[2] https://eur-lex.europa.eu/legal-content/NL/TXT/HTML/?uri=CELEX:32022L2555

Behalve de NIS2 zijn er nog **andere sectorspecifieke richtlijnen in ontwikkeling**. Op dit moment betreft dit **de Digital Operational Resilience Act (DORA)** die toeziet op extra maatregelen in de financiële sector en de **Network Code on Cybersecurity (Netcode) voor de elektriciteitssector**, maar mogelijk komen hier in de toekomst nog andere richtlijnen bij. De DORA voorziet niet in extra taken voor sectorale CSIRT's, maar de Netcode wel. Omdat de Netcode nog in concept-fase is, is nog maar beperkt duidelijk wat de daadwerkelijke impact zal zijn. Op dit moment lijken de extra activiteiten zich voornamelijk te richten op het ondersteunen bij de opbouw van capaciteiten bij de entiteiten die met deze richtlijn te maken krijgen. De **daadwerkelijke impact** kan echter pas **worden bepaald als de richtlijn definitief is**.

Bij de analyse van het bestaande CSIRT-landschap is ook onderzocht i**n hoeverre er frameworks** bestaan die kunnen helpen om meer **structuur en samenhang in het landschap** aan te brengen en kunnen ondersteunen bij de verdere ontwikkeling van het landschap. Hoewel er **geen breed geaccepteerde frameworks** zijn die voorzien in het **opbouwen van een samenhangend stelsel van sectorale CSIRT's**, zijn er wel **twee frameworks** die op **deelgebieden** toegevoegde waarde kunnen bieden:

1. Het **FIRST CSIRT Services Framework** voor het eenduidig afbakenen van kerntaken van een CSIRT.
2. Het **ENISA CSIRT Maturity Framework**, gebaseerd op het SIM3-volwassenheidsmodel dat gebruikt kan worden voor het meten van taakvolwassenheid van CSIRT's.

Helaas is er (nog) **geen framework** dat voorziet in **structuur** voor de taken van een **nationale CSIRT** dat coördinerende taken heeft over een stelsel heen.

Op basis van de analyse van de bestaande situatie en de aankomende verplichtingen, waaronder die op basis van de NIS2, is de overtuiging ontstaan dat een **herontwerp van het stelsel niet alleen wenselijk is, maar noodzakelijk**. Het advies is daarom om het **stelsel te gaan voorzien** van **meer structuur en samenhang** en daarbij rekening te houden met de volgende **onderscheidende uitgangspunten**:

1. NIS2 en andere richtlijnen:
    a. De komst van **NIS2 en andere wet- en regelgeving** zorgt voor **stringente eisen** op gebied van CSIRT-taken, taakvolwassenheid en samenwerking.
    b. Gezien de reikwijdte van de toepassing van de NIS2 is **haalbaarheid van de uitvoering** van de CSIRT-taken belangrijk.
2. NLCS:
    a. De NLCS stelt dat taken **centraal** worden belegd **als het kan** en **decentraal als het moet**.
    b. Daar waar **sectorale functionaliteit** zich langere tijd met hoogstaande kwaliteit **bewezen** heeft, dient een afweging gemaakt te worden tussen de voor- en nadelen van centralisatie.

   c. Voor de doelgroepen van de CSIRT's is het belangrijk dat zij terecht kunnen bij **één loket** voor hun sectorale CSIRT-dienstverlening[3].
   d. Het is van belang om in het stelsel **effectief** om te gaan met **schaarse menskracht en middelen**.
3. Er is in het stelsel ruimte voor CSIRT's die een doelgroep bedienen die niet onder de sectoren zoals genoemd in de NIS2 (of andere richtlijnen) vallen. Deze CSIRT's worden in het rapport verder '**vrijwillige CSIRT's**' genoemd.
4. Het is van belang een stelsel te ontwikkelen waarvan de **complexiteit zo laag mogelijk** is
5. Daar waar gekozen oplossingen in het stelsel een wettelijke borging vragen is het van belang dat deze **juridisch te implementeren** is.

De komst van een nationale CSIRT, passend bij de NLCS en NIS2 regietaken is in alle scenario's te realiseren en is daarom niet als separaat onderscheidend uitgangspunt opgenomen. Dit geldt ook voor het uitgangspunt dat de politieke verantwoordelijkheid voor sectoren bij de desbetreffende vakminister blijft, zoals dit ook geldt voor toezicht op entiteiten in het kader van de NIS2.

Tijdens de verkenningsgesprekken met de verschillende stakeholders zijn er drie mogelijke scenario's (met varianten) verkend. Dit zijn:

1. De **huidige situatie zonder wijzigingen voortzetten**, waarbij nieuwe wettelijke taken zoveel mogelijk worden geïntegreerd in het al bestaande landschap.
2. Inrichting van een **stelsel met meerdere sectorale CSIRT's** met **wijzigingen** voor wat betreft **taakverdeling, governance en toezicht**. Hiervoor zijn **twee varianten** denkbaar:
   a. Scenario 2a: één nationale CSIRT voor sector-overstijgende taken; **alle sectorale CSIRT's** die onder NIS2 vallen voeren **dezelfde set taken** uit
   b. Scenario 2b: één nationale CSIRT voor overstijgende taken; **alle sectorale CSIRT's** die onder NIS2 vallen voeren **taken naar vermogen** uit; wat zij niet kunnen uitvoeren, delegeren ze naar het NCSC/CSIRT-DSP
3. Alle **bestaande sectorale CSIRT's** worden **geïntegreerd tot één enkele CSIRT** die de wettelijke taken uitvoert voor sectoren die onder de NIS2 vallen.

Deze scenario's met varianten zijn vergeleken met de uitgangspunten die zijn geformuleerd. Onderstaande tabel geeft een korte samenvatting van deze analyse gebruik makend van de volgende vijfpuntschaal:

-- Uitgangspunt is zeer moeilijk te realiseren
- Uitgangspunt is moeilijk te realiseren
+- Uitgangspunt is te realiseren
+ Uitgangspunt is goed te realiseren
++ Uitgangspunt is zeer goed te realiseren

[3] Dit staat los van de discussie of er in Nederland 1 centraal meldpunt moet komen in verband met de meldplicht. In dit uitgangspunt gaat het om het aanspreekpunt voor CSIRT-dienstverlening.

Scenario	1a NIS2-eisen	1b Haalbaarheid uitvoering	2a NLCS-centraal/decentraal	2b Bewezen sectorale impact	2c Eén loket	2d Inzet schaarse capaciteit	3 Kwaliteitsborging vrijwillige CSIRT's	4 Lage complexiteit	5 Juridisch haalbaar
1 Wettelijke taken in huidig landschap	--	--	--	+	-	+-	--	-	--
2a Structuur + homogene CSIRT's	+	+	+-	++	+	++	+	+-	+
2b Structuur + maatwerk-CSIRT's	+-	-	+-	++	--	+-	+	-	-
3 Eén centraal CSIRT voor alle sectoren	++	-	+	--	++	+-	+	+	+

Tabel 1 Mapping uitgangspunten op scenario's CSIRT-stelsel

Bij de definitieve weging van de scenario's zijn de volgende uitgangspunten zwaarder meegewogen:

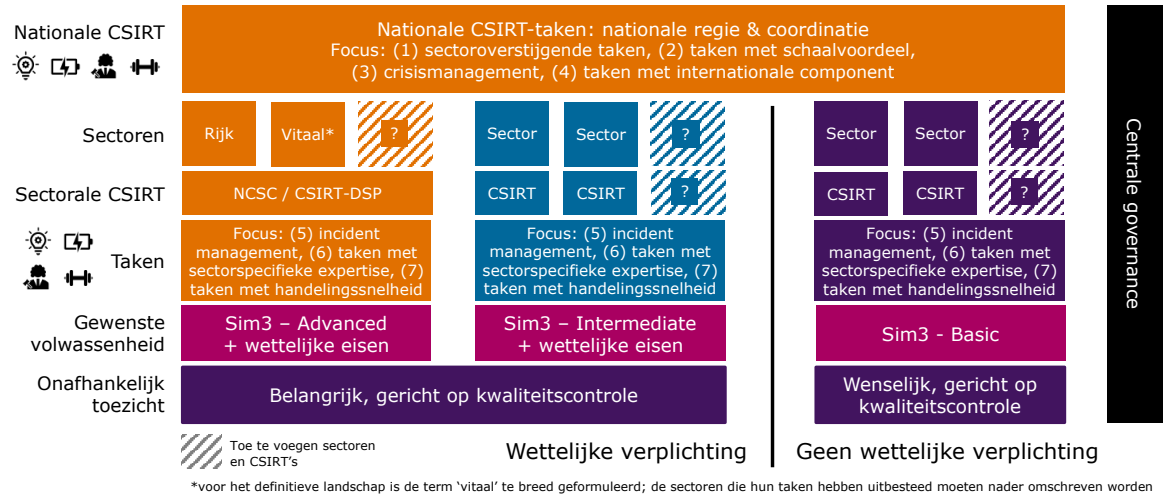
- 1a NIS2-eisen
- 1b Haalbaarheid uitvoering
- 2b Bewezen sectorale impact
- 2c Eén loket
- 5 Juridische haalbaarheid

Op basis van de scores en de weging komt naar voren dat **scenario 2a als meest optimale scenario** naar voren komt. In de analyse valt op dat dit het **enige scenario is dat positief scoort op haalbaarheid** en **overall geen negatieve scores** behaalt. Verder wordt duidelijk dat het eerste scenario, waarbij de wettelijke taken zonder substantiële wijzigingen in het huidige landschap worden geïntegreerd niet haalbaar is. Voor enkele belangrijke uitgangspunten pakken zowel scenario 2b als scenario 3 niet goed uit. Omdat de verschillen tussen de scenario's zo groot zijn en scenario 2a zo duidelijk uit de analyse naar voren komt als voorkeursscenario, is ervoor **gekozen** om in dit rapport **alleen dit scenario in detail uit te werken**.

In de verkenning zijn op basis van de input uit de verkenningsgesprekken en de uitgangspunten de verschillende elementen die van belang zijn voor het CSIRT-stelsel nader uitgewerkt. Deze elementen zijn:

1. **Scheiding** tussen **nationale** en **sectorale CSIRT-taken**. In de nationale CSIRT worden overkoepelende taken belegd, in de sectorale CSIRT's operationele taken voor specifieke sectoren.
2. **Aanbrengen van scope** in de **kerntaken** van een sectorale CSIRT. Er komt een vast takenpakket per CSIRT. Er zijn kaders gedefinieerd voor welke taken door het nationale CSIRT en welke taken door sectorale CSIRT's moeten worden uitgevoerd. In Nederland zal het NCSC/CSIRT-DSP een dubbelrol vervullen: zowel nationaal CSIRT als sectoraal CSIRT voor meerdere sectoren. Geadviseerd wordt om het FIRST CSIRT Services Framework te gebruiken voor een bredere scoping van de kerntaken van CSIRT's.
3. Stellen van **eisen aan de taakvolwassenheid** van sectorale CSIRT's. Deze worden ingegeven door de wettelijke eisen. Geadviseerd wordt om aanvullend het ENISA CSIRT Maturity Framework te gaan hanteren met als niveaus *Advanced* voor NCSC/CSIRT-DSP, *Intermediate* voor overige sectorale CSIRT's met wettelijke taken en *Basic* voor vrijwillige CSIRT's die willen toetreden tot het CSIRT-stelsel.
4. **Ruimte** geven aan **vrijwillige sectorale CSIRT's**. Belangrijk is om ruimte te bieden in het stelsel aan sectorale CSIRT's zonder wettelijke taken. CSIRT's die een hybride doelgroep hebben vallen in het stelsel aan de kant met wettelijke verplichtingen.
5. Het **verbeteren** van de **besturing** van het CSIRT-stelsel. Het is nodig om enkele besturingsmaatregelen te nemen, zoals het inrichten van benodigde governance en toezicht op het CSIRT-stelsel.
6. Het **verbeteren** en **bevorderen** van onderlinge **samenwerking**.

In onderstaande figuur zijn de elementen 1 tot en met 5 schematisch weergegeven. Deze zijn in het rapport stap voor stap toegelicht evenals een advies over het verbeteren en bevorderen van onderlinge samenwerking tussen de CSIRT's.



Figuur 2 - Visie op toekomstig CSIRT-stelsel

Om het CSIRT-stelsel in de praktijk te implementeren zijn in het rapport enkele adviezen voor vervolgstappen meegegeven:

1. **Juridische context** in relatie tot NIS2 en andere sectorspecifieke regelgeving uitwerken
2. CSIRT-ondersteuning borgen voor **alle NIS2-doelgroepen**
3. **Taakverdeling** tussen nationale en sectorale CSIRT's vaststellen
4. Bepalen hoe de **huidige CSIRT's verder gaan** in het CSIRT-stelsel
5. **Inrichten van de besturing** van het stelsel (governance/toezicht)
6. **Koppelen** van het landschap aan het **Landelijk Dekkend Stelsel**
7. **Verbeteren** van **onderlinge samenwerking** tussen CSIRT's
8. **Onderzoeken** hoe een **kostprijsmodel** kan worden toegepast

INTRODUCTIE EN VRAAGSTELLING

In Nederland is in de loop van de jaren een landschap ontstaan waarin verschillende sectorale Computer Security Incident Response Teams (CSIRT's[4]) een rol hebben in het bieden van ondersteuning aan organisaties die te maken hebben met cyberincidenten. De in omvang grootste sectorale CSIRT in Nederland is die van het Nationaal Cyber Security Centrum (NCSC). Daarnaast zijn er nog 5 andere sectorale CSIRT's aangewezen: CERT-WM, CSIRT-DSP, IBD, SURF-CERT en Z-CERT. Op dit moment is er in Nederland (nog) geen nationale CSIRT, hoewel vanuit het buitenland het NCSC als zodanig wordt gezien. Binnen Nederland zijn de wettelijke taken vanuit de Wet beveiliging netwerk- en informatiesystemen (Wbni) bij het NCSC en het CSIRT voor digitale diensten (CSIRT-DSP) belegd.

AANLEIDING VERKENNING

In de afgelopen jaren is binnen Europa gewerkt aan de herziening van de richtlijn op het gebied van cybersecurity, de Security of Network and Information Systems Directive (NIS2)[5]. Deze richtlijn beschrijft maatregelen die moeten zorgen voor een hoog gezamenlijk niveau van cybersecurity binnen de Europese Unie en is de opvolger van de NIS-richtlijn die sinds 2016 van kracht is. Door deze nieuwe richtlijn krijgen meer sectoren verplichtingen op het gebied van cybersecurity.

De NIS2-richtlijn verplicht (net als in de NIS) de lidstaten tot het inrichten van één of meerdere CSIRT's die deze sectoren ondersteunen. De NIS2 vereist aan deze CSIRT's hogere eisen meer taken dan in de NIS. De NIS2 wordt in oktober 2024 van kracht.

---

[4] In dit rapport wordt de algemene term CSIRT gebruikt als verzamelnaam voor CSIRT's en CERT's. CERT is een door Carnegie Mellon University gehanteerd handelsmerk waarvoor bij gebruik in het verleden een licentie moest worden aangevraagd, zie https://www.sei.cmu.edu/our-work/cybersecurity-center-development/authorized-users/. De term CSIRT heeft in de context van de NIS(2) en Wbni een officiële definitie met daaraan verbonden taken en eisen, maar daarbuiten niet.

[5] https://eur-lex.europa.eu/legal-content/NL/TXT/HTML/?uri=CELEX:32022L2555

Voor die tijd zal deze in Nederlandse wetgeving worden omgezet. Dit zal plaatsvinden in de Wbni.

Voor een aantal sectoren waarin NIS2-verplichtingen van toepassing zullen worden zijn al CSIRT's actief. Er zijn echter ook sectoren waarvoor er nog geen CSIRT is ingericht die de in de NIS2 omschreven taken op zich neemt. Op dit moment vinden er gesprekken plaats over hoe dit zal moeten worden ingevuld.

Naast het feit dat vanaf oktober 2024 de nationale NIS2-wetgeving van kracht zal zijn, zijn er sectoren die sectorspecifieke wet- en regelgeving implementeren op gebied van cybersecurity. Ook deze richtlijnen hebben impact op het CSIRT-landschap. Een voorbeeld van zo'n richtlijn is de Digital Operational Resilience Act (DORA) die toeziet op extra maatregelen in de financiële sector en in november 2022 is aangenomen. Een ander voorbeeld is de Network Code on Cybersecurity (Netcode) voor de elektriciteitssector die naar verwachting van kracht wordt rond de zomer van 2023. De bijbehorende CSIRT-bepalingen uit de Netcode zullen na 12 maanden (verwachting is zomer 2024) operationeel moeten zijn.

Tot slot zijn er mogelijkheden om aan efficiëntie te winnen door betere samenwerking, maar ook door sommige CSIRT-taken centraal te beleggen. Het is daarom goed om binnen de kaders en uitgangspunten zoals beschreven in de Nederlandse Cybersecuritystrategie 2022 – 2028 (NLCS) te onderzoeken voor welke taken dit geldt en of daarmee efficiëntie kan worden behaald zonder de voordelen van een sectorspecifieke aanpak te verliezen.

Deze elementen vormden gezamenlijk de aanleiding voor de stuurgroep van het programma Versterkte Aanpak Vitaal[6] (VAV) om over dit onderwerp een verkenning te laten uitvoeren. Dit rapport is het resultaat van deze verkenning die is uitgevoerd door Petra Oldengarm.

VRAAGSTELLING

De hoofdvraag van de verkenning luidt:

Hoe kan een beleidskader voor het herinrichten van het CSIRT-stelsel met een nationale en sectorale CSIRT's worden vormgegeven, rekening houdend met de impact van de NIS2 en sectorale cybersecurityrichtlijnen?

Om te komen tot zo'n beleidskader is in het najaar van 2022 een verkenning uitgevoerd onder de bestaande sectorale CSIRT's, de vakdepartementen die betrokken zijn bij deze CSIRT's en de vakdepartementen die gaan over sectoren die onder één van de nieuwe cybersecurityrichtlijnen gaan vallen. Op basis van deze verkenning is een advies opgesteld voor het herontwerpen van het CSIRT-stelsel. Dat advies wordt in dit rapport nader uitgewerkt en toegelicht.

[6] Zie voor meer context: https://www.nctv.nl/onderwerpen/nationale-veiligheid-strategie/versterkte-aanpak-van-risicos-en-dreigingen/vitale-infrastructuur

ONDERZOEKSVRAGEN EN LEESWIJZER

ONDERZOEKSVRAGEN

Vanuit de geformuleerde hoofdvraag (zie pagina 9) zijn diverse verdiepende vragen geformuleerd die tijdens de verkenning zijn besproken met de betrokken CSIRT's en vakdepartementen. Deze vragen zijn onderverdeeld in drie thema's: taken, taakvolwassenheid en randvoorwaarden. Hieronder zijn de initiële vragen op een rij gezet.

Taken

1. Welke van de taken zoals die zijn geformuleerd in het FIRST CSIRT Services Framework[7] en welke van de (nieuwe) NIS2 taken worden nu al uitgevoerd in het CSIRT?
2. Welke van deze taken vragen om sectorspecifieke kennis?
3. Welke uitgangspunten zijn van belang om te komen tot een goede verdeling van taken?
4. Wat is omwille van efficiëntie en effectiviteit een goede verdeling van taken tussen de sectorale CSIRT's en een nationaal CSIRT? Wat zijn de voordelen, nadelen en risico's?
5. Welke additionele taken zijn er nodig in het stelsel, bijvoorbeeld vanuit (verwachte) sectorspecifieke regulering, maar ook voor het verkrijgen van een goed werkend CSIRT-stelsel?

Taakvolwassenheid

6. In hoeverre wordt de volwassenheid van het CSIRT (structureel) gemeten?
7. Zo ja:
    a. Welk raamwerk wordt gebruikt om dit te toetsen?
    b. Op welk niveau in dat raamwerk is de dienstverlening ingeschaald?

[7] https://www.first.org/standards/frameworks/csirts/csirt_services_framework_v2.1

c. Wat is het ambitieniveau en wat is nodig om op het gewenste niveau te komen/blijven?

8. Zo nee:
   a. Wat is de inschatting van de huidige volwassenheid?
   b. Waarop is deze inschatting gebaseerd?
9. In hoeverre vinden CSIRT's dat volwassenheid een rol kan/moet spelen in de keuze of taken sectoraal of nationaal moeten worden uitgevoerd?
10. Welke criteria zijn daarbij van belang?
11. Indien volwassenheidsmeting wenselijk is in de toekomst, hoe moet dit dan worden ingericht (bijvoorbeeld: tijdslijn voor groei, hoe volwassenheid meten, etc.)?

Randvoorwaarden

12. Welke andere randvoorwaarden zijn van belang bij de keuze om taken sectoraal of nationaal uit te voeren (bijv. op gebied van mensen, middelen, wetgeving, etc.)?
13. Welke *harde* en *zachte* criteria zijn van belang bij het maken van een goede keuze voor de verdeling van taken?
14. Zijn er aanvullende randvoorwaarden nodig vanuit het perspectief van een stelsel-aanpak?

LEESWIJZER

Op basis van de gevoerde gesprekken (zie in de bijlagen op pagina 76) en open bronnenonderzoek is een analyse gemaakt van het huidige landschap (zie pagina 12). Er is vervolgens bestudeerd wat de impact is van de NIS2 op het landschap met sectorale CSIRT's (zie pagina 21). Ook is onderzocht welke sectorspecifieke regelgeving ontwikkeld is/wordt en hoe dit impact heeft op het CSIRT-landschap (zie pagina 27). Daarna is uiteengezet welke frameworks er bestaan voor CSIRT's die meer structuur kunnen geven aan een CSIRT-landschap (zie pagina 27).

In het tweede deel van het rapport wordt ingegaan op de uitgangspunten voor het CSIRT-landschap en de mogelijke scenario's die er zijn om dit landschap verder te ontwikkelen. Deze zijn op elkaar gemapt met als resultaat een voorkeursscenario (zie pagina 35). Vervolgens is dit voorkeurscenario in verder detail uitgewerkt (zie pagina 59) en worden tot slot adviezen gegeven voor vervolgstappen (zie pagina 72).

HUIDIGE CSIRT-LANDSCHAP

DEFINITIE (NATIONALE EN SECTORALE) CSIRT

Bij het in kaart brengen van het huidige CSIRT-landschap rijst allereerst de vraag wat de definitie is van een CSIRT. Zoals in de introductie werd aangestipt is CSIRT de afkorting voor Computer Security Incident Response Team. Soms wordt de alternatieve term CERT gebruikt, dat staat voor Computer Emergency Response Team, een door Carnegie Mellon University gehanteerd handelsmerk waarvoor in het verleden bij gebruik een licentie moest worden aangevraagd[8].

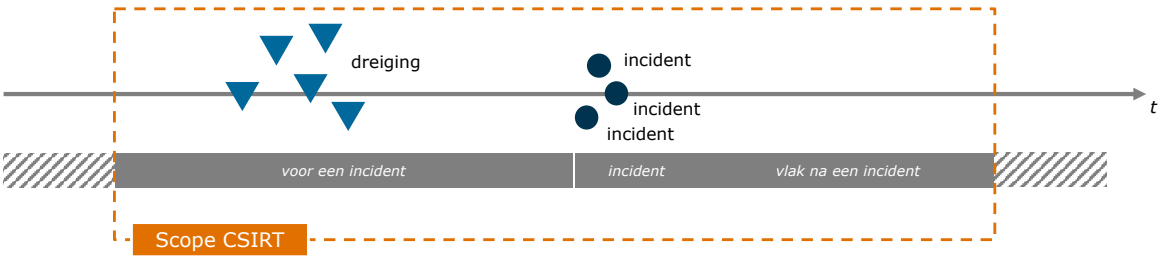
De term CSIRT heeft in het kader van de Wbni een officiële definitie met daaraan verbonden eisen, maar daarbuiten niet. Voor wat betreft de definitie van CSIRT in de Wbni wordt in artikel 1 verwezen naar de definitie van een CSIRT in de eerste versie van de Security of Network and Information Systems Directive[9] (NIS), artikel 9, die op zijn beurt verwijst naar bijlage I. Daarin wordt een CSIRT gedefinieerd als een organisatie met de volgende taken:

- Monitoren van incidenten op nationaal niveau
- Ten bate van de betrokken belanghebbende partijen zorgen voor vroegtijdige waarschuwingen, alarmmeldingen, aankondigingen en verspreiding van informatie over risico's en incidenten
- Reageren op incidenten
- Zorgen voor een dynamische risico- en incidentanalyse en situatiekennis
- Deelnemen aan het CSIRT-netwerk

Buiten de definitie van de Wbni/NIS wordt een CSIRT gezien als een organisatie die zich bezighoudt met cybersecurity-gerelateerde incidenten. Een hoofddoel van een CSIRT is vaak om snel en efficiënt te reageren op cyberincidenten, het adequaat afhandelen ervan en het minimaliseren van schade. Een tweede belangrijk doel richt

[8] https://www.sei.cmu.edu/our-work/cybersecurity-center-development/authorized-users/
[9] https://eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=CELEX:32016L1148&from=NL

zich op de fase voorafgaande aan het incident, namelijk het bieden van ondersteuning bij het voorkomen van incidenten, zie Figuur 3.



Figuur 3 – Scope van een CSIRT

In de praktijk zien CSIRT's hun taak vaak (wat) breder dan de periode vlak rondom cyberincidenten. Het is vanzelfsprekend geen probleem dat CSIRT-organisaties ook andere taken op zich nemen. In dit rapport wordt primair de focus gelegd op de kerntaken van een CSIRT die binnen de scope van Figuur 3 vallen en de eisen waaraan CSIRT's voor deze taken moeten voldoen.

De doelgroep en scope van een CSIRT kan verschillen. In dit rapport wordt onderscheid gemaakt tussen drie typen CSIRT's:

1. Nationale CSIRT
2. Sectorale CSIRT's
3. Niet-sectorale CSIRT's

Nationale CSIRT

Een nationale CSIRT (ook wel nCSIRT genoemd) is een CSIRT die is aangewezen door een land die een specifieke nationale verantwoordelijkheid heeft voor dat land. Het fungeert als centraal contactpunt voor zowel nationale incident-response stakeholders als voor andere nCSIRT's wereldwijd. Een nCSIRT coördineert incident response op nationaal en internationaal niveau en veel nCSIRT's hebben ook sectorale taken voor het beschermen van kritieke infrastructuur[10].

In Nederland is op het moment van schrijven van dit rapport (nog) geen nationaal CSIRT actief, hoewel in de Nationale Cybersecurity Strategie (NLCS) wel de ambitie is uitgesproken om zo'n nationale CSIRT in Nederland aan te wijzen. Door nationale CSIRT's buiten Nederland wordt het NCSC op dit moment gezien als nCSIRT, hoewel het NCSC dit formeel gezien niet is.

Sectorale CSIRT's

Een sectoraal CSIRT is een CSIRT dat ondersteuning biedt aan entiteiten die actief zijn binnen een specifieke sector. Er is geen breed geaccepteerde definitie van de kerntaken van een sectoraal CSIRT, maar ook deze vallen binnen de scope van Figuur 3. Sectorale CSIRT's hebben vaak een uitgebreid netwerk, enerzijds onder hun doelgroep, maar anderzijds onder leveranciers van sectorspecifieke hard- en

[10] Bron: https://d1y8sb8igg2f8e.cloudfront.net/documents/CSIRTs-incident-response.pdf

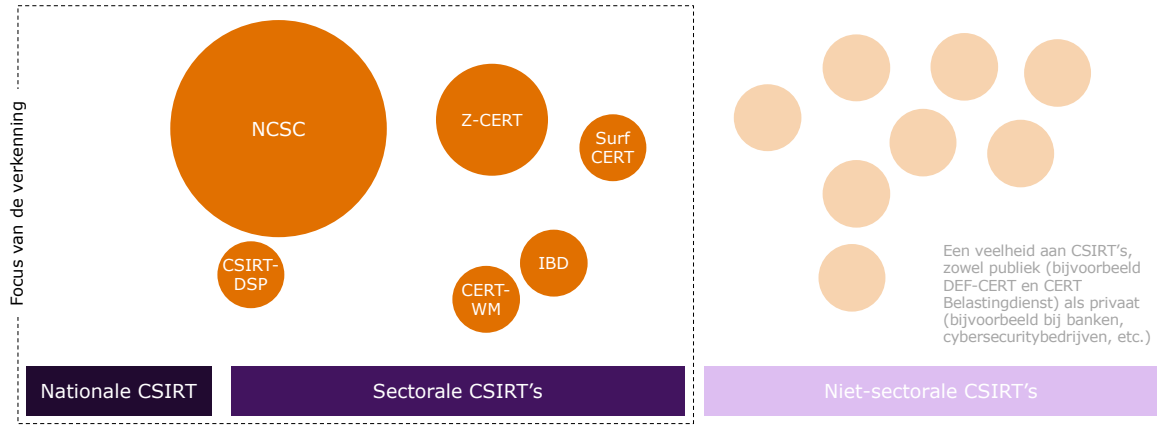
software. Ook ontwikkelen ze sectorspecifieke kennis over binnen een sector gangbare processen en systemen zodat zij hun adviezen en ondersteuning hier zo goed mogelijk op kunnen afstemmen.

Niet-sectorale CSIRT's

In dit rapport is ervoor gekozen om de overige CSIRT's als één groep te beschouwen, die buiten scope van de verkenning vallen. Dit betreft bijvoorbeeld CSIRT's die binnen een organisatie zijn ontstaan (bijvoorbeeld CSIRT's van financiële instellingen, of van publieke organisaties zoals de Belastingdienst). Het gaat ook over CSIRT's die voor een bredere doelgroep ingezet worden, bijvoorbeeld de CSIRT's die cybersecuritybedrijven inzetten bij de ondersteuning van hun klanten. Ook deze CSIRT's voeren allemaal kerntaken uit binnen de scope van Figuur 3.

BESTAANDE SECTORALE CSIRT'S

Er is in Nederland in de loop van de jaren een landschap ontstaan waarin verschillende sectorale en niet-sectorale CSIRT's actief zijn. Sommige van deze CSIRT's bedienen organisaties in en vanuit het publieke domein en andere in en vanuit het private domein (of een mix van beide). Binnen deze verkenning ligt de focus op de sectorale CSIRT's die zijn aangewezen op grond van de Wbni. Daarvan is er op het moment van schrijven van dit rapport een zestal in Nederland actief zoals weergegeven in onderstaande figuur.



Figuur 4 - CSIRT-landschap in Nederland

In de Wbni zijn twee van deze CSIRT's benoemd, die naast de sectorale taken ook enkele nationale/coördinerende taken uitvoeren:

1. Het Nationaal Cyber Security Centrum voor de Rijksoverheid en vitale organisaties (NCSC)
2. Het CSIRT voor digitale diensten (CSIRT-DSP)

Bij ministeriële regeling van de minister van Justitie en Veiligheid zijn er in januari 2020 in het kader van de Wbni additioneel vier sectorale CSIRT's aangewezen[11]:

[11] https://zoek.officielebekendmakingen.nl/stcrt-2022-32041.html

1. CERT Watermanagement (CERT-WM) voor de waterschappen
2. Informatiebeveiligingsdienst (IBD) voor de Nederlandse gemeentes, onderdeel van de Vereniging van Nederlandse Gemeenten (VNG)
3. Het CSIRT van SURF (SURF-CERT) voor kennisinstellingen
4. Z-CERT, het sectorale CSIRT voor de zorgsector

Deze sectorale CSIRT's hebben allemaal een eigen plek in het landschap ingenomen met een set van taken die aansluit op de behoeften van de doelgroep die wordt bediend en in overeenstemming is met beschikbare capaciteit en financiële middelen. In dit hoofdstuk worden de sectorale CSIRT's met elkaar vergeleken voor wat betreft hun doelgroepen en diensten, maar ook ten aanzien van hun governance. Dat laatste is met name van belang bij het toebedelen van wettelijke CSIRT-taken zoals die worden voorgeschreven in de NIS2.

Overigens is in 2022 besloten dat het NCSC en CSIRT-DSP (en het Digital Trust Center – DTC) gaan integreren en een nieuwe organisatie gaan vormen[12]. Voor wat betreft de visie op het toekomstige landschap zal in dit rapport daarom gesproken worden over NCSC/CSIRT-DSP om uiting te geven aan deze integratie.

CSIRT-DIENSTEN EN -DOELGROEPEN

Op het eerste oog lijken de sectorale CSIRT's in Nederland veel van elkaar te verschillen. Allereerst in omvang: van enkele medewerkers bij de kleinere sectorale CSIRT's tot ongeveer 200 medewerkers bij het NCSC[13]. Maar ook in dienstverlening en in de doelgroepen die worden bediend zijn er grote verschillen vast te stellen.

Figuur 5 - CSIRT's leveren uiteenlopende dienstverlening

Als je kijkt naar de dienstverlening dan heeft ieder van de CSIRT's zijn eigen pakket aan dienstverlening ontwikkeld. Soms is dat een beperkt pakket, maar vaak ook een breder pakket aan diensten. Geen van de sectorale CSIRT's gebruikt voor het afbakenen van de diensten op dit moment een bestaand dienstenframework. Dat maakt vergelijken lastig. Bovendien zien we in sommige gevallen dat er extra weerbaarheidsinitiatieven voor een bepaalde sector onder het CSIRT worden geschaard, ook als die minder passen binnen de kerntaken van een CSIRT zoals die in Figuur 3 zijn weergegeven. Hoewel er goede redenen voor kunnen zijn dat deze taken binnen de scope van een CSIRT worden uitgevoerd maakt dit het zicht op de

[12] https://www.rijksoverheid.nl/documenten/kamerstukken/2022/09/13/tk-uitvoerder-programmaplan-sporen-integratie-csirt-dsp-dtc-ncsc
[13] Niet alle, maar wel een groot deel van de NCSC-medewerkers zijn betrokken bij de CSIRT-taken

kerntaken van een CSIRT meer diffuus. Door deze brede taakopvatting ontbreekt een gezamenlijk kader voor en visie op sectorale kerntaken van een CSIRT.

Hoewel het vanuit een landelijk perspectief lastig is dat de CSIRT's moeilijk te vergelijken zijn, stellen we ook vast dat de CSIRT's vanuit een sectoraal perspectief zo goed mogelijke aansluiting hebben gezocht op de eigen doelgroep, passend binnen de mogelijkheden die ze daarvoor hebben (financieel, maar ook voor wat betreft capaciteit en expertise). De CSIRT's geven aan hierdoor veel waarde toe te voegen voor de eigen doelgroep. Elke sectorale CSIRT heeft geïnvesteerd in het opbouwen van kennis over de eigen sector, met name over binnen de sector gebruikte systemen en processen. Daarmee wordt gewaarborgd dat adviezen die door CSIRT's worden gegeven goed aansluiten op de realiteit van de doelgroep. In enkele gevallen zijn relaties ontwikkeld met leveranciers van sectorspecifieke hard- of software waardoor bij kwetsbaarheden snel kan worden geschakeld richting de doelgroep. Het is de wens van de CSIRT's dat deze kennis en relaties in een vernieuwd landschap beschikbaar blijven en waar mogelijk worden versterkt.

Er is met de CSIRT's tijdens de verkenning gesproken over hun taakvolwassenheid. Ook hierin is duidelijk geworden dat vergelijken lastig is, omdat er geen afspraken in het stelsel zijn over het meten van taakvolwassenheid en er ook geen gezamenlijke methodiek hiervoor wordt gehanteerd. In veel gevallen zijn er zelf-assessments uitgevoerd (op basis van vragenlijsten van TF-CSIRT[14], een task force voor samenwerking en coördinatie tussen CSIRT's in Europa en aanpalende regio's), soms aangevuld met collegiale toetsing en een enkele keer met een externe audit. Door het ontbreken van actuele objectieve informatie is het niet goed mogelijk iets te zeggen over de huidige taakvolwassenheid van de sectorale CSIRT's. Uit de besproken zelfassessments komt het beeld naar voren dat er een basisniveau van volwassenheid aanwezig is en dat in sommige gevallen hogere niveaus van taakvolwassenheid worden bereikt. Er zijn tijdens de verkenning geen rapporten over volwassenheid ingezien. Taakvolwassenheid is met het oog op de steeds verdergaande eisen aan lidstaten op het gebied van CSIRT-ondersteuning in het kader van NIS2 een belangrijk onderwerp dat binnen diverse sectorale CSIRT's aan aandacht wint.

Een ander belangrijk element is de aanwezige vakkennis binnen een CSIRT. Onder vakkennis verstaan we enerzijds cybersecuritykennis en anderzijds kennis die sectorspecifiek is, bijvoorbeeld over sectorspecifieke processen of systemen. Dit soort kennis is schaars en moeilijk te werven. Vacatures staan lang open waardoor de (kwaliteit van) dienstverlening onder druk kan komen te staan. Dit geldt voor alle sectorale CSIRT's. Bij het ontwikkelen van een visie op de toekomst van het stelsel is een wens vanuit de CSIRT's om aandacht te hebben voor dit gegeven. Dit speelt met name als er nagedacht wordt over een eventuele samenvoeging van CSIRT's of het verschuiven van taken. Zo'n samenvoeging of verschuiving van taken houdt niet per se in dat personen met de benodigde expertise willen gaan werken op een andere

[14] https://tf-csirt.org/

plek hetgeen kan leiden tot een verlies van experts. Sommige medewerkers vinden het prettiger in een kleinere organisatie te werken en anderen juiste in een grotere. Ook speelt mee waar de CSIRT's in Nederland gevestigd zijn of medewerkers mee zouden kunnen (en willen) verplaatsen.

Figuur 6 - De doelgroepen van CSIRT's lopen erg uiteen

Ook voor wat betreft de doelgroepen zijn er diverse verschillen. De CSIRT's die grotere doelgroepen onder hun hoede hebben, hebben vaak methoden ontwikkeld om effectief te zijn voor dit soort grote groepen. Andere CSIRT's hebben juist een heel nauw contact met hun doelgroep omdat deze klein en homogeen is en daarmee overzichtelijk. Bij de toename van te ondersteunen entiteiten binnen de NIS2 valt lering te trekken uit de sectorale CSIRT's die al effectief zijn in het bedienen van grotere doelgroepen en deze kennis daarmee breder toe te passen.

Niet alle doelgroepen van sectorale CSIRT's zullen in de toekomst verplichtingen hebben op basis van de NIS2 of sectorspecifieke richtlijnen. Toch is het belangrijk om ook deze CSIRT's een goede rol te (blijven) geven in het landschap omdat informatiedeling ook voor deze organisaties van essentieel belang is en blijft. Daarnaast komt het voor dat entiteiten vallen onder verschillende sectoren en daardoor te maken hebben met meerdere sectorale CSIRT's. Tot slot zal voor de meeste sectorale CSIRT's met NIS2-doelgroepen gelden dat zij ook entiteiten bedienen die geen NIS2-verplichtingen hebben. De sectorale CSIRT's hebben aangegeven dat met deze aspecten in het landschap rekening moet worden gehouden, onder andere in relatie tot het bredere Landelijk Dekkend Stelsel[15].

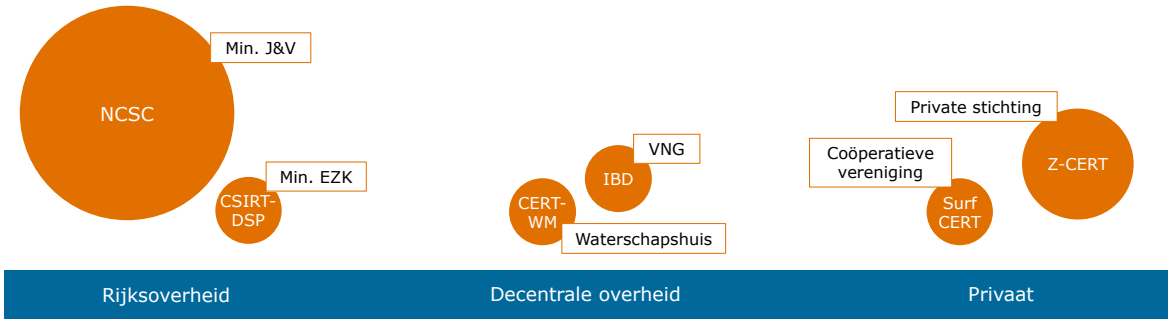
SAMENWERKING TUSSEN SECTORALE CSIRT'S

In de verkenningsgesprekken is ook gesproken over onderling samenwerking. Hieruit komt het beeld naar voren dat er met name veel bilaterale contacten zijn waarin informatie wordt uitgewisseld, samenwerkingen worden gerealiseerd en best practices worden gedeeld. Voor sommige sectorale CSIRT's is deze samenwerking heel beperkt, maar ook hierin zijn er verschillen. In een enkel geval zijn er afspraken over het overnemen van bepaalde taken buiten kantooruren, of het werken met liaisons die de samenwerking moeten bevorderen. Meer overkoepelende samenwerking is beperkt. Er zijn soms bredere overleggen met alle CSIRT's samen die als vrijblijvend ervaren worden.

[15] https://www.ncsc.nl/onderwerpen/samenwerkingspartner-worden/aansluiting-op-het-landelijk-dekkend-stelsel-lds

VERSCHIL IN GOVERNANCE TUSSEN CSIRT'S

Het eigenaarschap, de aansturing en financiering van sectorale CSIRT's is divers en het toevoegen van additionele wettelijke taken vormt daardoor een uitdaging.



Figuur 7 - Governance van sectorale CSIRT's

De twee in de Wbni genoemde CSIRT's, het NCSC en het CSIRT-DSP, zijn beiden CSIRT's die vallen binnen de aansturing van de Rijksoverheid. Dat is voor de andere vier sectorale CSIRT's niet het geval. Als in de huidige governance-structuur wettelijke taken die voortkomen uit bijvoorbeeld de NIS2 of andere sectorale richtlijnen moeten worden belegd bij deze organisaties dan zal dat op een andere manier moeten dan dit voor het NCSC en CSIRT-DSP mogelijk is. In onderstaande tabel wordt dit nader toegelicht.

Eigenaarschap	Sturing bij (additionele) wettelijke taken
Rijksoverheid	• In dit geval is rechtstreekse sturing mogelijk.
Decentrale overheid	• Hier zullen taken via getrapte sturing (via decentraal bestuur) bij de organen moeten worden belegd.
Privaat	• In dit geval zal er sturing moeten worden ingericht vergelijkbaar met het aansturen van een leverancier waarbij afspraken over taken, kwaliteitseisen, financiering en toezicht expliciet moeten worden vastgelegd[16]. • Een andere optie is het wijzigen van de governance structuur zodat voor (een deel van) de taken van de organisatie rechtstreekse sturing mogelijk wordt. Dat zou bijvoorbeeld kunnen via een Rechtspersoon met Wettelijke Taak (RWT)

Tabel 2 - Sturing bij het toekennen van wettelijke CSIRT-taken aan sectorale CSIRT's

Er zou vanwege de huidige governance-structuur in theorie een situatie kunnen ontstaan waarbij een al bestaande sectorale CSIRT die niet valt onder de Rijksoverheid wettelijke taken zoals die voortkomen uit de NIS2 niet op zich wil nemen. In dat geval moeten deze taken elders worden belegd. Het meest voor de

[16] Vanzelfsprekend moeten er ook bij de andere sectorale CSIRT's afspraken worden gemaakt over taken, kwaliteit en toezicht. In dit overzicht gaat het erom dat die afspraken geformaliseerd moeten worden via een leveranciersconstructie om sturing mogelijk te maken.

hand liggend is dan het NCSC/CSIRT-DSP. Als de bestaande sectorale CSIRT zijn overige taken continueert kan het in zo'n situatie gebeuren dat een sector in de praktijk bediend wordt door twee sectorale CSIRT's. Dit zorgt voor een onwenselijke situatie vanuit het perspectief van organisaties in zo'n sector waarvoor het dan onduidelijk wordt bij wie zij moeten zijn voor ondersteuning. Bij de keuze van een scenario voor het CSIRT-landschap is het verstandig om dit element mee te nemen.

CONCLUSIES BESTAANDE CSIRT-LANDSCHAP

Er zijn diverse conclusies te trekken uit de analyse van het bestaande CSIRT-landschap.

Sectorale CSIRT's voegen waarde toe aan het landschap

De sectorale CSIRT's hebben aangegeven veel waarde toe te voegen aan de doelgroeporganisaties die zij bedienen. Binnen de sectorale CSIRT's is een breed netwerk binnen de eigen sector is opgebouwd en inmiddels veel kennis is over sectorspecifieke systemen en processen. Daarmee kan snel en effectief geschakeld worden. Sommige CSIRT's zijn al vele jaren actief en hebben in die tijd veel vertrouwen bij hun doelgroep opgebouwd.

Er ontbreekt overzicht en samenhang in het CSIRT-landschap

Waar de sectorale CSIRT's de afgelopen jaren vooral de focus hebben gehad op de eigen doelgroep, is er een gemis op het goed en effectief laten functioneren van het netwerk van sectorale CSIRT's. Inmiddels is er sprake van een landschap met beperkte samenhang. Er ontbreken structuren die duidelijkheid geven over gewenste taken en taakvolwassenheid. Hoewel er soms gesproken wordt van een CSIRT-stelsel ontbreken belangrijke elementen om een stelsel effectief te laten functioneren op gebied van structuur, governance en kwaliteitstoezicht. Hierdoor is er in slechts beperkte mate overzicht en ontbreken mogelijkheden voor sturing. Daarnaast worden kansen gemist voor wat betreft onderlinge samenwerking en het verstevigen van het CSIRT-netwerk.

Nieuwe wetgeving vergroot de eisen aan het CSIRT-landschap

Nieuwe wetgeving (zoals de NIS2, maar ook sectorspecifieke richtlijnen) stelt richting de toekomst extra eisen en taken aan de sectorale CSIRT's en vraagt daarmee om het beter functioneren van het landschap (zie pagina 21). Er moet volgens de nieuwe NIS2-richtlijn nog beter informatie worden uitgewisseld én er is een enorme toename voorzien in doelgroepen die moeten worden bediend. Die toename van doelgroepen alleen is al een enorme extra uitdaging. Het is nodig om in het stelsel te borgen dat aan alle aanvullende eisen wordt voldaan. Het aanbrengen van meer structuur en betere samenwerking is daarmee niet alleen wenselijk, maar noodzakelijk.

De governance-inrichting van het huidige landschap bemoeilijkt het beleggen van wettelijke taken

Door eigenaarschap, de aansturing en financiering van sectorale CSIRT's divers is, vormt het toevoegen van additionele wettelijke taken daardoor een uitdaging. Als in de huidige governance-structuur wettelijke taken die voortkomen uit bijvoorbeeld de NIS2 of andere sectorale richtlijnen moeten worden belegd bij de bestaande sectorale CSIRT's die per ministeriële regeling zijn aangewezen, dan zal dat op een andere manier moeten dan voor het NCSC en CSIRT-DSP. In dat geval zijn er mogelijk aanpassingen nodig in de governance-inrichting.

NIS2-GEVOLGEN VOOR CSIRT-TAKEN

In december 2022 is de definitieve tekst gepubliceerd van de Security of Network and Information Systems Directive (NIS2)[17], de tweede versie van deze Europese richtlijn die nog meer en steviger eisen stelt aan de cybersecurity van organisaties in lidstaten dan zijn voorganger (de NIS-richtlijn). De NIS2 is een minimumharmonisatie richtlijn en beschrijft maatregelen die moeten zorgen voor een hoog gezamenlijk niveau van cybersecurity binnen de Europese Unie.

In de nieuwe richtlijn, die in oktober 2024 van kracht wordt via implementatie in nationale wetgeving[18], is een uitgebreid onderdeel opgenomen over de ondersteuning die lidstaten dienen te geven aan entiteiten die actief zijn in de essentiële en belangrijke sectoren. Dit moet gebeuren in de vorm van één of meerdere Computer Security Incident Response Teams (CSIRT's). Er is geformuleerd aan welke eisen deze CSIRT's moeten voldoen én welke taken zij tenminste op zich moeten nemen. Deze eisen en taken zijn voornamelijk omschreven in de artikelen 10 en 11 van de NIS2. In de bijlagen van de NIS2 is omschreven welke essentiële (bijlage I) en belangrijke (bijlage II) entiteiten binnen de reikwijdte van de richtlijn vallen.

VERPLICHTE CSIRT-TAKEN

De verplichte CSIRT-taken die door elke CISRT moeten worden uitgevoerd staan in de NIS2 voornamelijk omschreven in artikel 11. Vanuit de verkenning is geanalyseerd wat deze taken inhouden in termen van activiteiten. Een deel van de taken gaat over operationele activiteiten. Deze vinden plaats op de gebieden:

1. Monitoring. Hierbij gaat het over het voortdurend monitoren van dreigingen die sectoren kunnen raken:

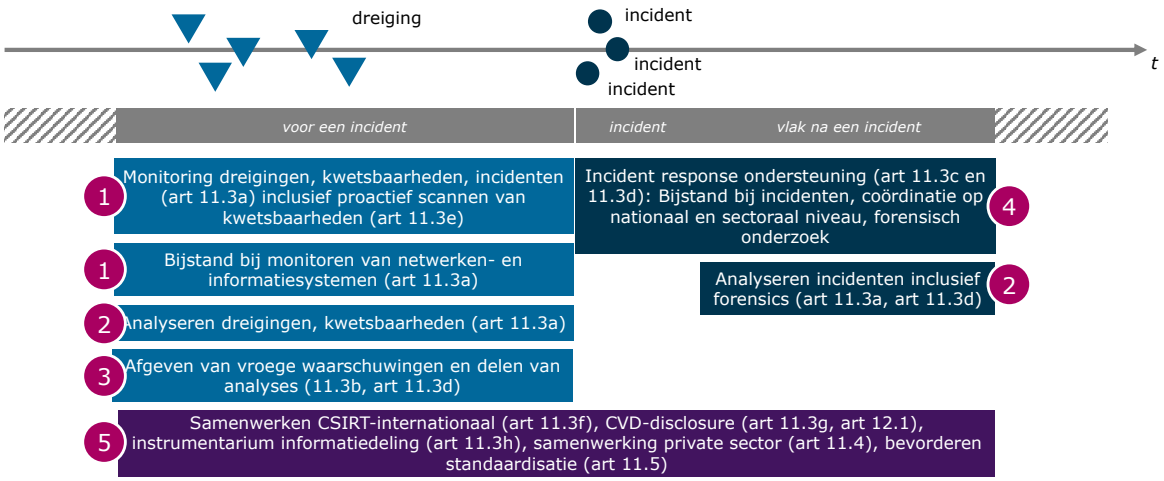
[17] https://eur-lex.europa.eu/legal-content/NL/TXT/HTML/?uri=CELEX:32022L2555
[18] In Nederland in de Wet Beveiliging Netwerken en Informatiesystemen – Wbni 2024. De eerste Wbni wordt op dat moment ingetrokken.

    a. Monitoren van kwetsbaarheden, inclusief proactief scannen (art. 11.3a, 11.3e)
    b. Monitoren van dreigingen (art. 11.3a)
    c. Monitoren van incidenten (art. 11.3a)
    d. Bijstand leveren aan het monitoren van netwerken en informatiesystemen (art. 11.3a)
2. Analyse. De informatie die via het monitoren wordt verkregen zal moeten worden geanalyseerd, bijvoorbeeld voor wat betreft de impact op de betreffende doelgroep:
    a. Analyse van kwetsbaarheden (art. 11.3a)
    b. Analyse van dreigingen (dreigingsanalyse, fenomeenanalyse) (art. 11.3a)
    c. Incident-analyse inclusief forensics (11.3a, 11.3d)
3. Meldingen. Belangrijke taak van de CSIRT's is natuurlijk het doen van meldingen aan de doelgroep over de actualiteiten:
    a. Het afgeven van vroege waarschuwingen en het delen van analyses (11.3b)
4. Incident response. Als er incidenten plaatsvinden binnen de sector heeft een CSIRT tot taak om ondersteuning te bieden:
    a. Het verlenen van bijstand bij incidenten (art. 11.3c)
    b. Coördinatie op nationaal en sectoraal niveau (art. 11.3c)
    c. Het bieden van ondersteuning bij forensics (art. 11.3d)

Naast deze operationele taken zijn er in artikel 11 van de NIS2 ook enkele regietaken gedefinieerd.

5. Regie en coördinatie:
    a. Deelnemen aan het internationaal CSIRT-netwerk (voor elke CSIRT die een sector bedient) (art. 11.3f)
    b. Gecoördineerd bekend maken van kwetsbaarheden (door 1 CSIRT per lidstaat) (art. 11.3g)
    c. Ontwikkelen van een instrumentarium voor informatiedeling (art. 11.3h)
    d. Bevorderen van samenwerken met de private sector (art. 11.4)
    e. Bevorderen van standaardisatie (art. 11.5)

Deze vijf categorieën van taken passen goed binnen de scope afbakening zoals deze in Figuur 3 is weergegeven. Dit is zichtbaar gemaakt in onderstaande figuur.



Figuur 8 - Mapping NIS2 op scope-afbakening CSIRT-taken

EISEN AAN LIDSTATEN EN CSIRT'S

Naast de taken die vereist zijn voor CSIRT's vanuit de NIS2 stelt de richtlijn ook eisen. Deels zijn dat eisen die gesteld worden aan de lidstaten, met name gericht op het creëren van de juiste randvoorwaarden. Deels betreft dit eisen aan de CSIRT's zelf. In onderstaande tabel zijn de belangrijkste eisen op een rijtje gezet.

Eisen aan de lidstaten	Eisen aan CSIRT's
1. Elke lidstaat wijst 1 of meer CSIRT's aan (art 10.1) 2. Lidstaten dragen zorg voor voldoende middelen (art 10.2) 3. Lidstaten moeten zorgen voor beschikbaarheid van passende infrastructuur voor veilige informatie-uitwisseling (art 10.3) 4. Lidstaten zorgen voor goede samenwerking in het (internationale) CSIRT-netwerk (art 10.6) 5. Lidstaten informeren de Commissie over de wijze van invulling van de CSIRT-taken (art 10.9) 6. Bewerkstelligen van samenwerking en informatie-uitwisseling in nationaal verband (art 13) 7. Faciliteren van vrijwillige meldingen over cyberdreigingen en bijna-incidenten (art 30.1)	1. Garantie op hoge mate van beschikbaarheid van CSIRT's (art 11.1a) 2. CSIRT's moeten gebruik maken van beveiligde locaties (art 11.1b) 3. CSIRT's moeten een systeem hebben voor het beheren en routeren van verzoeken (art 11.1c) 4. Er moet voldoende personeel beschikbaar zijn (art 11.1d) 5. De continuïteit moeten worden gewaarborgd door redundantie (IT-systemen en werkruimte) (art 11.1e) 6. CSIRT's moeten de mogelijkheid hebben om deel te nemen aan internationale samenwerkingsnetwerken (art 11.1f, art 10.7 en art 10.8) 7. CSIRT's werken samen en wisselen indien nodig informatie uit (art 10.4) 8. CSIRT's nemen deel aan intercollegiale toetsingen (art 10.5) 9. Onverwijld bijstand verlenen bij significante incidenten (art 23)

Tabel 3 - NIS2 eisen aan lidstaten en CSIRT's

ENTITEITEN DIE ONDER DE NIS2 VALLEN

Naast de bijstand die lidstaten moeten inrichten door middel van één of meerdere CSIRT's schrijft de NIS2 voor welke sectoren de nieuwe richtlijn gaat gelden. Deze zijn opgesomd in Bijlage I (voor de essentiële entiteiten) en Bijlage II (voor de belangrijke entiteiten). De NIS2 gaat gelden voor entiteiten binnen deze sectoren met meer dan 50 medewerkers en een omzet van meer dan € 10M. Entiteiten die niet aan deze criteria voldoen kunnen alsnog door de Rijksoverheid worden aangewezen als essentieel of belangrijk.

Er wordt al geruime tijd onderzoek gedaan naar hoeveel entiteiten in Nederland straks moeten gaan voldoen aan de nieuwe regels. Op het moment van schrijven van dit rapport zijn de cijfers hierover helaas nog steeds onduidelijk.

In 2020 heeft het CBS een onderzoek uitgevoerd naar het aantal entiteiten dat binnen de NIS2 zou gaan vallen en kwam toen op een eerste inschatting van 4.355 entiteiten[19]. Nader onderzoek vanuit de verschillende vakdepartementen lijkt erop te wijzen dat het aantal entiteiten in de praktijk veel hoger ligt. Zij schatten dat er in totaal tussen de 10.600 en 11.600 entiteiten te maken zullen krijgen met de nieuwe wetgeving. Met uitzondering van het ministerie van VWS (die net als het CBS ongeveer 1.500 entiteiten heeft berekend) betekent dit voor de andere sectoren een fors hogere inschatting[20]. In Tabel 4 zijn de inschattingen van de vakdepartementen weergegeven.

Vakdepartement	Verwachte # entiteiten i.k.v. NIS2
Economische Zaken en Klimaat	3.000
Binnenlandse Zaken en Koninkrijksrelaties	500
Infrastructuur en Waterstaat	4.500
Volksgezondheid, Welzijn en Sport	1.500 – 2.000
Landbouw, Natuur en Voedselkwaliteit	1.000 – 1.500
Totaal	10.600 – 11.600

Tabel 4 - Inschatting vakdepartementen reikwijdte NIS2[21]

[19] https://www.cbs.nl/nl-nl/maatwerk/2022/30/sectoren-die-onder-de-nib2-richtlijn-vallen-2020
[20] Tijdens de verkenning is bij het ministerie van Economische Zaken en Klimaat een nadere onderbouwing ingezien van de genoemde cijfers. Het ministerie van Volksgezondheid, Welzijn en Sport volgt nagenoeg de CBS-berekeningen. Bij andere vakdepartementen vinden nog berekeningen plaats (bijvoorbeeld voor het duiden van dubbele tellingen tussen de vakdepartementen).
[21] Nota Update implementatiefase Versterkte Aanpak Vitaal (incl. planning + werkwijze) d.d. 15 november 2022

In Tabel 5 staat een samenvatting van het onderzoek van het CBS uit 2020. Omdat entiteiten in sommige sectoren binnen de reikwijdte van meerdere vakdepartementen vallen, is er sprake van enige overlap.

Sector	Middenbedrijf	Grootbedrijf	Totaal
Energie	115	35	150
Vervoer	30	80	115
Bankwezen	20	45	70
Infrastructuur financiële markt	x	x	x
Gezondheidszorg	615	885	1.505
Drinkwater	5	5	10
Afvalwater	5	5	10
Digitale infrastructuur	10	60	65
Overheidsdiensten	220	245	465
Ruimtevaart	5	5	10
Post- en koeriersdiensten	10	15	25
Afvalstoffenbeheerder	15	80	95
Vervaardiging, productie en distributie van chemische stoffen	45	160	200
Productie, verwerking en distributie van levensmiddelen	165	805	965
Vervaardiging	115	595	705
Digitale aanbieders	5	15	20
Totaal			4.355

Tabel 5 - Sectoren die volgens het CBS onder de NIS2 vallen[22]

Bestudering van beide overzichten met cijfers over de NIS2-reikwijdte geeft een aantal extra inzichten:

1. De huidige sectorale CSIRT's bedienen slechts een deel van de entiteiten die binnen de reikwijdte van de NIS2 gaan vallen:

[22] https://www.cbs.nl/nl-nl/maatwerk/2022/30/sectoren-die-onder-de-nib2-richtlijn-vallen-2020

a. Voor sommige sectoren is er nog geen sectorale CSIRT aangewezen voor de uit te voeren taken. Het onderzoek van het CBS laat zien dat dit in elk geval voor twee grote sectoren het geval is, namelijk de *levensmiddelenindustrie* en de *maakindustrie*.
b. Sommige doelgroepen van bestaande CSIRT's worden substantieel groter doordat als gevolg van NIS2 meer entiteiten aan de bestaande doelgroep moeten worden toegevoegd.

2. Het aantal entiteiten dat ondersteund moet worden vanuit wettelijke verplichtingen neemt fors toe ten opzichte van de NIS.

Het is van belang in verband met de implementatie van de NIS2, maar ook vanwege duidelijkheid voor de entiteiten én sectorale CSIRT's om op korte termijn helderheid te brengen in de keuzes op dit gebied. De aangewezen CSIRT's voor de essentiële en belangrijke sectoren moeten halverwege oktober 2024 aan de eisen uit de NIS2 voldoen en de verplichte taken moeten kunnen uitvoeren.

SECTORSPECIFIEKE REGELGEVING

Behalve de NIS2 zijn er nog andere sectorspecifieke richtlijnen in ontwikkeling. Op dit moment betreft dit de Digital Operational Resilience Act (DORA) die toeziet op extra maatregelen in de financiële sector en de Network Code on Cybersecurity (Netcode) voor de elektriciteitssector, maar mogelijk komen hier in de toekomst nog andere richtlijnen bij. Telkens wanneer een nieuwe cybersecurityrichtlijn wordt vastgesteld moet worden vastgesteld in hoeverre deze voorschriften heeft op gebied van sectorale CSIRT's, hun taken en de eisen die er aan CSIRT's worden gesteld.

In dit hoofdstuk wordt een overzicht gegeven van de DORA en de Netcode en de implicaties die deze richtlijnen hebben voor het CSIRT-landschap.

DIGITAL OPERATIONAL RESILIENCE ACT (DORA)

De Digital Operational Resilience Act[23] (DORA) ziet toe op extra cybersecuritymaatregelen in de financiële sector (voor bijvoorbeeld banken, verzekeraars en handelsplatformen). Deze Europese verordening, die op 28 november 2022 is aangenomen en sinds 16 januari 2023 in werking, schrijft maatregelen voor om de digitale weerbaarheid van financiële instellingen te vergroten. De verordening vindt zijn oorsprong in initiatieven van Europese toezichthouders en ondernemingen hebben tot 17 januari 2025 om aan de verplichtingen van DORA te voldoen.

DORA verplicht de meeste financiële ondernemingen om maatregelen te nemen voor het verhogen van de cyberweerbaarheid op gebied van ICT-risicomanagement, ICT-gerelateerde incidenten, periodieke testen van digitale operationele weerbaarheid en de beheersing van risico's bij uitbesteding aan ICT-dienstverleners. Ook is uitgewerkt hoe informatie over cyberdreigingen kan worden uitgewisseld.

[23] https://eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=CELEX:32022L2556

In DORA zijn geen bepalingen opgenomen die lidstaten verplichtingen opleggen in het kader van CSIRT-ondersteuning. DORA heeft daarmee geen impact op het CSIRT-landschap in Nederland.

NETWORK CODE ON CYBERSECURITY (NETCODE)

Op dit moment wordt er in Europees verband gewerkt aan de ontwikkeling van de *Network Code on Sector-specific Rules for Cybersecurity Aspects of Cross-border Electricity Flows* (Netcode). Deze cybersecuritycode heeft als doel om bij te dragen aan het verhogen van de cyberweerbaarheid van elektriciteitssystemen in Europa. Op het moment van schrijven van dit rapport is de Netcode in de fase van een vergaand concept, maar nog niet definitief vastgesteld[24]. De definitieve Netcode wordt naar verwachting van kracht rond de zomer van 2023. De bepalingen uit de Netcode zullen na 12 maanden (naar verwachting in de zomer van 2024) operationeel moeten zijn.

De Netcode bevat voorschriften over verschillende aspecten van cybersecurity voor de elektriciteitssector, bijvoorbeeld op gebied van:

- Een gezamenlijk raamwerk om maatregelen te standaardiseren
- Inrichting van governance van cybersecurity
- Een proces van risicobeheer voor de gehele keten
- Informatiedeling
- Incident respons en crisismanagement
- Een kader voor het oefenen met incidenten
- Regels voor beveiligen van informatie-uitwisseling
- Een raamwerk voor monitoren, rapportages en het uitvoeren van benchmarks.

In tegenstelling tot de DORA geeft de Netcode wel voorschriften over de rol van een CSIRT die ondersteuning moet bieden aan de sector. Er moet volgens de Netcode een *National Competent Authority* (NCCS-NCA) worden aangewezen die belast is met de verantwoordelijkheid om de Netcode in een lidstaat uit te voeren. In Nederland is de NCCS-NCA het ministerie van Economische Zaken en Klimaat. De verantwoordelijke toezichthouder (in de Netcode CS-NCA genoemd, *competent authority for cybersecurity*) is in Nederland de Rijksinspectie Digitale Infrastructuur (RDI). De NCCS-NCA heeft (conform art. 5.3) de bevoegdheid om bepaalde taken te delegeren aan andere organisaties binnen de lidstaat. Dit geldt ook voor de gedefinieerde CSIRT-taken. Als de sectorale CSIRT en de NCA twee verschillende organisaties zijn, stelt de Netcode dat zij nauw moeten samenwerken.

De taken voor een sectoraal CSIRT die in het huidige concept van de Netcode staan geformuleerd zijn:

- Het ontvangen van meldingen over kwetsbaarheden van kritieke dienstverleners (art. 30). Feitelijk is dit een taak die in de Netcode aan de NCCS-NCA wordt

[24] De huidige draft d.d. 6 juli 2022: https://www.acer.europa.eu/sites/default/files/documents/Recommendations/Revised%20Network%20Code%20on%20Cybersecurity%20%28NCCS%29_1.pdf

toegewezen, maar in de praktijk zal de sectorale CSIRT hierin een belangrijke rol spelen.
- Het ondersteunen van de NCCS-NCA bij het uitvoeren van risicoanalyses (art. 32)
- Informatie analyseren en delen bij cybersecurity incidenten, zero-day kwetsbaarheden en cyberdreigingen (art. 40)
- Het bieden van ondersteuning bij de ontwikkeling van een *cybersecurity incidents classification scale* (art. 40)
- Ondersteuning bieden aan *high-impact* en *critical-impact* entiteiten om de capaciteiten te ontwikkelen die nodig zijn om gedetecteerde incidenten af te handelen (art. 42).
- Ondersteuning bieden aan *high-impact* en *critical-impact* entiteiten om de capaciteiten te ontwikkelen voor de detectie en mitigatie van cybersecuritycrises die een bredere impact hebben op de keten (art 43).
- Het ondersteunen van de *national competent authority* voor risicoprocessen (RP-NCA) bij het organiseren van cybersecurityoefeningen (art 46).

De Netcode is een specificatie van de NIS2 voor de elektriciteitssector en stelt op sommige onderdelen aanvullende (meer specifieke of scherpere) eisen, bijvoorbeeld op gebied van termijnen voor het melden van incidenten en het doordelen van informatie door een CSIRT. De voornaamste impact van de Netcode op sectorale CSIRT's, aanvullend op wat vanuit de NIS2 al verplicht gaat worden, lijkt op dit moment dat er ondersteuning moet worden geboden bij het opbouwen van capaciteiten van *high-impact* en *critical-impact* entiteiten. Uit de tekst van de Netcode blijkt nog niet heel duidelijk op welk moment dat moet gebeuren (voor, tijdens en/of na een incident). Deels overlappen de activiteiten (zoals bijvoorbeeld gezamenlijk oefenen en het ontvangen van informatie over kwetsbaarheden).

Net als bij de NIS2 moet nog worden bepaald welke entiteiten binnen de reikwijdte van de Netcode zullen gaan vallen. Vanuit de elektriciteitssector is de verwachting dat er veel overlap zal zijn met entiteiten die onder de NIS2 gaan vallen. De RDI zal in Nederland belast worden met het aanwijzen van entiteiten voor de Netcode binnen 6 maanden na inwerkingtreding. Of de overlap volledig zal zijn, is nu nog niet duidelijk. Er moet ook rekening worden gehouden met de mogelijkheid dat er entiteiten zijn die wel onder de Netcode gaan vallen, maar niet onder de NIS2. Voor deze entiteiten zal de impact aanzienlijk groter zijn en er moet worden gewaarborgd dat ook zij bediend worden door een (sectorale) CSIRT.

Op dit moment wordt gewerkt aan een volgend concept van de Netcode en is het mogelijk dat verschillende artikelen, waaronder artikelen die impact hebben op de activiteiten van een CSIRT, nog kunnen wijzigen.

In de verdere analyse zijn daarom de sectorale regelingen in algemene zin meegenomen bij de uitwerking. Pas als de Netcode definitief is, is het mogelijk een finale analyse te maken om te bekijken of er nog extra aanvullende impact zal zijn.

BESTAANDE CSIRT-FRAMEWORKS

Uit de analyse van het huidige CSIRT-landschap is gebleken dat overzicht en samenhang in het CSIRT-landschap ontbreekt. Een mogelijkheid voor het aanbrengen van meer structuur is het toepassen van geaccepteerde standaarden. Op basis van open bronnenonderzoek en gesprekken met specialisten uit de sectorale CSIRT's is onderzocht welke actuele frameworks binnen het CSIRT-domein voorhanden zijn, in hoeverre deze breed (internationaal) worden geaccepteerd en toegepast en of deze mogelijk bruikbaar zijn binnen het Nederlandse CSIRT-stelsel.

Er is helaas geen framework voorhanden dat voorziet in het opbouwen van een samenhangend nationaal stelsel van sectorale CSIRT's dat als basis kan dienen voor een CSIRT-stelsel in Nederland. Er zou houvast kunnen worden ontleend aan de wijze waarop het EU CSIRT's Network[25] is ingericht voor wat betreft de onderlinge samenwerking tussen sectorale CSIRT's.

Wel zijn er frameworks die ondersteuning kunnen bieden voor delen van het CSIRT-landschap. Specifiek gaat het om:

1. Het FIRST CSIRT Services Framework[26] dat gebruikt kan worden voor een eenduidige afbakening van kerntaken van specifieke sectorale CSIRT's
2. Het ENISA CSIRT Maturity Framework[27], gebaseerd op het SIM3-volwassenheidsmodel dat gebruikt kan worden voor het meten van taakvolwassenheid van CSIRT's

Helaas is er (nog) geen framework dat voorziet in structuur voor de taken van een nationale CSIRT dat coördinerende taken heeft over het stelsel heen.

[25] https://csirtsnetwork.eu/
[26] https://www.first.org/standards/frameworks/csirts/csirt_services_framework_v2.1
[27] https://www.enisa.europa.eu/publications/enisa-csirt-maturity-framework/@@download/fullReport

In dit hoofdstuk geven we een toelichting op de twee genoemde frameworks en de toepasbaarheid ervan in de Nederlandse context.

FIRST CSIRT SERVICES FRAMEWORK

Het FIRST CSIRT Services Framework beschrijft op een gestructureerde manier welke diensten en functies passen bij een CSIRT. Het framework is ontwikkeld door experts vanuit de FIRST community met support van de Task Force CSIRT[28] (TF-CSIRT) en de International Telecommunications Union[29] (ITU). Het framework is bedoeld om ondersteuning te bieden bij het verbeteren van CSIRT-werkzaamheden. Het framework beschrijft mogelijke taken die een CSIRT op zich kan nemen, en heeft geen dwingend karakter, maar wordt gezien als leidraad bij het opzetten en verder ontwikkelen van CSIRT's. Het voorziet in standaard terminologie die binnen de CSIRT-community kan worden gebruikt en helpt dus bij standaardisatie en vergelijken van werkzaamheden.

Het framework bestaat uit vijf hoofdcategorieën van CSIRT-taken waarbinnen telkens een aantal subtaken is gedefinieerd. Deze zijn in Figuur 4 weergegeven. In totaal zijn er in detail 21 taken binnen dit framework beschreven.

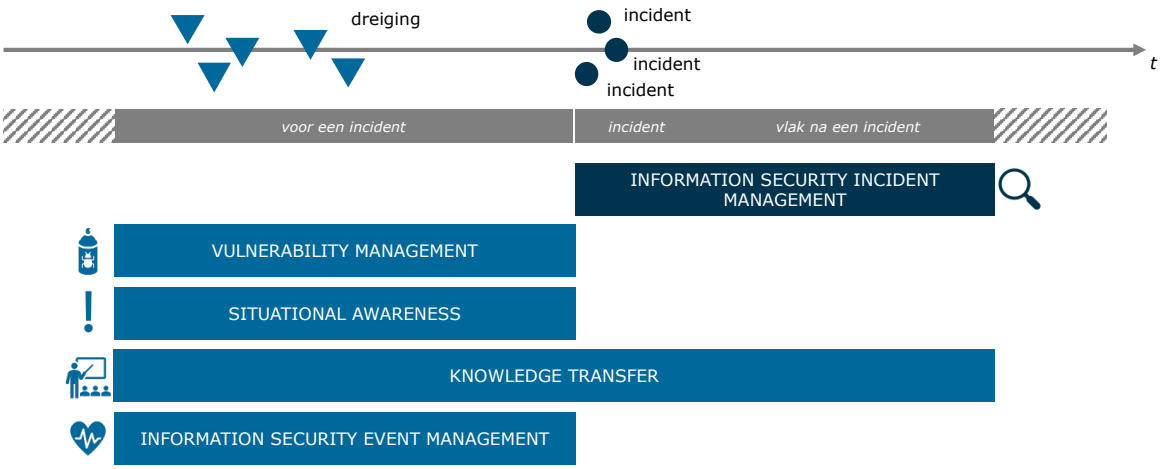
INFORMATION SECURITY INCIDENT MANAGEMENT	VULNERABILITY MANAGEMENT	SITUATIONAL AWARENESS	KNOWLEDGE TRANSFER	INFORMATION SECURITY EVENT MANAGEMENT
1. Information Security Incident Report Acceptance 2. Information Security Incident Analysis 3. Artefact and Forensic Evidence Analysis 4. Mitigation and Recovery 5. Information Security Incident Coordination 6. Crisis Management Support	7. Vulnerability Discovery/Research 8. Vulnerability Report Intake 9. Vulnerability Analysis 10. Vulnerability Coordination 11. Vulnerability Disclosure 12. Vulnerability Response	13. Data Acquistion 14. Analysis and Synthesis 15. Communication	16. Awareness Building 17. Training and Education 18. Exercises 19. Technical and Policy Advisory	20. Monitoring and Detection 21. Event Analysis

Figuur 9 – Overzicht van taken in het FIRST CSIRT Services Framework

Het FIRST CSIRT Services Framework is breed geaccepteerd en heeft een heldere indeling van taken en hoofdcategorieën. Ook ENISA ziet dit framework als een goede manier om de taken van een CSIRT af te bakenen en verwijst er zelf actief naar in haar eigen documenten en adviezen[30]. Door gebruik van dit framework wordt enerzijds aangesloten bij de twee grote internationale CSIRT-communities FIRST en TF-CSIRT, maar ook bij ENISA.

Daarnaast past het framework ook goed binnen de scope-afbakening die binnen deze verkenning is aangebracht. Zie daarvoor Figuur 10.

[28] https://tf-csirt.org/
[29] https://www.itu.int/
[30] https://www.enisa.europa.eu/publications/how-to-set-up-csirt-and-soc



Figuur 10 - Mapping CSIRT Service Framework op scope-afbakening CSIRT-taken

Om het framework goed bruikbaar te maken in de Nederlandse context is het van belang dat ook de verplichte NIS2-taken goed passen binnen de context van dit framework. Er is daarom gekeken hoe de NIS2-taken zich relateren aan de taakgebieden zoals die omschreven zijn in dit framework. Daarin is vastgesteld dat de kern van de NIS2-taken met name binnen de eerste drie taak-categorieën passen. Zie daarvoor Figuur 11. Er is een kleine link met de vijfde categorie: Information Security Event Management. In het framework gaat dit deel voornamelijk over het inrichten van netwerk monitoring activiteiten. In veel gevallen worden deze nu niet vanuit sectorale CSIRT's uitgevoerd. De NIS2 schrijft niet voor dat CSIRT's zelf monitoren, maar wel dat er bijstand moet worden verleend, bijvoorbeeld in de vorm van het aanleveren van indicators of compromise (IOC's).

INFORMATION SECURITY INCIDENT MANAGEMENT	VULNERABILITY MANAGEMENT	SITUATIONAL AWARENESS	KNOWLEDGE TRANSFER	INFORMATION SECURITY EVENT MANAGEMENT
1. Information Security Incident Report Acceptance 2. Information Security Incident Analysis 3. Artefact and Forensic Evidence Analysis 4. Mitigation and Recovery 5. Information Security Incident Coordination 6. Crisis Management Support	7. Vulnerability Discovery/Research *8. Niet: Vulnerability Report Intake* *9. Niet: Vulnerability Analysis* 10. Vulnerability Coordination 11. Vulnerability Disclosure 12. Vulnerability Response	13. Data Acquistion 14. Analysis and Synthesis 15. Communication	*16. Niet: Awareness Building* *17. Niet: Training and Education* *18. Niet: Exercises* *19. Niet: Technical and Policy Advisory*	20. Beperkt: Monitoring and Detection (bijv. IOC's leveren) *21. Niet: Event Analysis*

Figuur 11 - Mapping van NIS2-taken op CSIRT Services Framework

Uit deze analyse wordt tot de conclusie getrokken dat het CSIRT Services Framework een goede kapstok biedt voor de afbakening van de taken van een sectorale CSIRT, zowel als het gaat om verplichte taken vanuit de NIS2, als bij een vrijwillige bredere set aan taken die de CSIRT kan oppakken. Het framework is daarmee breder dan wat vereist wordt vanuit de NIS2 en biedt daarmee voldoende ruimte om ook bredere taken van CSIRT's mee af te bakenen.

ENISA CSIRT MATURITY FRAMEWORK

Voor het meten van taakvolwassenheid van een CSIRT is er inmiddels een breed geaccepteerd model voor taakvolwassenheid voorhanden: het Security Incident Management Maturity Model (SIM3)[31]. Dit model, ontwikkeld door de Open CSIRT Foundation maakt gebruikt van in totaal 45 parameters om de volwassenheid van een CSIRT te meten. Deze zijn ingedeeld in 4 categorieën:

1. O: Organisational (11). De basisaspecten van een CSIRT (zoals mandaat, setup en diensten)
2. H: Human (7). Elementen die gerelateerd zijn aan de staf (zowel inhoudelijke medewerkers als ondersteuning)
3. T: Tools (10). Tools en technologie die door het CSIRT wordt ingezet (van lijsten, Excel sheets, tot geavanceerde tools)
4. P: Processes (17). Dit gaat in op de set met processen die goed moeten zijn georganiseerd om het CSIRT goed te laten functioneren. Processen is daarbij breed gedefinieerd.

CSIRT's kunnen op basis van een assessment hun volwassenheidsniveau bepalen waarbij de scores variëren van 0 (laagste niveau) tot 4 (hoogste niveau). Het is niet aannemelijk dat CSIRT's meteen de maximale score voor alle parameters kunnen bereiken. Dit zullen zij vaak incrementeel doen, bijvoorbeeld aan de hand van een Plan-Do-Check-Act (PDCA) cyclus. In meerdere iteraties kan dan een steeds hoger niveau worden behaald.

Het SIM3 model wordt gebruikt door TF-CSIRT/TI voor de (optionele) certificering van haar leden en FIRST overweegt om delen van SIM3 te gebruiken in het lidmaatschapsproces. Ook is SIM3 de basis van het volwassenheidsmodel dat ENISA heeft ontwikkeld voor EU nationale CSIRT's (het ENISA CSIRT Maturity Framework), dat vervolgens weer de basis vormt van het model dat de GFCE-community wereldwijd gebruikt.

In het ENISA CSIRT Maturity Framework worden de waarden van de SIM3-parameters aan drie niveaus gekoppeld: *basic*, *intermediate* en *advanced*. Daarmee maakt ENISA in feite het SIM3-model goed hanteerbaar in de praktijk doordat het zicht geeft op waar de focus voor ontwikkeling van een CSIRT zou moeten liggen. Overigens is er formeel gezien nog een 4^{e} niveau, genaamd *under-basic*, voor CSIRT's die op enkele parameters nog niet het basic-niveau hebben bereikt en deze indeling willen gebruiken voor het onderbouwen van het inzetten van meer resources.

De overige drie niveaus worden als volgt gedefinieerd (zie voor nadere toelichting en gewenste score per parameter het document van Enisa[32]):

[31] https://opencsirt.org/csirt-maturity/sim3-and-references/
[32] https://www.enisa.europa.eu/publications/enisa-csirt-maturity-framework/@@download/fullReport

1. Basic. Teams hebben een goede basis met betrekking tot mandaat en inrichting. Ze zijn bereikbaar en hebben een functioneel proces voor incident behandeling. De meeste organisatorische parameters moeten al een behoorlijk volwassenheidsniveau hebben van tenminste 3. De overige parameters hoeven nog maar een score van 1 of 2 te hebben.
2. Intermediate. Dit bouwt voort op Basic en richt zich met name op de controls m.b.t. hoger management en juridisch kader. De organisatorische parameters moeten toenemen naar niveau 4. Andere parameters ontwikkelen incrementeel mee.
3. Advanced. Op dit niveau scoren organisatorische parameters op niveau 4 en de overige voornamelijk op 3 (enkele op niveau 4). Op dit niveau gaat het niet alleen meer om samenwerken, maar om op hoog professioneel niveau omgaan met incidenten, kwetsbaarheden en dreigingsinformatie.

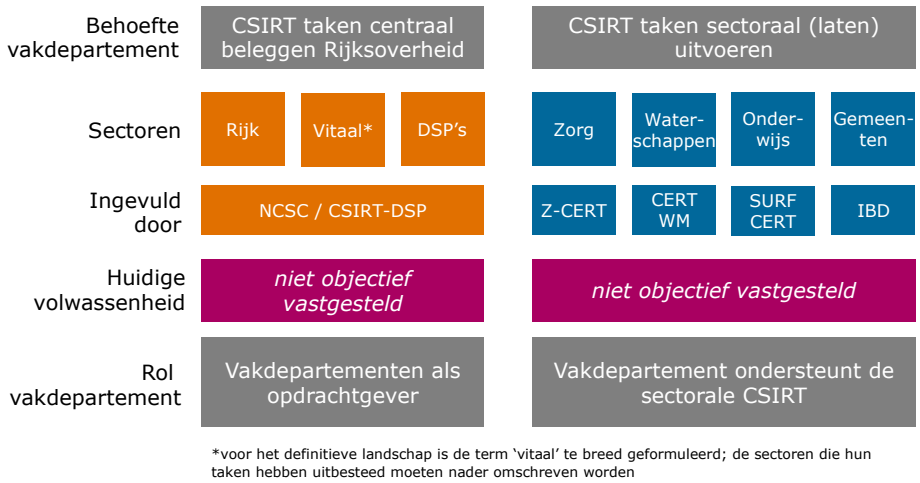
Het EU CSIRTs Network[33] moedigt zijn leden aan tenminste het intermediate niveau van het ENISA CSIRT Maturity Framework van de aangesloten CSIRT's te behalen.

Gezien de brede acceptatie van SIM3, de praktische toepasbaarheid in drie niveaus van het ENISA CSIRT Maturity Framework en de bredere internationale adoptie van dit model in het Global CSIRT Maturity Framework is het ENISA CSIRT Maturity Framework op basis van SIM3 binnen de Nederlandse context goed bruikbaar voor het meten van taakvolwassenheid van sectorale CSIRT's.

[33] https://csirtsnetwork.eu/

VISIE OP GEWENST CSIRT-LANDSCHAP

In Nederland zijn vanuit verschillende behoeften zes sectorale CSIRT's ontstaan. In geval van NCSC/CSIRT-DSP[34] fungeren de vakdepartementen (informeel) als opdrachtgever, hoewel deze rol beperkt is ingevuld in de praktijk. In geval van de overige vier sectorale CSIRT's vallen deze niet onder de Rijksoverheid, maar worden deze gesteund vanuit de betreffende vakdepartementen[35]. De sectorale CSIRT's maken (onder andere) deel uit van het Landelijk Dekkend Stelsel (LDS). Uit de verkenningsgesprekken blijkt dat alle CSIRT's onderling (relevante) informatie uitwisselen over actuele dreigingen.



Figuur 12 - Huidige landschap met sectorale CSIRT's

[34] Vanwege de ophanden zijnde integratie tussen NCSC en CSIRT-DSP wordt in dit rapport gesproken over 'NCSC/CSIRT-DSP'
[35] In sommige gevallen betekent dit financiële steun, in andere situaties (ook) inhoudelijke steun voor het initiatief

De komst van de NIS2 heeft een grote impact op de bestaande en (eventueel) toekomstige CSIRT's. Veel entiteiten die bediend worden door de huidige sectorale CSIRT's moeten gaan voldoen aan de NIS2 en moeten een sectorale CSIRT krijgen toebedeeld die hen ondersteuning moet gaan bieden. Dit betekent dat een (groot) deel, maar wellicht niet alle van de huidige sectorale CSIRT's te maken krijgen met de NIS2 en mogelijk zelf moeten gaan voldoen aan de eisen die de NIS2 aan CSIRT's stelt en vast omschreven taken uit de richtlijn gaan uitvoeren. Er zijn extra taken in het kader van regie en coördinatie die de komst van een nationale CSIRT wenselijk maken[36]. Er moet voldoende aandacht gaan naar taakvolwassenheid van CSIRT's én de CSIRT's moeten onderling goed samenwerken. Tot slot is het nodig dat in het CSIRT-stelsel naast de NIS2-entiteiten ook CSIRT-ondersteuning voor de overige entiteiten voldoende aandacht krijgt.

Behalve de NIS2 zijn er nog andere sectorspecifieke richtlijnen in ontwikkeling. Op dit moment betreft dit de DORA en de Netcode, maar mogelijk komen hier in de toekomst nog andere richtlijnen bij. Deze richtlijnen hebben mogelijk een impact op het CSIRT-stelsel.

Het kabinet heeft daarnaast in de NLCS enkele strategische kaders bepaald:
- Centraal waar het kan, decentraal als het moet
- Heldere aanspreekpunten bij de overheid voor organisaties
- Effectieve en efficiënte inzet van mensen, middelen en expertise
- Het NCSC zal zich door ontwikkelen tot een nationale CSIRT

Dit alles werpt de vraag op of er veranderingen nodig zijn ten aanzien van de bestaande Nederlandse CSIRT's, en zo ja welke. Gezien het feit dat eventuele veranderingen alle bestaande en (eventuele) toekomstige CSIRT's zouden kunnen raken, is een aanpalende vraag of de huidige situatie met een zestal CSIRT's in Nederland baat heeft bij een doorgroei naar een stelsel van CSIRT's, waarbij informatie-uitwisseling, taakeffectiviteit en governance op een meer geïntegreerde wijze tot stand komen. De omvorming van de bestaande situatie met zes afzonderlijke CSIRT's naar een toekomstig stelsel kan eveneens een positieve bijdrage leveren aan kennisuitwisseling, het delen van schaarse menskracht en middelen en het vergroten van de efficiëntie en slagkracht in geval van incidenten. Meer samenhang en meer structuur kunnen bovendien leiden tot duidelijkheid in termen van taakstelling en verantwoordelijkheden. Dit is van belang voor de CSIRT's zelf, maar ook voor de sectoren die zij bedienen en de partners met wie zij in de cybersecurity-weerbaarheidsketen samenwerken.

In het eerste deel van dit rapport is ingegaan op het feit dat de bestaande CSIRT's in Nederland geconfronteerd worden met allerlei veranderingen in het licht van

[36] De NIS2 schrijft voor dat alle lidstaten tenminste één sectorale CSIRT moeten hebben (artikel 10). Daarnaast moet er, om snelle en effectieve internationale samenwerking te waarborgen, een netwerk van "nationale CSIRT's" (artikel 15, lid 1) in Europa worden gecreëerd. Dit hoeft niet per se een overkoepelende CSIRT voor elke lidstaat te zijn. Echter, gezien de taakstelling van de CSIRT's in dit Europese netwerk (artikel 15, lid 3), o.a. op het gebied van informatie-uitwisseling en interoperabiliteit, is het waarschijnlijk dat lidstaten één (nationale) CSIRT aanwijzen als overkoepelend.

aankomende wet- en regelgeving, en welke implicaties dit heeft. Die veranderingen vragen om een integrale blik op het huidige en toekomstige landschap van CSIRT's, hetgeen een stelselaanpak rechtvaardigt. Ook is in kaart gebracht welke frameworks voorhanden zijn bij het verder structureren het CSIRT-stelsel. In dit tweede deel van het rapport wordt ingegaan op de vraag: hoe zou een stelsel van CSIRT's in Nederland eruit kunnen zien, en welke randvoorwaarden zijn daarbij van belang?

UITGANGSPUNTEN CSIRT-STELSEL

Op basis van de analyse van de bestaande situatie (zie pagina 19) en de aankomende verplichtingen, waaronder die vanuit de NIS2 (zie pagina 21 en pagina 27), is de overtuiging ontstaan dat een herontwerp van het stelsel niet alleen wenselijk is, maar noodzakelijk. Het advies is daarom om het stelsel te gaan voorzien van meer structuur en samenhang en daarbij rekening te houden met de volgende onderscheidende uitgangspunten:

1. NIS2 en andere richtlijnen:
    a. De komst van NIS2 en andere wet- en regelgeving zorgt voor stringente eisen op gebied van CSIRT-taken, taakvolwassenheid en samenwerking.
    b. Gezien de reikwijdte van de toepassing van de NIS2 is haalbaarheid van de uitvoering van de CSIRT-taken belangrijk.
2. NLCS:
    a. De NLCS stelt dat taken centraal worden belegd als het kan en decentraal als het moet.
    b. Daar waar sectorale functionaliteit zich langere tijd met hoogstaande kwaliteit bewezen heeft, dient een afweging gemaakt te worden tussen de voor- en nadelen van centralisatie.
    c. Voor de doelgroepen van de CSIRT's is het belangrijk dat zij terecht kunnen bij één loket voor hun sectorale CSIRT-dienstverlening[37].
    d. Het is van belang om in het stelsel effectief om te gaan met schaarse menskracht en middelen.
3. Er is in het stelsel ruimte voor CSIRT's die een doelgroep bedienen die niet onder de sectoren zoals genoemd in de NIS2 (of andere richtlijnen) vallen. Deze CSIRT's worden in het rapport verder 'vrijwillige CSIRT's' genoemd.
4. Het is van belang een stelsel te ontwikkelen waarvan de complexiteit zo laag mogelijk is
5. Daar waar gekozen oplossingen in het stelsel een wettelijke borging vragen is het van belang dat deze juridisch te implementeren is.

De komst van een nationale CSIRT, passend bij de NLCS en NIS2 regietaken is in alle scenario's te realiseren en is daarom niet als separaat onderscheidend uitgangspunt opgenomen. Dit geldt ook voor het uitgangspunt dat de politieke verantwoordelijkheid

[37] Dit staat los van de discussie of er in Nederland 1 centraal meldpunt moet komen in verband met de meldplicht. In dit uitgangspunt gaat het om het aanspreekpunt voor CSIRT-dienstverlening.

voor sectoren bij de desbetreffende vakminister blijft, zoals dit ook geldt voor toezicht op entiteiten in het kader van de NIS2.

SCENARIO'S VOOR HET CSIRT-STELSEL

Tijdens de verkenningsgesprekken met de verschillende stakeholders zijn er drie mogelijke scenario's (met varianten) verkend. Dit zijn:

1. De huidige situatie zonder wijzigingen voortzetten, waarbij nieuwe wettelijke taken zoveel mogelijk worden geïntegreerd in het al bestaande landschap.
2. Inrichting van een stelsel met meerdere sectorale CSIRT's met wijzigingen voor wat betreft taakverdeling, governance en toezicht. Hiervoor zijn twee varianten denkbaar.
3. Alle bestaande sectorale CSIRT's worden geïntegreerd tot één enkele CSIRT die de wettelijke taken uitvoert voor sectoren die onder de NIS2 vallen.

In onderstaande paragrafen worden deze scenario's nader toegelicht.

Scenario 1: De huidige situatie zonder wijzigingen voortzetten, waarbij nieuwe wettelijke taken zoveel mogelijk worden geïntegreerd in het al bestaande landschap

In het eerste scenario wordt de huidige situatie voortgezet met een aantal bestaande zelfstandige CSIRT's die elk eigen sectoren bedienen. Het aantal CSIRT's kan in de toekomst gelijk blijven, maar zou eventueel naar behoefte kunnen worden vergroot (of verkleind). Van centrale aansturing of regie is weinig tot geen sprake, en samenwerkingsverbanden zoals die op dit moment bestaan kunnen worden gehandhaafd.

Een groot deel van de bestaande CSIRT's zal te maken krijgen met de NIS2, omdat zij sectoren bedienen die in die richtlijn zijn opgenomen. Een klein deel zal vrijwillig zijn en blijven, en hoeft geen wettelijke kaders te volgen. Hiermee kan een onderscheid gemaakt worden tussen CSIRT's binnen het stelsel die wel aan alle wettelijke vereisten moeten voldoen, en CSIRT's waarvoor dit niet geldt.

Voor de CSIRT's die te maken krijgen met de NIS2 betekent dit in scenario 1 dat binnen het huidige landschap gekeken wordt hoe de verplichte wettelijke taken kunnen worden belegd bij, of onderling verdeeld over, de bestaande sectorale CSIRT's. In de praktijk betekent dit dat de bestaande CSIRT's de wijzigingen die voortvloeien uit NIS2 binnen hun eigen sectorale verantwoordelijkheid zullen moeten implementeren en adresseren. Het collectief van sectorale CSIRT's zal samen zorg moeten dragen voor compliance met alle eisen die NIS2 stelt. Als de governance-inrichting van een specifieke sectorale CSIRT het beleggen van wettelijke taken belemmert (doordat deze CSIRT niet onder de Rijksoverheid valt), moet deze worden gewijzigd.

Een noodzakelijke toevoeging aan het landschap in dit scenario is het aanwijzen van een nationale CSIRT, die overkoepelende, sector overstijgende en/of (zeer) geavanceerde taken zoals geformuleerd in de NIS2 op zich neemt.

Scenario 2: Inrichting van een stelsel met meerdere sectorale CSIRT's met wijzigingen

In het tweede scenario wordt een stelsel gecreëerd bestaande uit meerdere CSIRT's, maar wordt daarnaast meer structuur aangebracht op gebied van onderlinge taakverdeling, kwaliteitsborging, governance en toezicht (op het stelsel).

Ook hier is een toevoeging het aanwijzen van een nationale CSIRT, die overkoepelende, sector overstijgende en/of (zeer) geavanceerde taken op zich neemt.

Naast deze nationale CSIRT zullen sectorale CSIRT's (blijven) bestaan, waarbij sommige, net als in scenario 1, wettelijk verplichte taken uitvoeren voor specifieke, in de NIS2 genoemde sectoren, en andere CSIRT's op vrijwillige basis functioneren voor sectoren die buiten de NIS2 vallen.

Binnen scenario 2 zijn twee mogelijke varianten overwogen.

Scenario 2a: één nationale CSIRT voor sector-overstijgende taken; alle sectorale CSIRT's die onder NIS2 vallen voeren dezelfde set taken uit

In dit scenario bestaan (naast de nationale CSIRT) sectorale CSIRT's, die elk een eigen (set van) sector(en) bedienen. Het takenpakket dat aan deze sectorale CSIRT's wordt toegewezen, is gelijk: alle sectorale CSIRT's voeren dezelfde set taken uit, en moeten dus zodanig zijn ingericht dat ze in staat zijn deze taken uit te voeren[38].

De sector overstijgende taken versus sectorspecifieke taken moeten in dit scenario nader worden uitgewerkt. Voorbeelden zijn bijvoorbeeld het centraal in kaart brengen van generieke ICT-kwetsbaarheden en het sectoraal bepalen van impact op een doelgroep. Daarnaast kunnen ook faciliteiten centraal worden belegd, bijvoorbeeld het centraal testen/ontwikkelen/inkopen/beheren van tooling en bronnen om efficiency voor sectorale CSIRT's te bevorderen.

Het huidige NCSC/CSIRT-DSP heeft in dit scenario een dubbelrol. Ze fungeert enerzijds als nationale CSIRT en anderzijds als sectorale CSIRT voor diverse aangewezen sectoren.

Scenario 2b: één nationale CSIRT voor overstijgende taken; alle sectorale CSIRT's die onder NIS2 vallen voeren taken naar vermogen uit; wat zij niet kunnen uitvoeren, delegeren ze naar het NCSC/CSIRT-DSP

In dit scenario is er eveneens bestaan (naast de nationale CSIRT) sectorale CSIRT's, die elk een eigen (set van) sector(en) bedienen. Het takenpakket van deze sectorale

[38] Waar nodig kunnen contracten worden afgesloten met externe commerciële partners voor het leveren van diensten die nodig zijn voor een deel van de werkzaamheden. De sectorale CSIRT is en blijft echter verantwoordelijk voor het met de juiste kwaliteit leveren van de gevraagde dienstverlening.

CSIRT's wordt aangepast aan de middelen, de mogelijkheden en het taakvolwassenheidsniveau van de individuele sectorale CSIRT.

Sectorale CSIRT's nemen die taken voor hun rekening die zij naar wettelijke standaarden en gestelde kwaliteitseisen kunnen uitvoeren. Wat zij niet aankunnen, wordt bij de het NCSC/CSIRT-DSP belegd in haar rol als sectorale CSIRT (het NCSC/CSIRT-DSP heeft een dubbelrol, zowel als nationale CSIRT als sectorale CSIRT voor diverse aangewezen sectoren). Het betreft maatwerk voor elke individuele sectorale CSIRT, waarbij voortdurend bekeken wordt of/in welke mate een sectorale CSIRT beter of minder goed in staat is haar taken uit te voeren, en of, in antwoord daarop, taken beter belegd kunnen worden bij het NCSC/CSIRT-DSP of juist terug moeten verhuizen naar de sectorale CSIRT.

Scenario 3: Alle bestaande sectorale CSIRT's worden geïntegreerd tot één enkele CSIRT die de wettelijke taken uitvoert voor sectoren die onder de NIS2 vallen

In het derde scenario worden alle bestaande sectorale CSIRT's geïntegreerd in één nieuwe organisatie. In Nederland is er dan nog één sectoraal CSIRT dat alle sectoren uit de NIS2 bedient. Vrijwillige CSIRT's kunnen blijven bestaan. Dit betekent dat al die sectorale CSIRT's die momenteel in het landschap aanwezig zijn en onder de NIS2 (komen te) vallen samengaan onder de noemer van het NCSC/CSIRT-ISP. Uiteraard zullen verschillende sectoren met CSIRT-functionaliteit moeten worden bediend, dus zullen waarschijnlijk sectorspecifieke afdelingen of subdivisies gecreëerd worden binnen de (zeer omvangrijke) organisatie.

In het geval dat er sectoren zijn met entiteiten die niet allemaal NIS2-verplichtingen hebben, zal aanvullend moeten worden besloten hoe deze bediend zullen worden. Mogelijk moeten hiervoor nieuwe separate vrijwillige CSIRT's worden ingesteld. Voor de kortere termijn lijkt het in dit scenario niet haalbaar om ook voor entiteiten zonder NIS2-verplichtingen het gezamenlijke CSIRT beschikbaar te maken als in ogenschouw wordt genomen dat de uitbreiding van entiteiten als gevolg van de NIS2 al een enorme uitdaging met zich meebrengt alsook een integratietraject om een gezamenlijk CSIRT te vormen.

ANALYSE VAN DE VERSCHILLENDE SCENARIO'S

Om een keuze te kunnen maken uit de genoemde scenario's is een analyse gemaakt, waarbij de drie scenario's (met varianten) zijn getoetst aan de geformuleerde uitgangspunten:

1. Wettelijke kaders:
   a. Voldoet een scenario aan de wettelijke eisen gesteld in de NIS2 en andere al bekende richtlijnen?
   b. Is de uitvoering van taken in een scenario haalbaar voor alle CSIRT's, (ook) in het licht van de NIS2?
2. De NLCS:

    a. Hoe is de balans tussen centralisatie en decentralisatie bij het genoemde scenario?
    b. Worden zaken die in het verleden hun nut bewezen hebben voldoende behouden?
    c. Is er één loket voor doelgroepen bij hun sectorale CSIRT voor dienstverlening?
    d. Wordt er effectief en efficiënt omgegaan met schaarse menskracht en middelen?
3. Vrijwillige CSIRT's:
    a. Is er in dit scenario ruimte voor vrijwillige CSIRT's en in welke mate worden zij geprikkeld om voldoende aan kwaliteitsborging te doen?
4. Complexiteit
    1. Zorgt dit scenario voor veel of weinig complexiteit in termen van governance, wet- en regelgeving, samenwerking, en herkenbaarheid?
5. Juridische haalbaarheid
    a. Welke mate van juridische haalbaarheid kent het scenario?

De drie scenario's (met varianten) zijn op basis van bovenstaande vragen vergeleken en voorzien van een score, gebruik makend van de volgende vijfpuntschaal:

-- Uitgangspunt is zeer moeilijk te realiseren
- Uitgangspunt is moeilijk te realiseren
+- Uitgangspunt is te realiseren
+ Uitgangspunt is goed te realiseren
++ Uitgangspunt is zeer goed te realiseren

Hieronder volgt een uitwerking van de analyse van de genoemde mapping.

Scenario 1: De huidige situatie zonder wijzigingen voortzetten, waarbij nieuwe wettelijke taken zoveel mogelijk worden geïntegreerd in het al bestaande landschap

Dit scenario impliceert dat er binnen de huidige CSIRT's bekeken wordt hoe verplichte taken kunnen worden belegd, maar dat er geen stappen worden gemaakt richting meer/andere samenwerking of het creëren van een gestructureerd CSIRT-stelsel. Bij de mapping van de verschillende uitgangspunten op dit scenario komt het volgende beeld naar voren.

Scenario 1 - wettelijke kaders (waaronder NIS2)

Het is zeer lastig om binnen de huidige situatie adequaat om te gaan met de nieuwe eisen die voortvloeien uit de NIS2 (--). In de eerste plaats komt dit doordat de CSIRT's in Nederland nog niet in een stelsel vervat zijn. De NIS2 formuleert verschillende randvoorwaarden, taken en eisen waaraan een (landschap van) CSIRT's in lidstaten moeten voldoen, bijvoorbeeld ten behoeve van internationale samenwerking, informatie-uitwisseling en regie. Omdat het huidige landschap in Nederland geen vastgelegde taak- en rolverdeling kent, maar sectoren elk worden bediend door een afzonderlijke aangewezen CSIRT, wordt het uitdagend invulling te

geven aan die overstijgende taken zonder structurele wijzigingen in het bestaande landschap.

Daarnaast is het ook de haalbaarheid voor het beleggen van NIS2-taken in dit scenario zeer lastig (--). Behalve het aanbrengen van wijzigingen in de governance-inrichting van diverse sectorale CSIRT's gaat het om het beleggen van een brede set van wettelijke taken en dito eisen. Taken die nu nog niet allemaal door sectorale CSIRT's worden uitgevoerd en eisen waaraan niet alle sectorale CSIRT's op dit moment voldoen[39]. De NIS2 stelt bijvoorbeeld dat alle CSIRT's die onder haar kaders vallen verplicht zijn forensisch materiaal te verzamelen, dynamische risico- en incidentanalyses moeten maken, en situational awareness moeten bieden. Daarnaast zouden CSIRT's bijvoorbeeld proactief de netwerken van entiteiten moeten kunnen scannen. Voor CSIRT's met weinig capaciteit en beperkte middelen lijken dergelijke geavanceerde eisen niet haalbaar.

Scenario 1 - NLCS

De bestaande situatie komt niet tegemoet aan de in de NLCS genoemde doelstelling van 'centraal als het kan en decentraal als het moet' (--). In de bestaande situatie zijn CSIRT's min of meer zelfstandig van elkaar functionerende entiteiten, en dus is het landschap in hoge mate decentraal. In dit scenario wordt niet gezocht naar optimalisaties die passen bij dit uitgangspunt van de NLCS. Waar centralisatie wel degelijk mogelijk zou zijn, en zou kunnen leiden tot meer efficiëntie, betere governance of een effectievere inzet van mensen en middelen, worden daardoor kansen onbenut gelaten.

Wel is het zo dat in dit scenario weinig zorgen hoeven te zijn over het afstoten van in het verleden succesvol gebleken activiteiten (+). Met het behoud van de huidige situatie kunnen immers alle activiteiten worden voortgezet. Tegelijk rijst de vraag of sectorale impact op sommige dossiers en in sommige situaties zou kunnen worden vergroot ten opzichte van het heden door meer structuur en centrale besturing aan te brengen.

Verder heeft de bestaande situatie als nadeel dat er geen sprake is van een duidelijk loket waar sectoren kunnen aankloppen (-). Dit geldt met name ten aanzien van de wettelijke taken die volgens de NIS2 door CSIRT's moeten worden vervuld. In het geval dat een sectorale CSIRT deze wettelijke taken niet accepteert, dan zouden deze moeten worden belegd bij het NCSC/CSIRT-DSP. Daardoor ontstaat onduidelijkheid voor afnemers waar zij terecht kunnen.

Tot slot blijft de situatie rondom capaciteit ongewijzigd (+-): omdat de huidige context gehandhaafd blijft, kunnen mensen en middelen niet efficiënter worden ingezet, maar worden ze ook niet minder efficiënt verdeeld dan nu het geval is.

[39] Deze conclusie is gebaseerd op basis van een eerste oordeel na de verkenningsgesprekken en kan nog nader onderbouwd worden door het uitvoeren van een bredere toets op taken en taakvolwassenheid.

Scenario 1 - vrijwillige CSIRT's

In de bestaande situatie wordt er geen uitdrukkelijke vraag om kwaliteitsborging neergelegd bij vrijwillige CSIRT's en gezien de uitgangspunten van scenario 1 zal dat niet wijzigen in de toekomst (--). Vrijwillige CSIRT's leggen zichzelf op het gebied van kwaliteitsborging in sommige gevallen wel degelijk verantwoordelijkheden op, maar er zijn geen afspraken tussen vrijwillige CSIRT's onderling, er is geen sprake van een gedeelde systematiek of gedeelde zelfopgelegde eisen. Voor de toekomst zijn er onder scenario 1 geen evidente prikkels tot verbetering te voorzien, mede omdat er geen sprake zal zijn van een stelsel van CSIRT's. De inzet van prikkels zoals opname in het LDS of onderdeel worden van informatie-uitwisselingssystemen is om die reden ingewikkeld. Voor afnemers is een gebrek aan kwaliteitsborging problematisch, omdat verschillende sectoren nu of in de toekomst bediend (kunnen) worden door CSIRT's met een (zeer) wisselende mate van kwaliteit en/of volwassenheid.

Scenario 1 - complexiteit

Voortzetting van de bestaande situatie betekent dat er binnen het landschap een zekere mate van complexiteit bestaat (-). Dit komt omdat er in de huidige situatie weinig structuur en samenhang is, en er een gebrek is aan overzicht. Een helder stelsel van CSIRT's ontbreekt, waardoor sturing en toezicht lastig zijn. Hoewel een landschap met zes sectorale CSIRT's overzichtelijk lijkt kan dit wijzigen zodra er meer nieuwe (vrijwillige) sectorale CSIRT's in het landschap ontstaan.

Scenario 1 - juridische haalbaarheid

In het licht van de eisen die gesteld worden door NIS2 is het juridisch niet haalbaar om taken te (blijven) beleggen zoals dat in het huidige landschap wordt gedaan (--). Zoals onder punt 1 uitgelegd voeren de CSIRT's in Nederland op dit moment niet alle taken uit die door de nieuwe richtlijn gaan worden geëist, en is het zeer moeilijk in deze situatie afdoende verandering te realiseren. Als er wettelijke taken (kunnen) worden belegd bij de sectorale CSIRT's zullen zij verantwoordelijk zijn voor de uitvoering hiervan en moeten voldoen aan alle gestelde eisen die de wet (Wbni2024) daaraan stelt.

De analyse van scenario 1 wordt in de onderstaande tabel samengevat.

Uitgangspunt	Score	Samenvatting toelichting
1a NIS2-eisen	--	Een stelsel van CSIRT's ontbreekt in Nederland. Daardoor is het lastig om sector overstijgende of overkoepelende taken uit de NIS2 te beleggen.
1b Haalbaarheid uitvoering	--	Er zijn zorgen over de haalbaarheid ten aanzien van het beleggen van de NIS2-taken en de eisen die er worden gesteld. De NIS2 verlangt dat alle aangewezen CSIRT's (deels) zeer complexe en

		geavanceerde taken moeten uitvoeren. Met de beperkte omvang en middelen die zij hebben is dat momenteel niet haalbaar.
2a NLCS centraal/decentraal	--	Er blijft een landschap met veel decentrale onderdelen en komt ook geen sturing op het meer centraliseren waar dat wel mogelijk is.
2b Bewezen sectorale impact	+	Op diverse plekken in het landschap is sprake van bewezen sectorale impact. Deze blijft behouden. Bij meer structuur en centrale besturing kan deze impact echter verder worden vergroot.
2c Eén loket	-	De situatie kan ontstaan dat een sectorale CSIRT de nationale taken die de NIS2 voorschrijft niet accepteert. Deze zullen dan moeten worden belegd bij het NCSC/CSIRT-DSP. Daardoor ontstaat onduidelijkheid voor afnemers waar zij terecht moeten in welke situatie.
2d Inzet schaarse capaciteit	+-	De situatie rondom capaciteit blijft ongewijzigd.
3 Kwaliteitsborging bij vrijwillige CSIRT's	--	Sectorale CSIRT's die buiten de NIS2 vallen worden op dit moment niet uitdrukkelijk uitgenodigd om aan kwaliteitsborging te doen. Dit betekent dat sectoren (zeer) wisselend bediend kunnen worden. Er zijn geen prikkels aanwezig om hierin verandering te brengen.
4 Lage complexiteit	-	Er is in dit scenario sprake van complexiteit door gebrek aan structuur, samenhang en overzicht.
5 Juridisch haalbaar	--	De eisen uit de NIS2 zullen moeten worden geïmplementeerd maar sluiten slecht aan bij de wijze waarop het landschap nu is ingericht.

Scenario 2a: één nationale CSIRT voor sector overstijgende taken; alle sectorale CSIRT's die onder NIS2 vallen voeren dezelfde set taken uit

In dit scenario wordt een stelsel gecreëerd met één nationale CSIRT, en daarnaast meerdere sectorale CSIRT's. Alle sectorale CSIRT's moeten hetzelfde takenpakket zelfstandig (kunnen) uitvoeren en alle sectorale CSIRT's die vallen onder de NIS2 moeten aan dezelfde standaarden voldoen. Bij de mapping van de verschillende uitgangspunten op dit scenario komt het volgende beeld naar voren.

Scenario 2a - wettelijke kaders (waaronder NIS2)

Het is goed mogelijk om binnen het genoemde scenario adequaat om te gaan met de nieuwe eisen die de NIS2 stelt (+). De nationale CSIRT die wordt aangewezen zal in dit scenario de overkoepelende en/of (zeer) geavanceerde taken op zich nemen die in de NIS2 opgelegd worden. Zo kunnen taken op het gebied van gezamenlijke standaarden en instrumentarium voor informatievoorziening hier worden opgepakt. Ook kunnen andere te centraliseren taken hier worden belegd. Daarnaast krijgen de sectorale CSIRT's een volwaardige taak die voor alle sectorale CSIRT's hetzelfde is opgelegd. Gezamenlijk zijn zo alle taken uit de NIS2 goed te beleggen in het stelsel. Daarnaast moeten de sectorale CSIRT's hierbij gezamenlijk alle aangewezen sectoren afdekken. Ook dit is goed mogelijk. Merk hierbij op dat het NCSC/CSIRT-DSP hierbij een dubbelrol krijgt en zowel optreedt als nationale CSIRT als ook sectorale CSIRT, voor de sectoren die aan deze CSIRT worden toegewezen.

Nadeel van dit scenario is dat de nationale CSIRT ook een behoorlijke set taken krijgt toebedeeld hetgeen mogelijk leidt tot taakverschuivingen binnen het NCSC/CSIRT-DSP. Een voordeel van dit scenario is het feit dat het kansrijk is in termen van haalbaarheid (+). Alle elementen die in het huidige landschap van sectorale CSIRT's goed functioneren, kunnen worden behouden en verder uitgebouwd. Door het scheppen van een nationale CSIRT en het verdelen van de taken tussen die CSIRT en de sectorale CSIRT's kan een optimale uitvoer van alle in de NIS2 gestelde eisen worden verwezenlijkt. Het leidende principe zou daarbij moeten zijn: taken worden belegd bij de schouders die ze het beste kunnen dragen.

Scenario 2a - NLCS

Aansluitend op bovenstaande kan men stellen dat in scenario 2a enigszins tegemoetgekomen wordt aan de in de NLCS genoemde doelstelling van 'centraal als het kan en decentraal als het moet' (+-). Er is sprake van centralisatie door de creatie van een nationale CSIRT, en het beleggen van een deel van de (wettelijke) CSIRT-taken bij die entiteit. Ook is er sprake in dit scenario van centrale sturing en kwaliteitsborging. Tegelijkertijd blijft er sprake van een landschap met meerdere zelfstandig opererende sectorale CSIRT's, waardoor de vraag opgeworpen kan worden in welke mate decentralisatie echt 'moet', zoals het principe in de NLCS stelt.

Daarentegen sluit dit scenario juist zeer goed aan bij de wens om bewezen impact zo veel mogelijk te handhaven: activiteiten die hun effect bewezen hebben, kunnen worden voortgezet (++). Bovendien kan er, met de komst van een nationale CSIRT en een stelselaanpak van sectorale CSIRT's met eenzelfde takenpakket, een helder beeld gegeven worden welke sectoren vallen onder welke sectorale CSIRT's (bij voorkeur één, maar soms meerdere als een entiteit in meerdere sectoren valt).

Voor entiteiten in sectoren is de hen toegewezen CSIRT het loket, hetgeen daarmee aansluit op de behoefte aan duidelijkheid (+). In de meeste gevallen is dit één CSIRT, in sommige gevallen meerdere doordat entiteiten in meerdere sectoren kunnen vallen. De reden dat dit uitgangspunt niet de maximale score krijgt is dat er nog

onduidelijkheid is over het verdelen van de taken tussen de sectorale CSIRT en nationale CSIRT. Dit moet gebeuren op een wijze dat dit uitgangpunt gehandhaafd blijft.

Tot slot maakt scenario 2a zeer goed gebruik van de inzet van capaciteit en middelen (++): door de verdeling van taken tussen een nationale CSIRT en sectorale CSIRT's kan een optimale spreiding van schaarse mensen en middelen worden bewerkstelligd. Zeer specialistische kennis kan worden ingezet op de plekken waar zij de meeste impact kan bereiken, en door betere integratie en meer overzicht kunnen middelen efficiënter en effectiever worden ingezet.

Scenario 2a - vrijwillige CSIRT's

In scenario 2a zullen sectorale CSIRT's die gaan over sectoren die onder de NIS2 vallen moeten voldoen aan alle wettelijke eisen. Maar in dit scenario wordt daaraan toegevoegd dat er ook een uitdrukkelijke vraag om kwaliteitsborging wordt neergelegd bij vrijwillige CSIRT's als zij onderdeel willen blijven of worden van het stelsel van CSIRT's (+). Daar waar in scenario 1 geen sprake is van het creëren van een CSIRT-stelsel, is dat hier wel het geval. Juist door het scheppen van een stelsel, wordt het mogelijk duidelijke voorwaarden te stellen voor toetreding tot dit stelsel; een uitdrukkelijke vraag tot kwaliteitsborging bij vrijwillige CSIRT's is daar een voorbeeld van.

Op basis van de frameworks op pagina 27 zullen vrijwillige CSIRT's moeten kunnen aantonen dat zij aan bepaalde volwassenheidsniveaus voldoen. Het betreft hier geen harde, wettelijke eisen – de vrijwillige CSIRT's vallen immers buiten de wettelijke kaders. Maar wanneer vrijwillige CSIRT's willen aansluiten op onderdelen van het CSIRT-stelsel, bijvoorbeeld voor informatiedeling of om onderdeel te worden van het LDS, dan kan een mate van volwassenheid op het gebied van kwaliteitsborging als hefboom gebruikt worden. Wel zal uitdagend zijn om toe te zien op deze eisen omdat ze geen dwingend wettelijk karakter hebben maar uit oogpunt van informatiedeling en kwaliteit zeer wenselijk zijn.

Scenario 2a - complexiteit

In scenario 2a wordt een stelsel gecreëerd met twee componenten: een nationale CSIRT die overkoepelende en (zeer) geavanceerde taken op zich neemt, en een set van sectorale CSIRT's, die allemaal dezelfde set van taken uitvoeren. In termen van complexiteit heeft dit systeem sterkere en minder sterke punten (+-). Door een heldere en vaste taakverdeling tussen de nationale CSIRT enerzijds en de sectorale CSIRT's anderzijds ontstaat ordening en herkenbaarheid. Sectorale CSIRT's worden vergelijkbaar met elkaar, in elk geval in hun taakstelling, en het is helder welke taken zij uitvoeren, en welke taken centraal worden belegd. Tegelijkertijd is het systeem niet optimaal eenvoudig, omdat er nog steeds sprake is van een stelsel met verschillende zelfstandige sectorale CSIRT's.

Scenario 2a – juridische haalbaarheid

Scenario 2a is op basis van eerste inschattingen van de wetgevingsjuristen is een haalbaar scenario (+). De NIS2 schrijft niet zozeer de komst van een nationale CSIRT voor, maar dat bepaalde CSIRT-taken met bepaalde eisen worden belegd bij 1 of meerdere CSIRT's. Deels betreft dat operationele taken en deels coördinerende regietaken. Als het gaat om de taken van een CSIRT dan is uitgangspunt voor de wetgeving dat een CSIRT een volledig takenpakket krijgt toebedeeld zoals dit in de wet wordt vastgelegd inclusief de eisen die hieraan worden gesteld.

De analyse van scenario 2a wordt in de onderstaande tabel samengevat.

Uitgangspunt	Score	Samenvatting toelichting
1a NIS2-eisen	+	Door het volledig beleggen van taken en eisen aan een nationale CSIRT en sectorale CSIRT's is dit scenario passend te maken.
1b Haalbaarheid uitvoering	+	Door het scheppen van een nationale CSIRT en het verdelen van de taken tussen die CSIRT en de sectorale CSIRT's kan een goede uitvoer van alle in de NIS2 gestelde eisen worden verwezenlijkt.
2a NLCS centraal/decentraal	+-	Door een deel van de taken te beleggen bij de nationale CSIRT is sprake van centralisatie; door het behoud van sectorale CSIRT's kan discussie blijven bestaan over de vraag of er voldoende gecentraliseerd is om tegemoet te komen aan dit principe uit de NLCS.
2b Bewezen sectorale impact	++	Er wordt hier goed gekeken naar al bewezen impact en deze wordt zoveel mogelijk gehandhaafd.
2c Eén loket	+	Door heldere verdeling van de sectoren over de sectorale CSIRT's is er voor elke sector 1 duidelijk loket. Uitdaging zijn de entiteiten die onder meerdere sectoren vallen.
2d Inzet schaarse capaciteit	++	Mensen en middelen kunnen zo efficiënt mogelijk worden verdeeld tussen de nationale CSIRT en de sectorale CSIRT's.
3 Kwaliteitsborging bij vrijwillige CSIRT's	+	Er worden prikkels ingezet om vrijwillige CSIRT's aan te zetten tot kwaliteitsborging wanneer zij toe willen treden tot het stelsel. Wel is toezicht hierop lastig.

4 Lage complexiteit	+-	Er is sprake van enige complexiteit doordat er een landschap blijft met meerdere sectorale CSIRT's.
5 Juridisch haalbaar	+	Doordat een eenduidig takenpakket per CSIRT wordt bepaald (alle CSIRT's hetzelfde pakket) is dit haalbaar. Onderscheid tussen nationale en sectorale CSIRT's (en dubbelrol NCSC/CSIRT-DSP) is punt van aandacht.

Scenario 2b: één nationale CSIRT voor overstijgende taken; alle sectorale CSIRT's die onder NIS2 vallen voeren taken naar vermogen uit; wat zij niet kunnen uitvoeren, delegeren ze naar het NCSC/CSIRT-DSP

In dit scenario wordt een stelsel gecreëerd met één nationale CSIRT, en daarnaast meerdere sectorale CSIRT's. In dit scenario voeren individuele sectorale CSIRT's op basis van maatwerk een eigen takenpakket uit, en delegeren zij de taken die zij niet zelfstandig kunnen uitvoeren, of waarvoor ze niet kunnen voldoen aan de wettelijk gestelde standaarden, over aan het NCSC/CSIRT-DSP in haar rol als sectorale CSIRT.

Hoewel alle sectorale CSIRT's die vallen onder de NIS2 aan de wettelijke eisen van die richtlijn moeten voldoen, zal bij al deze CSIRT's gezocht worden naar het optimale takenpakket voor hun specifieke context. Doorheen de tijd kan het takenpakket van individuele CSIRT's worden aangepast op basis van veranderingen in hun volwassenheidsniveau. Daardoor zouden dan meer taken terugvloeien van het NCSC/CSIRT-DSP naar de individuele CSIRT of andersom. Dit systeem biedt maximale flexibiliteit ten opzichte van het huidige landschap van CSIRT's. Bij de mapping van de verschillende uitgangspunten op dit scenario komt het volgende beeld naar voren.

Scenario 2b - wettelijke kaders (waaronder NIS2)

Net als in scenario 2a is het mogelijk om binnen het genoemde scenario om te gaan met de nieuwe eisen die de NIS2 stelt. De maatwerk-aanpak van dit scenario kan een negatieve impact hebben de stevigheid van het CSIRT-stelsel en maakt sturing, toezicht en controleerbaarheid daardoor uitdagend. (+-). De nationale CSIRT die wordt aangewezen zal in dit scenario de overkoepelende en/of (zeer) geavanceerde taken op zich nemen die in de NIS2 opgelegd worden. Zo kunnen taken op het gebied van gezamenlijke standaarden en instrumentarium voor informatievoorziening hier worden opgepakt. Ook kunnen andere te centraliseren taken hier worden belegd. Daarnaast krijgen de sectorale CSIRT's een maatwerktaak die voor alle sectorale CSIRT's verschillend is, afhankelijk van elementen zoals expertise en capaciteit. Gezamenlijk zijn zo alle taken uit de NIS2 goed te beleggen in het stelsel. Daarnaast moeten de sectorale CSIRT's hierbij gezamenlijk alle aangewezen sectoren afdekken. Ook dit is goed mogelijk. Merk hierbij op dat het NCSC/CSIRT-DSP hierbij een dubbelrol krijgt en zowel optreedt als nationale CSIRT als ook sectorale CSIRT, voor

de sectoren die aan deze CSIRT worden toegewezen. Een nadeel van de constructie zoals geformuleerd in scenario 2b is dat er een gebrek aan overzicht kan ontstaan over de taakverdeling tussen het NCSC/CSIRT-DSP enerzijds en de andere sectorale CSIRT's anderzijds, omdat die laatsten allemaal een ander takenpakket uitvoeren, en dit takenpakket bovendien doorheen de tijd flexibel aan te passen is op basis van de volwassenheid van individuele CSIRT's. Dit maakt het houden van toezicht erg complex, en vereist voortdurende, kostbare afstemming tussen het NCSC/CSIRT-DSP en de individuele sectorale CSIRT's. Het bewaken van, en sturen op, het CSIRT-stelsel wordt bovendien uitdagend gezien de maatwerkconstructie die de kern vormt van dit scenario. Ook de controleerbaarheid van compliance met wet- en regelgeving wordt uitdagender wanneer het takenpakket van individuele CSIRT's niet geharmoniseerd is en veranderbaar doorheen de tijd. In het uiterste geval kan een situatie ontstaan waarin bepaalde eisen uit de NIS2 lastig te verwezenlijken worden of taken tussen wal en schip vallen.

In termen van haalbaarheid scoort dit scenario niet zo goed (-). Net als bij scenario 2a wordt ook hier een nationale CSIRT gecreëerd die een deel van de meest geavanceerde of overkoepelende taken kan overnemen. Tegelijk zit er fluïditeit in het landschap van sectorale CSIRT's, waarbij taken soms wel en soms niet gedragen worden door het NCSC/CSIRT-DSP in haar taak als sectorale CSIRT. Dit zorgt voor complexiteit in de uitvoering, en extra risico's voor wat betreft fouten en incidenten. Er moet met regelmaat gecontroleerd worden wat het volwassenheidsniveau is van individuele CSIRT's in relatie tot hun takenpakket om te bezien of zij (nog) aan de wettelijke eisen voldoen. Dit betekent intensief toezicht enerzijds, en veel afstemming tussen de individuele CSIRT's en het NCSC/CSIRT-DSP anderzijds. Er bestaat een risico dat taken soms door de hoge mate van flexibiliteit (tijdelijk) tussen de wal en het schip belanden, wat leidt tot uitdagingen op het gebied van compliance. Dit scenario behoudt veel van het goede dat in het heden beschikbaar is in het landschap en geeft maximale flexibiliteit naar de toekomst, maar heeft als keerzijde hoge kosten en verminderde effectiviteit tot gevolg.

Scenario 2b - NLCS

Net als bij scenario 2a wordt ook in scenario 2b enigszins tegemoetgekomen aan de in de NLCS genoemde doelstelling van 'centraal als het kan en decentraal als het moet' (+-). Er is sprake van centralisatie door de creatie van een nationale CSIRT, en het beleggen van een deel van de (wettelijke) CSIRT-taken bij die entiteit. Ook is er sprake in dit scenario van centrale sturing en kwaliteitsborging. Tegelijkertijd blijft er sprake van een landschap met meerdere zelfstandig opererende sectorale CSIRT's, waardoor de vraag opgeworpen kan worden in welke mate decentralisatie echt 'moet', zoals het principe in de NLCS stelt.

Daarentegen sluit dit scenario net als het vorige zeer goed aan bij de wens om bewezen impact zo veel mogelijk te handhaven: activiteiten die hun effect bewezen hebben, kunnen worden voortgezet (++).

Wat betreft de wens om één duidelijk loket te creëren voor afnemers is scenario 2b niet kansrijk (--). Door de maatwerkoplossingen die gecreëerd worden op het gebied van de taakverdeling tussen individuele CSIRT's en het NCSC/CSIRT-DSP is er een grote kans is dat maar een zeer klein aantal afnemers daadwerkelijk één loket heeft. Het overgrote deel van de afnemers zal voor een deel van de dienstverlening terechtkunnen bij hun sectorale CSIRT (NB één of meerdere), en voor de rest van de dienstverlening bij het NCSC/CSIRT-DSP. Hoewel op papier afgesproken kan worden dat het loket de eigen sectorale CSIRT is, zal bij communicatie toch contact ontstaan met het NCSC/CSIRT-DSP waardoor er in de praktijk toch sprake is van een dubbel loket en daardoor onduidelijkheid. Wanneer de taakverdeling dan ook nog eens doorheen de tijd anders kan worden verdeeld tussen die organisaties, wordt het voor doelgroepen lastig duurzaam vast te stellen bij wie ze terechtkunnen voor welke vraag.

Tot slot maakt scenario 2b goed gebruik van de inzet van capaciteit en middelen (+-): door de verdeling van taken tussen een nationale CSIRT, het NCSC/CSIRT-DSP en de overige sectorale CSIRT's kan een goede spreiding van schaarse mensen en middelen worden bewerkstelligd. Zeer specialistische kennis kan worden ingezet op de plekken waar zij de meeste impact kan bereiken, en door betere integratie en meer overzicht kunnen middelen in principe efficiënt en effectief worden ingezet. Tegelijk zal er in dit scenario vanwege het maatwerk in de taakverdeling veel afstemming moeten plaatsvinden tussen de individuele sectorale CSIRT's en het NCSC/CSIRT-DSP, en verhoudingsgewijs meer middelen vrijgemaakt moeten worden voor toezicht, omdat ook dit laatste in dit scenario maatwerk vereist. Al met al zal dit betekenen dat er meer geïnvesteerd moet worden in sturing, controle en afstemming, waardoor minderen middelen en menskracht vrijgemaakt kunnen worden voor de inhoudelijke taken van de nationale en sectorale CSIRT's.

Scenario 2b - vrijwillige CSIRT's

Wat betreft de kwaliteitsborging voor vrijwillige CSIRT's geldt in scenario 2b hetzelfde als in scenario 2a (+).

Scenario 2b - complexiteit

In termen van complexiteit scoort scenario 2b niet zo goed (-). Weliswaar is er sprake van het scheppen van een CSIRT-stelsel, waardoor duidelijkheid ontstaat in het landschap en er meer sturing en betere governance mogelijk is. Tegelijkertijd zorgt het behoud van individuele sectorale CSIRT's voor meer complexiteit dan wanneer Nederland slechts één sectorale CSIRT zou hebben. Daarnaast zorgt het loslaten van het gelijktrekken van alle taken van alle sectorale CSIRT's voor aanzienlijke complexiteit: ordening en herkenbaarheid worden erdoor ondergraven, sectorale CSIRT's zijn hierdoor onderling niet vergelijkbaar, en kunnen moeilijk aan dezelfde standaarden worden gehouden. Voor elke CSIRT gelden effectief andere afspraken, en die kunnen doorheen de tijd veranderen in het licht van de veranderende volwassenheid van een individuele sectorale CSIRT. Dit maakt het stelsel complex.

Scenario 2b – juridische haalbaarheid

Scenario 2b is op basis van eerste inschattingen van de wetgevingsjuristen een niet goed haalbaar scenario (-). De NIS2 schrijft niet zozeer de komst van een nationale CSIRT voor, maar dat bepaalde CSIRT-taken met bepaalde eisen worden belegd bij 1 of meerdere CSIRT's. Deels betreft dat operationele taken en deels coördinerende regietaken. Als het gaat om de taken van een CSIRT dan is uitgangspunt voor de wetgeving dat een CSIRT een volledig takenpakket krijgt toebedeeld zoals dit in de wet wordt vastgelegd inclusief de eisen die hieraan worden gesteld. In dit scenario krijgt elke sectorale CSIRT echter een maatwerk takenpakket toebedeeld hetgeen stuit op zeer grote juridische complexiteit (zo niet onmogelijkheid). Ook ontstaan er risico's wanneer er taken tussen wal en schip raken omdat onduidelijk is wie daarvoor dan aansprakelijk is.

De analyse van scenario 2b wordt in de onderstaande tabel samengevat.

Uitgangspunt	Score	Samenvatting toelichting
1a NIS2-eisen	+-	Door het scheppen van een nationale CSIRT en het behouden van sectorale CSIRT's kan aan de eisen van de NIS2 worden voldaan. De maatwerk-aanpak van dit scenario kan een negatieve impact hebben de stevigheid van het CSIRT-stelsel en maakt toezicht, sturing en controleerbaarheid zeer uitdagend.
1b Haalbaarheid uitvoering	-	Maatwerk en fluïditeit in het CSIRT-stelsel zorgen voor complexiteit in de uitvoering, stellen eisen aan maatwerk in toezicht, en compliceren aansturing.
2a NLCS centraal/decentraal	+-	Door behoud van sectorale CSIRT's wordt minder voldaan aan het in de NLCS geformuleerde principe.
2b Bewezen sectorale impact	++	Er wordt hier goed gekeken naar al bewezen impact en deze wordt zoveel mogelijk gehandhaafd.
2c Eén loket	--	Door een maatwerkoplossing in het verdelen van de taken tussen individuele CSIRT's en het NCSC/CSIRT-DSP belanden afnemers veelal bij meerdere loketten voor dienstverlening. Door flexibilisering van de taakverdeling ontstaat verdere onduidelijkheid bij doelgroepen waar zij met hun vragen naartoe kunnen.
2d Inzet schaarse capaciteit	+	Er wordt zoveel mogelijk maatwerk verricht en de expertise ingezet die op een bepaalde plek aanwezig is. Tegelijk

		vereist de maatwerk-aanpak veel tijd en afstemming en dit kost ook middelen en menskracht.
3 Kwaliteitsborging bij vrijwillige CSIRT's	+	Er worden prikkels ingezet om vrijwillige CSIRT's aan te zetten tot kwaliteitsborging wanneer zij toe willen treden tot het stelsel.
4 Lage complexiteit	-	De maatwerkaanpak ten aanzien van sectorale CSIRT's leidt tot complexiteit in het stelsel: elke CSIRT heeft eigen taken en verantwoordelijkheden, en die kunnen doorheen de tijd veranderen. Dit heeft nadelen in termen van de ordening van het stelsel, en CSIRT's zullen daarmee allemaal aan eigen standaarden gehouden moeten worden. Dit maakt toezicht en sturing eveneens complex.
5 Juridisch haalbaar	-	Hoewel het creëren van een CSIRT-stelsel dat in zijn totaliteit de in de NIS2 gestelde taken en eisen afdekt theorie mogelijk is, blijkt dit scenario juridisch moeilijk te realiseren. Met name het maatwerk takenpakket per CSIRT is hierin problematisch. Onderscheid tussen nationale en sectorale CSIRT's (en dubbelrol NCSC/CSIRT-DSP) is ook punt van aandacht.

Scenario 3: Alle bestaande sectorale CSIRT's worden geïntegreerd tot één enkele CSIRT die de wettelijke taken uitvoert voor sectoren die onder de NIS2 vallen

In het derde scenario worden alle bestaande sectorale CSIRT's geïntegreerd in één enkele CSIRT. Nederland heeft daarmee nog maar één enkele sectorale CSIRT die alle sectoren uit de NIS2 bedient. Daarnaast kunnen vrijwillige CSIRT's blijven bestaan. Dit betekent dat alle sectorale CSIRT's die momenteel in het landschap aanwezig zijn en onder de NIS2 (komen te) vallen samengaan. Uiteraard zullen verschillende sectoren met CSIRT-functionaliteit moeten worden bediend, dus zullen waarschijnlijk sectorspecifieke afdelingen of subdivisies gecreëerd worden binnen deze (zeer omvangrijke) organisatie.

Voor sectoren met entiteiten die niet allemaal NIS2-verplichtingen hebben, zal aanvullend moeten worden besloten hoe deze bediend worden. Mogelijk moeten hiervoor nieuwe separate vrijwillige CSIRT's worden ingesteld. Voor de kortere termijn lijkt het in dit scenario niet haalbaar om ook voor entiteiten zonder NIS2-verplichtingen het gezamenlijke CSIRT beschikbaar te maken als in ogenschouw wordt genomen dat de uitbreiding van entiteiten als gevolg van de NIS2 al een

enorme uitdaging met zich meebrengt alsook een integratietraject om een gezamenlijk CSIRT te vormen.

Bij de mapping van de verschillende uitgangpunten op dit scenario komt het volgende beeld naar voren.

Scenario 3 - wettelijke kaders (waaronder NIS2)

Dit scenario sluit heel goed aan bij de nieuwe taken eisen die de NIS2 stelt (++). Volgens de richtlijn moet elke lidstaat tenminste één sectorale CSIRT hebben, die aan alle in de wet gestelde eisen moet (kunnen) voldoen en waarbij alle taken worden uitgevoerd. Met het aanwijzen van een enkel CSIRT zou Nederland dus voldoen aan die wettelijke verplichting. Deze sectorale CSIRT zou dan wel alle taken uit de NIS2 onder haar hoede moeten nemen, van hoog technisch en zeer specialistisch tot generiek, en van sectorspecifiek tot sector-overstijgend en overkoepelend. Deze ene CSIRT zou in dit scenario alle sectoren die in de NIS2 worden genoemd moeten bedienen. Ook zou het als nationaal aanspreekpunt (nationale CSIRT) moeten fungeren.

Dit alles heeft stevige implicaties voor de omvang van de organisatie. Deze nieuwe gezamenlijke organisatie is een uitvoeringsorganisatie van stevig formaat, met implicaties voor organisatiebeheersbaarheid en slagkracht. In termen van haalbaarheid scoort dit scenario niet zo goed (-). Aan de ene kant kan integratie leiden tot meer efficiëntie in het beleggen van taken. Tegelijk zal de hoeveelheid taken én het aantal te bedienen entiteiten met de komst van de NIS2 zeer sterk toenemen, wat grote druk zet op de omvang van de organisatie en de haalbaarheid van het leveren van diensten aan al die groepen volgens de wettelijke eisen. Voor de korte termijn is het, in het licht van beschikbare capaciteit van mensen op de arbeidsmarkt, bovendien onwaarschijnlijk dat een dergelijke grote organisatie gerealiseerd kan worden. Voor de middellange termijn zal dit wellicht wel kunnen lukken. Een zeer grote organisatie heeft bovendien ook nadelen in termen van kosten en effectiviteit, doordat extra overhead ontstaat, samenwerkingsverbanden niet noodzakelijkerwijs beter verlopen binnen een grote organisatie dan tussen meerdere kleine organisaties, en slagkracht in een grote organisatie zoals gezegd ook onder druk kan komen te staan.

Scenario 3 - NLCS

In scenario 3 wordt tegemoetgekomen aan de in de NLCS genoemde doelstelling van ‘centraal als het kan en decentraal als het moet’ (+). Er is in dit scenario immers sprake van één enkele gecentraliseerde CSIRT. Tegelijkertijd roept volledige centralisatie de vraag op waar de tweede helft van het principe gebleven is: decentraal als het moet. Van decentrale activiteiten is namelijk geen sprake meer. Een grote centrale organisatie maakt toegankelijkheid voor de doelgroepen en zichtbare betrokkenheid een aanzienlijk grotere uitdaging.

Bovendien sluit dit scenario zeer slecht aan bij de wens om bewezen impact zo veel mogelijk te handhaven: activiteiten die hun impact bewezen hebben, worden desondanks geïntegreerd in één enkel CSIRT ondanks hun impact (--).

Daarentegen is er in dit scenario meer dan bij alle andere scenario's sprake van één duidelijk loket te voor afnemers (++). Immers, alle doelgroepen die vallen onder de NIS2 zullen voor alle in de richtlijn gestelde diensten worden bediend vanuit één enkele sectorale CSIRT, die bovendien ook de nationale CSIRT-rol zal vervullen.

Tot slot kan er in scenario 3 zowel winst geboekt worden ten aanzien van de inzet van capaciteit als ook verlies worden geleden (+-). Door centralisatie in één centrale CSIRT kunnen schaarse mensen en middelen ingezet worden binnen een enkele organisatie, en daarmee kan schaarse expertise maximaal benut worden. Tegelijkertijd is er bij een zeer omvangrijke organisatie ook een risico op het verlies van efficiëntie, bijvoorbeeld door de noodzaak van het creëren van extra overhead en het investeren in overlegstructuren om samenwerking te faciliteren. Tot slot kan werving lastiger zijn omdat niet iedereen zich thuis zal voelen bij zo'n grote organisatie.

Scenario 3 – vrijwillige CSIRT's

In dit scenario is de vraag hoe om te gaan met de entiteiten die geen NIS2-verplichtingen hebben. Op korte termijn lijkt het niet realistisch dat deze ook bediend kunnen worden door de centrale CSIRT. Dat betekent dat voor hen aparte vrijwillige CSIRT's moeten worden ontwikkeld. Omdat voor sommige (of wellicht zelfs veel) sectoren een hybride situatie aan de orde is waarbij een deel van de entiteiten onder de NIS2 gaat vallen kan dit betekenen dat de huidige sectorale CSIRT's in afgeslankte vorm zullen willen blijven bestaan.

Voor wat betreft de kwaliteitsborging voor **vrijwillige CSIRT's** geldt in scenario 3 hetzelfde als in scenario 2a en 2b (+). Hoewel er in dit scenario geen CSIRT-stelsel wordt gecreëerd omdat er slechts één CSIRT is, is het desondanks wel mogelijk om voorwaarden te stellen voor samenwerking met, of aansluiting op, die ene CSIRT. Dit betekent dat ook in dit scenario aan vrijwillige CSIRT's gevraagd zou kunnen worden om aan kwaliteitsborging te doen als voorwaarde om bijvoorbeeld aangesloten te kunnen worden op het LDS of onderdeel te worden van informatiedelingssystemen.

Scenario 3 – complexiteit

In termen van complexiteit scoort scenario 3 goed (+). In vergelijking met de andere scenario's biedt dit scenario de meest eenvoudige inrichting van het landschap. Wanneer alle taken bij één organisatie belegd worden en alle doelgroepen door die ene organisatie bediend worden, is de complexiteit zo laag mogelijk. Tegelijkertijd ligt er wel een extra uitdaging. Gezien het feit dat het nieuwe centrale CSIRT alle onder de NIS2 ressorterende sectoren zou moeten bedienen, is het waarschijnlijk dat betrokkenheid vanuit vakdepartementen bij dit ene CSIRT noodzakelijk is. Ook ligt er een extra uitdaging ten aanzien van de ondersteuning van de rest van het landschap

(zonder NIS2-verplichtingen). Zo kan er ongemerkt alsnog een nieuw complex landschap ontstaan voor entiteiten zonder NIS2-verplichtingen.

Scenario 3 – juridische haalbaarheid

Scenario 3 is op basis van eerste inschattingen van de wetgevingsjuristen haalbaar (+). Het is mogelijk om één sectorale CSIRT te creëren die alle wettelijke taken uit de NIS2 voor haar rekening neemt en alle sectoren bedient die onder deze richtlijn vallen. Een risico voor een geïntegreerde CSIRT in Nederland is dat de organisatie een 'single point of failure' wordt in juridische zin. Als deze CSIRT onvoldoende in staat zou blijken te voldoen aan de wettelijke eisen, of onvoldoende taken zou kunnen vervullen, dan zijn er geen andere sectorale CSIRT's aan wie een deel van die taken zouden kunnen worden overgedragen. Zeker voor de korte termijn, waarin het zoals gesteld uitdagend kan zijn een zo omvangrijke organisatie op te tuigen, wordt dit ingeschat als een reëel risico.

De analyse van scenario 3 wordt in de onderstaande tabel samengevat.

Uitgangspunt	Score	Samenvatting toelichting
1a NIS2-eisen	++	Met de keuze voor één sectorale CSIRT zou Nederland voldoen aan de basiseisen van de NIS2. Die ene sectorale CSIRT moet dan wel alle onder de NIS2 gestelde taken uitvoeren en alle onder die richtlijn benoemde sectoren bedienen. Dit betekent dat het een omvangrijke uitvoeringsorganisatie zou worden.
1b Haalbaarheid uitvoering	-	De haalbaarheid staat in dit scenario onder druk. De haalbaarheid is al een uitdaging door de toevoeging van extra sectoren onder de NIS2. Als daaraan een groot integratieprogramma tussen alle sectorale CSIRT's moet wordt toegevoegd komt de uitvoering van de NIS2 erg onder druk te staan. Bovendien kan ook de omvang van de organisatie een negatief effect hebben op samenwerking, slagkracht en effectiviteit.
2a NLCS centraal/decentraal	+	In dit scenario is alles gecentraliseerd. Dit komt in zekere zin tegemoet aan het principe van centralisatie zoals geformuleerd in de NLCS, maar roept wel (duurzaam) de vraag op of decentralisatie in sommige gevallen niet beter was (geweest).
2b Bewezen sectorale impact	--	In dit scenario wordt de behaalde sectorale impact tenietgedaan omdat de

		kleinere sectorale CSIRT's zullen opgaan in het nieuwe centrale CSIRT.
2c Eén loket	++	Er is nog maar één CSIRT voor de NIS2-sectoren in Nederland, dus daarmee is er één herkenbaar loket. Voor de overige entiteiten kunnen er aparte sectorale CSIRT's ontstaan en is dat hun loket.
2d Inzet schaarse capaciteit	+-	Er zijn voordelen aan het centraliseren van alle schaarse capaciteit in één enkele organisatie, zodat kennis en expertise maximaal benut kunnen worden. Tegelijkertijd kan een zeer grote organisatie ook hogere kosten met zich meebrengen en is er een risico dat efficiëntie verloren gaat of werving lastiger is vanwege de omvang van de organisatie.
3 Kwaliteitsborging bij vrijwillige CSIRT's	+	Ook in dit scenario is het mogelijk om aan de samenwerking tussen vrijwillige CSIRT's en de centrale CSIRT bepaalde voorwaarden te stellen in de vorm van kwaliteitsborging door de vrijwillige CSIRT's.
4 Lage complexiteit	+	Dit is de oplossing die het minst complex is. Wel kan voor de entiteiten die geen NIS2-verplichtingen hebben een onoverzichtelijk landschap ontstaan.
5 Juridisch haalbaar	+	De wettelijke NIS2-taken kunnen in dit scenario allemaal bij één organisatie worden belegd. Wel ontstaan er risico's doordat het ook kwetsbaar is om alle taken bij één organisatie te beleggen.

SCENARIOKEUZE

De analyse van de scenario's laat zien dat alle genoemde opties voor- en nadelen hebben wanneer ze gemapt worden op de uitgangspunten. Vaak kleven er (grote) voordelen aan een bepaald scenario in relatie tot een specifiek uitgangspunt, die in een ander scenario juist leiden tot grote nadelen of andersom. Zo scoort *bewezen impact* logischerwijs hoog bij de scenario's waarin sectorale CSIRT's worden behouden, en juist laag bij het scenario waarin zij worden opgeheven. En scoort *één loket* hoog bij centralisatie en lager bij een landschap met meerdere sectorale CSIRT's. Een gulden middenweg, waarbij op alle uitgangspunten maximaal gescoord kan worden, is er helaas niet. Dit betekent dat bij de keuze van een scenario twee zaken van belang zijn:

1. Met de komst van de NIS2 zullen er onherroepelijk wijzigingen moeten worden doorgevoerd ten opzichte van het heden. Daarbij zullen partijen moeten accepteren dat een keuze voor welk scenario dan ook naast veel goede zaken ook minder optimale consequenties zal hebben. Hieraan is niet te ontkomen.
2. Niet elk uitgangspunt weegt even zwaar mee in de definitieve afweging. Door gebruik te maken van een scoringsmechanisme, zoals in deze analyse is gedaan, kan de indruk ontstaan dat elk uitgangspunt even zwaar weegt. Een '-' onder *NLCS centraal/decentraal* zou zo bijvoorbeeld ogenschijnlijk hetzelfde gewicht hebben als een '-' onder *Haalbaarheid in uitvoering*.

In onderstaande tabel zijn de scores samengevat die in de vorige paragrafen inhoudelijk zijn toegelicht.

Scenario	1a NIS2-eisen	1b Haalbaarheid uitvoering	2a NLCS-centraal/decentraal	2b Bewezen sectorale impact	2c Eén loket	2d Inzet schaarse capaciteit	3 Kwaliteitsborging vrijwillige CSIRT' s	4 Lage complexiteit	5 Juridisch haalbaar
1 Wettelijke taken in huidig landschap	--	--	--	+	-	+-	--	-	--
2a Structuur + homogene CSIRT's	+	+	+-	++	+	++	+	+-	+
2b Structuur + maatwerk-CSIRT's	+-	-	+-	++	--	+-	+	-	-
3 Eén centraal CSIRT voor alle sectoren	++	-	+	--	++	+-	+	+	+

Tabel 6 Mapping uitgangspunten op scenario's CSIRT-stelsel

Bij de definitieve weging van de scenario's zijn de volgende uitgangspunten zwaarder meegewogen:

- 1a NIS2-eisen
- 1b Haalbaarheid uitvoering
- 2b Bewezen sectorale impact
- 2c Eén loket
- 5 Juridische haalbaarheid

Op basis van de scores en de weging komt naar voren dat **scenario 2a als meest optimale scenario** naar voren komt. In de analyse valt op dat dit het **enige**

scenario is dat positief scoort op haalbaarheid en **overall geen negatieve scores** behaalt. Verder wordt duidelijk dat het eerste scenario, waarbij de wettelijke taken zonder substantiële wijzigingen in het huidige landschap worden geïntegreerd niet haalbaar is. Deze haalt alleen op bewezen sectorale impact (+) en inzet schaarse capaciteit (+-) positieve scores, maar verder pakken alle uitgangspunten hier negatief uit. Verder valt op dat scenario 2a een positieve combinatie vormt van wat er goed tot zeer goed werkt in ofwel scenario 2b (bewezen sectorale impact) ofwel in scenario 3 (NIS2 taken beleggen, één loket en juridisch haalbaar), maar niet negatief scoort op enkele belangrijke uitgangspunten waar scenario 2b (haalbaarheid, één loket, lage complexiteit, juridisch haalbaar) of scenario 3 (haalbaarheid, bewezen sectorale impact) dat wel doen. Met andere woorden, voor enkele belangrijke uitgangspunten pakken zowel scenario 2b als scenario 3 niet goed uit.

Omdat de verschillen tussen de scenario's zo groot zijn en scenario 2a zo duidelijk uit de analyse naar voren komt als voorkeursscenario, is ervoor gekozen om in dit rapport alleen dit scenario in detail uit te werken.

HERONTWERP CSIRT-STELSEL

Uit de analyse van de mogelijke scenario's voor het CSIRT-stelsel is duidelijk geworden dat het nodig is om een herontwerp van het CSIRT-stelsel te maken. Er is gebleken dat er geen ideaal-oplossing is en dat er één scenario is dat veel voordelen heeft en de minste nadelen:

> *Scenario 2a: inrichting van een stelsel met meerdere sectorale CSIRT's met wijzigingen voor wat betreft taakverdeling, governance en toezicht; toevoeging van één nationale CSIRT voor sector overstijgende taken; alle sectorale CSIRT's die onder NIS2 vallen voeren dezelfde set taken uit*

In dit hoofdstuk wordt dit scenario in meer detail uitgewerkt.

Visie op het toekomstig CSIRT-stelsel

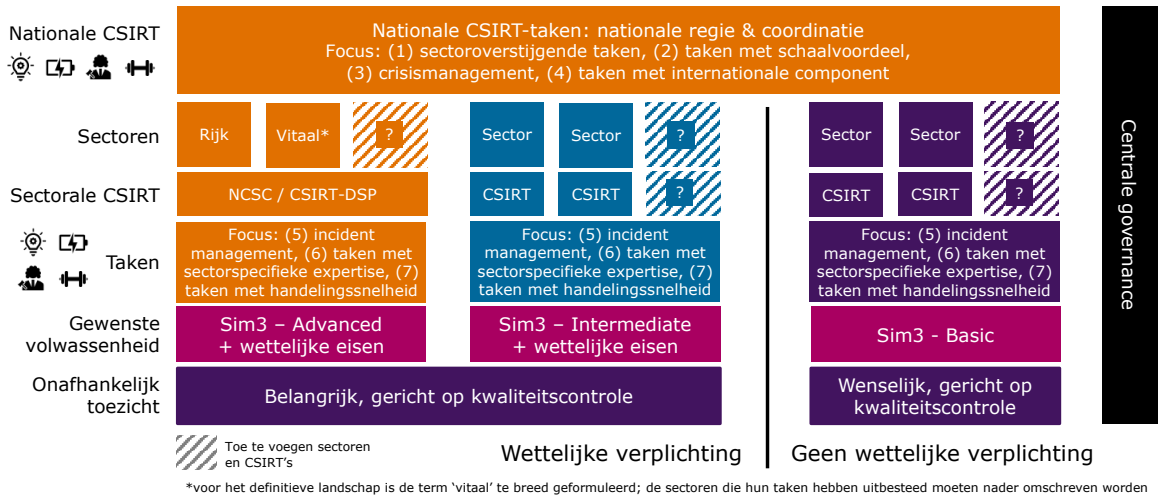
In de verkenning zijn op basis van de input uit de verkenningsgesprekken en de uitgangspunten de verschillende elementen die van belang zijn voor het CSIRT-stelsel nader uitgewerkt. Deze elementen zijn:

1. Scheiding tussen nationale en sectorale CSIRT-taken. In de NIS2 zijn er naast verplichte operationele CSIRT-taken ook enkele regie en coördinatietaken gedefinieerd. Passend binnen de NLCS is het de bedoeling deze toe te kennen aan een verder in te richten nationale CSIRT. In het stelsel moet dus een scheiding worden aangebracht tussen nationale en sectorale CSIRT-taken.
2. Aanbrengen van scope in de kerntaken van een sectorale CSIRT. Er moet worden bepaald hoe de taken binnen het stelsel worden verdeeld en gekeken of bestaande frameworks hierbij ondersteuning kunnen bieden.
3. Stellen van eisen aan de taakvolwassenheid van sectorale CSIRT's. Het is van belang om goede afspraken te maken over de wijze waarop taakvolwassenheid kan worden gemeten en welke ambitie het stelsel bij de taakvolwassenheid heeft.

Daarbij zijn de eisen uit de wettelijke richtlijnen (zoals de NIS2, Netcode) een minimale vereiste.

4. Ruimte geven aan vrijwillige sectorale CSIRT's. In de NIS2 staan sectoren vermeld waarvoor de NIS2-verplichtingen gaan gelden. Er zijn ook sectoren die niet met deze verplichting te maken krijgen en toch een sectoraal CSIRT willen inrichten. Vanuit het oogpunt van informatiedeling is het ook hier van belang om kaders te stellen. Daarnaast zal er in de praktijk sprake zijn van sectoren waarvan slechts een deel van de entiteiten te maken krijgen met de NIS2. Ook hier moet in het ontwerp rekening mee worden gehouden.
5. Het verbeteren van de besturing van het CSIRT-stelsel. Het inrichten van governance voor het stelsel alsook toezicht op de kwaliteit is hier belangrijk, zoveel mogelijk aansluitend op bestaande governancestructuren.
6. Het verbeteren en bevorderen van onderlinge samenwerking. Het wordt naar de toekomst nog belangrijker om binnen het CSIRT-stelsel samen te werken. Deels volgt dit uit de vereisten van de NIS2, maar ook is dit gewenst voor een optimale werking van het stelsel.

In onderstaande figuur zijn de elementen 1 tot en met 5 schematisch weergegeven. Deze zullen stap voor stap in de volgende paragrafen worden toegelicht gevolgd door een paragraaf over het verbeteren en bevorderen van onderlinge samenwerking tussen de CSIRT's.



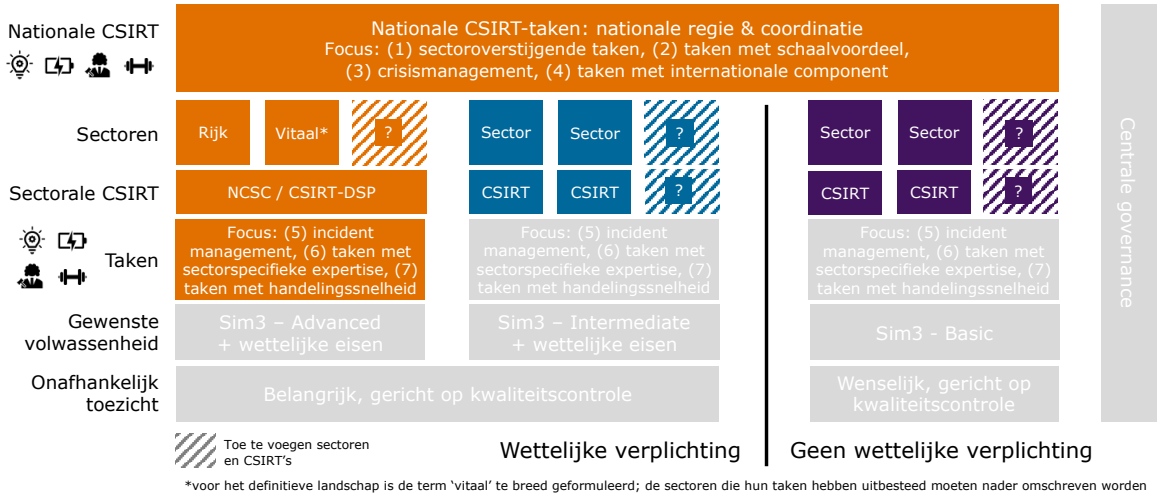
Figuur 13 - Visie op toekomstig CSIRT-stelsel

Scheiding tussen nationale en sectorale CSIRT-taken

In het herontwerp van het CSIRT-stelsel is ruimte gemaakt voor een nationale CSIRT. De regie- en coördinatietaken die voortkomen uit de NIS2 worden bij de nationale CSIRT belegd. Ook worden de centraal op te pakken taken in het stelsel toegekend aan de nationale CSIRT.

Daarnaast zijn er sectorale taken die moeten worden uitgevoerd. Deze worden belegd bij sectorale CSIRT's. Merk daarbij op dat het NCSC/CSIRT-DSP in het nieuwe stelsel een dubbelrol zal gaan vervullen en zowel de rol op zich zal nemen van nationale

CSIRT als de rol van sectorale CSIRT voor de aan deze organisatie toegewezen sectoren[40].



Figuur 14 - Nationaal versus sectoraal

Aanbrengen van scope in de kerntaken van een sectorale CSIRT

Voor wat betreft de CSIRT-taken wordt in dit scenario uitgegaan van een vast pakket met kerntaken voor alle sectorale CSIRT's. Elk sectorale CSIRT krijgt dus hetzelfde takenpakket met kerntaken toegewezen en moet zorgen dat deze kunnen worden uitgevoerd. Eventuele extra andere taken buiten dit pakket zijn natuurlijk ook mogelijk, maar dat valt verder buiten de scope van dit rapport.

In het huidige landschap zijn geen afspraken gemaakt over de kerntaken die een CSIRT zou moeten uitvoeren. Zoals in de analyse duidelijk is geworden is het in elk geval nodig om afspraken vast te leggen over de kerntaken die CSIRT's uitvoeren die entiteiten bedienen met wettelijke verplichtingen (vanuit de NIS2 en sectorspecifieke richtlijnen). Zij zullen in elk geval de taken moeten doen die in de betreffende richtlijn zijn vastgelegd. Daarnaast is het verstandig om eenduidigheid in het takenpakket aan te brengen door gebruik te gaan maken van een framework voor CSIRT-taken. Op basis van de analyse over bestaande frameworks is de conclusie dat het FIRST CSIRT Services Framework hiervoor geschikt is (zie pagina 31).

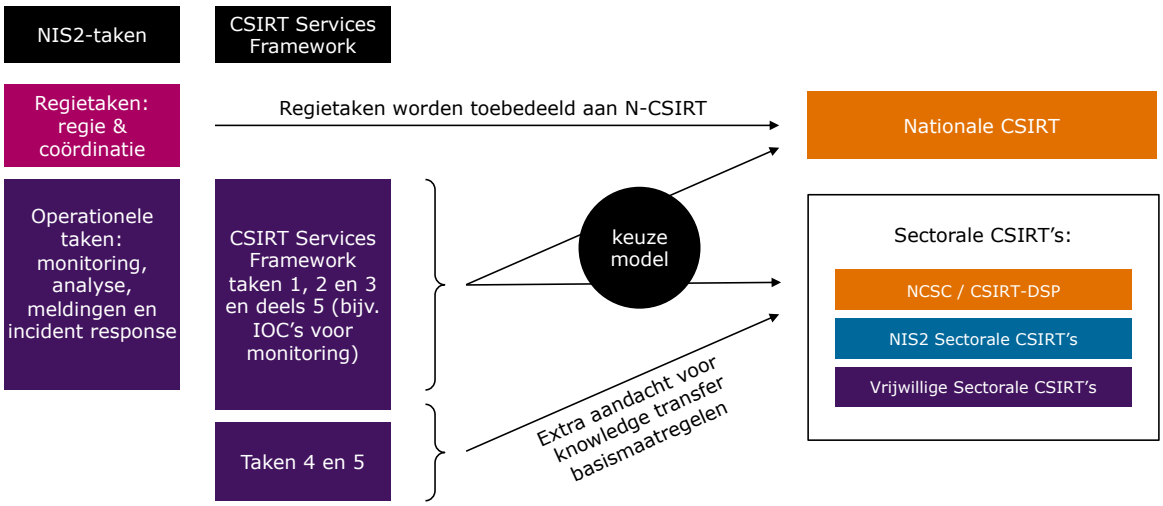
Dit framework is voldoende breed om te passen binnen de scope die binnen dit rapport is beschouwd voor de kerntaken van een CSIRT (zie Figuur 3) en beschrijft taken op gebied van ondersteuning bij incidenten, vulnerability management, situationeel beeld, kennisoverdracht en (ondersteuning bij) monitoring (zie Figuur 9). Het toepassen van dit framework maakt dat er duidelijkheid ontstaat over wat er van een CSIRT wordt verwacht en kunnen sectorale CSIRT's onderling worden vergeleken. Het gebruik van dit framework betekent dat alle sectorale CSIRT's de in het CSIRT Services Framework beschreven taken moeten inrichten.

[40] Merk op dat op dit moment het grootste deel van de taken van het NCSC/CSIRT-DSP sectorale taken betreft, zie de beschrijving van het huidige landschap op pagina 6.

Daarnaast moeten de CSIRT's die vallen binnen het NIS2-domein afspraken vastleggen over welke wettelijke taken door het nationale CSIRT en welke door de sectorale CSIRT's worden opgepakt. In het hoofdstuk over de frameworks (zie pagina 31) is duidelijk geworden dat deze taken passen binnen het CSIRT Services Framework, met name binnen de processen voor ondersteuning bij incidenten, vulnerability management en situationeel beeld.

Omdat de NIS2-richtlijn heel specifieke taken beschrijft is de algemene omschrijving in het CSIRT Services Framework niet afdoende om te borgen dat al deze taken goed worden belegd. Bovendien moeten de kerntaken verdeeld worden tussen de nationale CSIRT en de sectorale CSIRT's (met zoals eerder genoemd de dubbelrol van het NCSC/CSIRT-DSP). Een belangrijke vervolgvraag is daarom hoe de taken dan verdeeld moeten worden. Deels is deze vraag eenvoudig te beantwoorden (zie ook Figuur 15):

- De in de NIS2 gedefinieerde regie- en coördinatietaken (zie pagina 21) kunnen allemaal worden toebedeeld aan de nationale CSIRT.
- De taken in het CSIRT Services Framework die niet overlappen met de NIS2-taken kunnen allemaal worden toebedeeld aan de sectorale CSIRT's. Hierbij is uit de verkenningsgesprekken gebleken dat hier extra aandacht nodig is voor het overdragen van kennis over de basismaatregelen die in specifieke sectoren nodig zijn. Hoewel er geen wettelijke verplichting is om het volledige takenpakket uit het CSIRT Services Framework toe te bedelen, is het advies dit toch te doen om daarmee eenduidigheid in de taakverdeling van de CSIRT's aan te brengen.



Figuur 15 - Verdeling van taken tussen nationale CSIRT en sectorale CSIRT's

Voor de overige taken (de verplichte NIS2-taken, passend binnen de categorieën 1, 2 en 3 uit het CSIRT Services Framework) is de verdeling een complexer vraagstuk. Een deel van deze taken moet worden belegd bij het nationale CSIRT en een deel bij de sectorale CSIRT's. Uit analyse van deze taken is gebleken dat de toekenning niet eenduidig is en nadere afstemming tussen de CSIRT's behoeft. Op basis van enkele hoofdcriteria is een primaire indeling te maken.

Zo kunnen de volgende soorten taken primair worden toebedeeld aan de nationale CSIRT:

1. Taken die relevantie hebben voor veel verschillende sectoren
2. Taken die efficiënter/goedkoper uitgevoerd kunnen worden door centralisatie (schaalvoordeel)
3. Crisismanagement (grote incidenten en incidenten met een sector overschrijdend karakter)
4. Taken met brede internationale impact

Onderstaande taken zijn primair toe te kennen aan een sectorale CSIRT (waarbij de nationale CSIRT waar nodig samenwerkt en ondersteunt):

5. Incident management (incidenten die binnen een sector optreden)
6. Taken met sectorspecifieke expertise
7. Taken waarvoor handelingssnelheid nodig is richting sectorale organisaties en gebruik gemaakt moet worden van een breed beschikbaar netwerk

Echter, deze hoofdcriteria kunnen in specifieke situaties overlappen en er zijn daarom nadere afspraken nodig in welke situatie welk criterium als leidend wordt gezien. Als een incident bij een bepaalde organisatie begint maar uitgroeit tot een crisis, of na enige tijd blijkt dat er vergelijkbare incidenten in andere sectoren optreden, moet er vastgelegd worden hoe hiermee om te gaan. Het is nodig dat hiervoor vanuit de praktijk scenario's worden uitgewerkt en besloten en vastgelegd wordt hoe deze aan te pakken.

Ook spelen hierbij nog enkele andere criteria een rol:

A. Expertise. Is er voldoende (sectorspecifieke) expertise voor het uitvoeren van de benodigde taken?
B. Resources. Zijn er voldoende resources (mensen, geld, faciliteiten) beschikbaar?
C. Juridische grondslag. Biedt de wet voldoende mogelijkheden voor het uitvoeren van een taak door de sectorale of nationale CSIRT? Bijvoorbeeld doordat een sectorale CSIRT een afwijkend besturingsmodel heeft.
D. Maatschappelijk of economisch belang. Als er sprake is van situaties die de maatschappij breed raken of grote economische impact hebben, dan kan een overweging zijn deze vanuit de nationale CSIRT op te pakken. Wel moet heel helder zijn in welke situaties dit wel en niet gebeurt.

Het is van belang om de opgedane ervaring vanuit de CSIRT's te gebruiken om te komen tot een definitieve verdeling van taken vanuit praktijkscenario's. Bovendien moeten deze taken periodiek worden geëvalueerd omdat op basis van actuele ontwikkelingen en ervaring in sommige situaties andere keuzes in het takenpakket nodig kunnen blijken. Bij de start van het nieuwe stelsel zal eenmalig een eerste verdeling gezamenlijk moeten worden vastgesteld op basis van input van experts vanuit de CSIRT's die in het stelsel zullen deelnemen waarna een periodieke evaluatiecyclus kan worden ingericht. Het is van belang dat de keuze onder

begeleiding van de stelselcoördinator door de CSIRT's gezamenlijk wordt gemaakt op basis van de hierboven genoemde principes en criteria.

Tot slot is het vanuit de NIS2 nodig dat de CSIRT's die in dit deel van het CSIRT-stelsel actief zijn gezamenlijk alle sectoren bedienen die in de bijlagen van de NIS2 zijn opgenomen. Omdat in de verkenning helder is geworden dat in het huidige stelsel niet al deze sectoren kunnen rekenen op ondersteuning is het van belang dat hierin op korte termijn duidelijkheid ontstaat door:

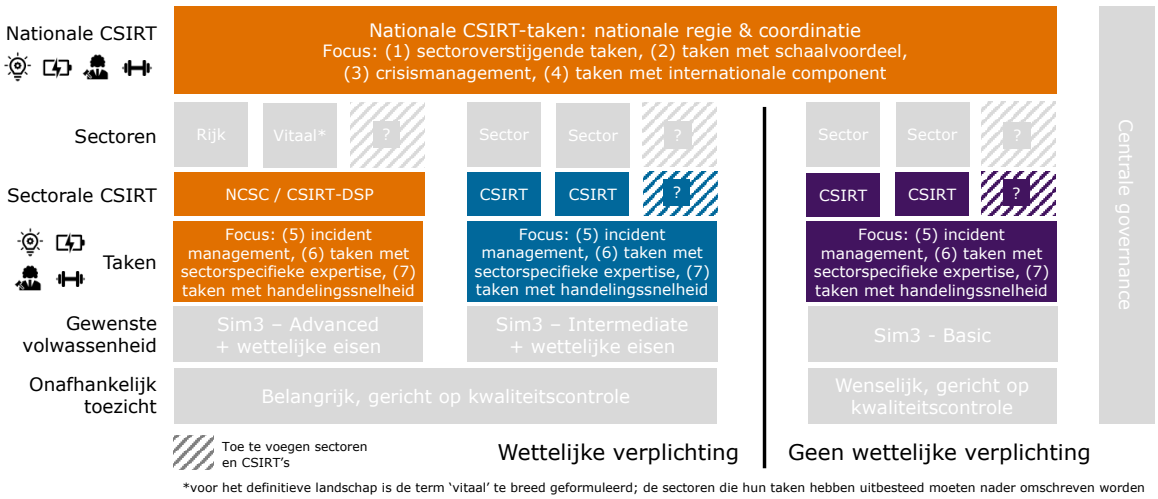
1. Vast te stellen welke doelgroeporganisaties in Nederland binnen de reikwijdte van de NIS2 gaan vallen.
2. Te analyseren welke van deze doelgroeporganisaties op dit moment nog niet bediend worden door een sectorale CSIRT of daar logischerwijs bij zouden horen.
3. Afspraken te maken over hoe deze organisaties binnen het CSIRT-stelsel een sectorale CSIRT krijgen toegewezen. Hiervoor zijn drie mogelijkheden:
    a. Deze worden toegevoegd als extra doelgroep aan het NCSC/CSIRT-DSP (in haar rol als sectorale CSIRT).
    b. Deze worden toegevoegd als extra doelgroep aan een andere bestaande sectorale CSIRT.
    c. Er moet voor deze sector een nieuwe sectorale CSIRT worden opgericht.

    Wel moet hierbij worden opgemerkt dat vanuit de NLCS de eerste te onderzoeken optie (a) is, maar bij moverende redenen ook voor opties (b) of (c) kan worden gekozen.

Een extra complexiteit bij de verdeling van taken kunnen (nieuwe) sectorspecifieke richtlijnen zijn. Voor iedere nieuwe sectorspecifieke richtlijn moet voorafgaande aan de inwerkingtreding worden geanalyseerd welke eisen deze stelt aan de CSIRT-taken en in hoeverre dit het takenpakket van een sectoraal CSIRT betreft. Idealiter worden extra taken aan alle sectorale CSIRT's toegekend om de uniformiteit in het stelsel te behouden. Als dit niet mogelijk of wenselijk blijkt, kan hier een uitzondering gemaakt worden in het takenpakket van de sectorale CSIRT die te maken krijgt met zo'n sectorspecifieke richtlijn.

Figuur 16 geeft schematisch weer hoe de primaire taakverdeling tussen de sectorale CSIRT's en nationale CSIRT eruit komt te zien (zonder de uitkomst van het proces met het keuzemodel expliciet zichtbaar te maken).

Tot slot moet worden opgemerkt dat het stelsel richting de toekomst flexibel om moet gaan met nieuwe ontwikkelingen, zoals bijvoorbeeld de introductie van nieuwe frameworks. Vanuit governance perspectief is het daarom verstandig om periodiek de wijze waarop de taken zijn gestructureerd te evalueren en waar nodig aan te passen aan nieuwe eisen en standaarden.



Figuur 16 - Verdeling van de sectorale CSIRT-taken

Stellen van eisen aan de taakvolwassenheid van sectorale CSIRT's

De NIS2 stelt heldere eisen aan de taakvolwassenheid (zie pagina 23). Deze eisen zijn vanzelfsprekend van toepassing op de sectorale CSIRT's in Nederland die doelgroepen bedienen die onder de NIS2 gaan vallen. Sectorspecifieke richtlijnen kunnen voor bepaalde sectorale CSIRT's nog aanvullende eisen stellen.

Hoewel er geen wettelijke plicht is om daarnaast nog andere eisen aan de nationale en sectorale CSIRT's op te leggen is het advies om ook hier aanvullend een framework in te zetten, namelijk het ENISA CSIRT Maturity Framework (zie pagina 33). Dit framework kent heldere niveaus toe aan de taakvolwassenheid van CSIRT's en maakt daarmee inzichtelijk wat het overal volwassenheidsniveau van een specifieke CSIRT is en biedt daarnaast de mogelijkheid tot het maken van vergelijkingen, hetgeen vanuit sturingsperspectief van belang is. Het gebruik van dit framework sluit bovendien aan bij het EU CSIRT's Network, dat aangesloten CSIRT's aanmoedigt het *Intermediate*-niveau te behalen.

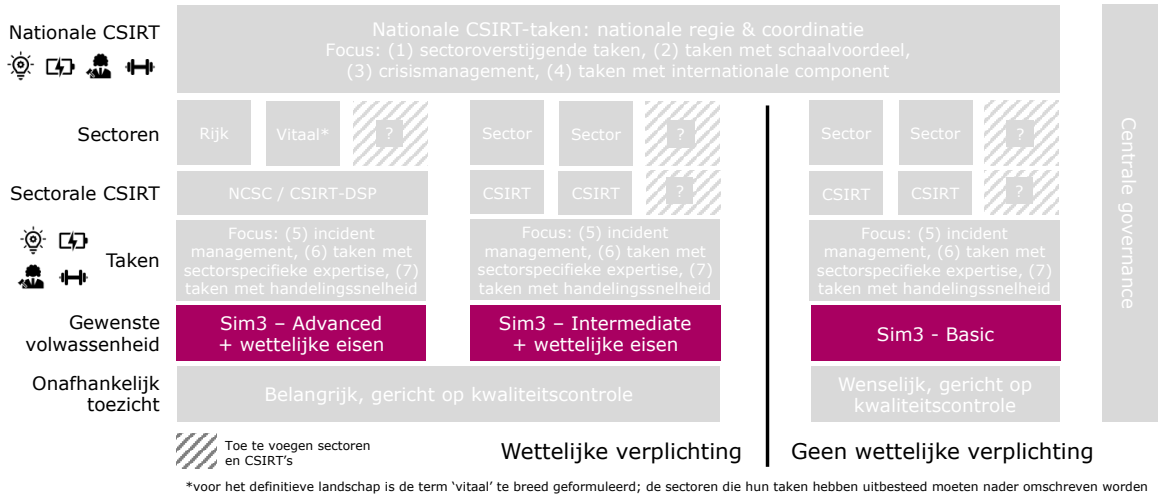
Het advies is om minimaal de volgende niveaus in volwassenheid te vereisen:

- *Basic* voor de vrijwillige sectorale CSIRT's die zijn aangesloten vanuit het Landelijk Dekkend Stelsel (zie volgende paragraaf).
- *Intermediate* voor de sectorale CSIRT's met wettelijke verplichtingen, in overeenstemming met aanmoediging vanuit het EU CSIRTs Network.
- *Advanced* voor het NCSC/CSIRT-DSP in haar dubbelrol als sectorale CSIRT en nationale CSIRT, omdat de nationale CSIRT-rol vraagt om een bredere verantwoordelijkheid waarbij het hoogste niveau van volwassenheid wenselijk is.

De verwachting is dat voor de meeste sectorale CSIRT's op dit moment het behalen van deze niveaus een uitdaging kan vormen. Advies is daarom om in 2023 een nulmeting uit te voeren voor de sectorale CSIRT's die in het stelsel actief zullen zijn en vanuit daar met ieder van hen vanuit governance-perspectief een realistisch groeipad af te spreken om het gewenste niveau te behalen. Let wel dat bij inwerkingtreding van de NIS2, Netcode en eventuele andere sectorspecifieke

richtlijnen de bijbehorende eisen op dat moment van kracht worden hetgeen betekent dat de nationale CSIRT en de sectorale CSIRT's die met deze richtlijnen te maken krijgen per die datum aan de gestelde eisen moeten voldoen.

Onderstaande figuur geeft schematisch de eisen aan volwassenheid weer.



Figuur 17 - Gewenste taakvolwassenheid van CSIRT's

Ruimte geven aan vrijwillige sectorale CSIRT's

In de verkenning is logischerwijs veel aandacht gegaan naar de implicaties van de wettelijke verplichtingen die ontstaan door de komst van de NIS2 richtlijn en sectorspecifieke richtlijnen. De verplichtingen zijn slechts voor een beperkt aantal entiteiten uit een aantal specifieke sectoren van toepassingen. Bij het creëren van een goed werkend CSIRT-stelsel is het echter van belang om ook een uitspraak te doen over CSIRT-ondersteuning voor entiteiten die niet met wettelijke verplichtingen te maken hebben.

Om te beginnen zal in veel sectoren de situatie optreden dat slechts een deel van de entiteiten te maken krijgt met wettelijke verplichtingen. In theorie zou ervoor gekozen kunnen worden om aparte sectorale CSIRT's te maken voor uitsluitend de entiteiten die te maken hebben met wettelijke verplichtingen. Als andere entiteiten uit dezelfde sector eveneens een beroep op een CSIRT zouden willen doen, dan zou hiervoor een aparte CSIRT kunnen worden gecreëerd. Dit zorgt echter voor versnippering in het landschap, maakt slecht gebruik van schaarse capaciteit en middelen en al opgebouwde sectorspecifieke kennis en netwerken. Het advies is daarom om sectorale CSIRT's die entiteiten voor een sector met wettelijke verplichtingen ondersteunen, deze gehele sector te laten ondersteunen als daaraan behoefte is. Zij hebben daarmee een hybride doelgroep (deels met wettelijke en deels zonder wettelijke verplichtingen).

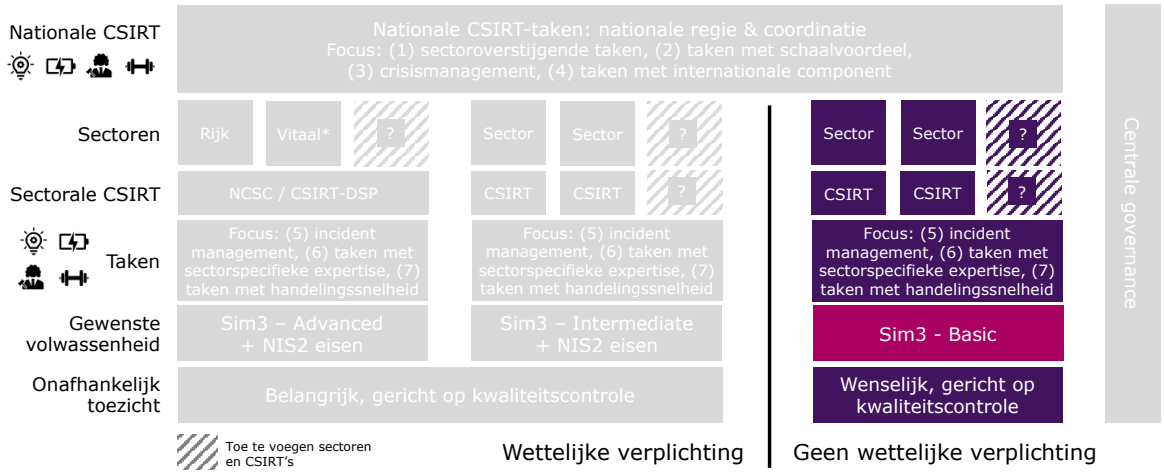
Er zullen ook sectoren kunnen zijn waarvoor (op dit moment) geen wettelijke verplichtingen bestaan om CSIRT-ondersteuning te bieden, maar die op eigen initiatief toch een sectorale CSIRT willen oprichten. Gezien het feit dat deze vrijwillige

CSIRT's buiten de wettelijke eisen vallen, is het uitdagend om ervoor te zorgen dat het niveau van dienstverlening en taakinvulling van vrijwillige CSIRT's afdoende is, en tussen sectoren een bepaalde mate van gelijkmatigheid vertoont. Beiden zijn in het belang van de sectoren die ze bedienen. Voor vrijwillige CSIRT's is het verstandig prikkels in te zetten die hen stimuleren om aan kwaliteitsborging te werken. Het advies is om als prikkel te eisen dat vrijwillige CSIRT's alleen onderdeel mogen worden van het CSIRT-stelsel (inclusief LDS of het informatiedelingslandschap) als zij een minimaal takenpakket uitvoeren en/of voldoende volwassenheid kunnen laten zien.

In dit kader is het advies:

1. Te toetsen of de taken goed passen binnen de scope van een CSIRT door gebruik van het FIRST CSIRT Services Framework.
2. Om een minimale taakvolwassenheid te vragen. Voorstel is om het *Basic*-niveau van het ENISA CSIRT Maturity Framework te hanteren waarvoor periodiek een zelf-assessment moet worden overlegd.
3. Om periodiek onafhankelijk te (laten) toetsen of de betreffende CSIRT nog aan deze eisen voldoet.

Onderstaande figuur geeft het ontwerp voor het vrijwillige deel van het CSIRT-stelsel weer. De CSIRT's met een hybride doelgroep vallen vanwege de wettelijke eisen die op een deel van de doelgroep van toepassing is in het verplichte deel van het CSIRT-stelsel.



Figuur 18 - Vrijwillige maar niet vrijblijvende sectorale CSIRT's

Het verbeteren van de besturing van het CSIRT-stelsel

Het hebben van een stelsel impliceert dat er sprake is van een centrale besturing, maar ook dat er onafhankelijk toezicht is op het nakomen van de gemaakte afspraken binnen het stelsel.

Voor wat betreft governance is belangrijk dat de bij het stelsel betrokken vakdepartementen gezamenlijk het stelsel gaan besturen. Het advies is om bij de implementatie tenminste de volgende elementen verder uit te werken:

- Bij het maken van keuzes in het stelsel is het verstandig de vakdepartementen te betrekken die verantwoordelijk zijn voor de entiteiten uit de sectoren zoals in bijlagen I en II bij NIS2 weergegeven, waarbij het voor de hand ligt om de NCTV als stelselcoördinator aan te stellen.
- De politieke verantwoordelijkheid over het CSIRT-stelsel (nationaal versus sectoraal) dient te worden afgestemd en belegd.

Vanuit governance-perspectief zijn er verschillende vraagstukken, waaronder:

- Het borgen van het juridisch en financieel kader
- Het vastleggen van processen voor wat betreft de toetreding tot het CSIRT-stelsel
- Het maken van keuzes over de ontwikkeling van bestaande sectorale CSIRT's
- Het maken van keuzes over toetredende nieuwe CSIRT's tot het stelsel
- Het maken van keuzes over de verdeling van taken tussen de sectorale CSIRT's en nationale CSIRT
- De inzet van (dezelfde) technische middelen en hoe infrastructuur met elkaar samenwerkt (interoperabiliteit)
- De wijze van invulling van opdrachtgeverschap voor vakdepartementen die hun doelgroepen laten bedienen vanuit het NCSC/CSIRT-DSP (aansturing, budget, etc.)

Voor wat betreft toezicht is het belangrijk dat er onafhankelijk wordt toegezien op de (kwaliteit van) uitvoering van de taken in het stelsel, vooral voor wat betreft de wettelijke verplichtingen. Toezicht op het stelsel gaat over:

- Een regelmatige toets op het uitvoeren van de (verplichte) taken binnen het stelsel.
- Kwaliteitscontrole op de uitvoering (door middel van audits op de taakvolwassenheid).
- Onafhankelijk onderzoek wanneer er incidenten rondom een sectorale CSIRT optreden.

Het is belangrijk om toezicht onafhankelijk in te richten en ook te bepalen hoe het toezicht op het stelsel[41] zich verhoudt tot het toezicht op de entiteiten die door sectorale CSIRT's worden bediend.

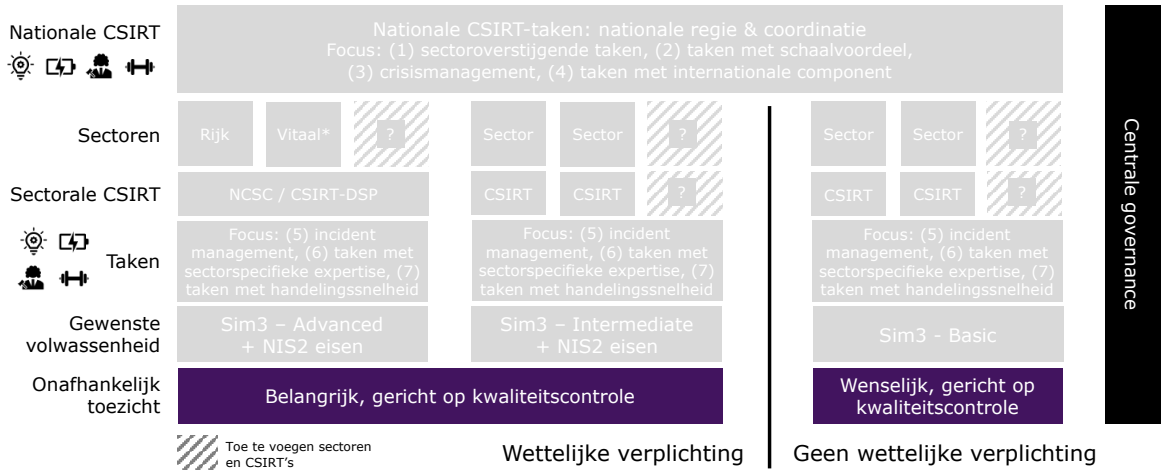
De specifieke invulling van governance en toezicht moet nog nader worden uitgewerkt waarbij het goed is om te zoeken naar oplossingen die goed aansluiten bij al bestaande structuren om extra overhead tot een minimum te beperken.

Tot slot moet worden opgemerkt dat vanuit een landschap met beperkte regie wordt toegewerkt naar een situatie met veel regie. Het zal waarschijnlijk enige tijd kosten

[41] Voor wat betreft toezicht gaat het hier nadrukkelijk niet over toezicht op de entiteiten die door CSIRT's worden bediend, maar over toezicht en controle op het functioneren van de verschillende CSIRT's en het CSIRT-stelsel als totaal.

om dit aspect goed in te richten en het advies is daarom om dit incrementeel aan te pakken.

Onderstaande figuur laat zien hoe governance en toezicht binnen het stelsel past.



Figuur 19 - Besturing van het CSIRT-stelsel

Het verbeteren en bevorderen van onderlinge samenwerking

Een laatste element in het herontwerp van het CSIRT-stelsel is het verbeteren en bevorderen van onderlinge samenwerking in het stelsel. Vanuit wettelijke verplichtingen zal de nationale CSIRT tot taak hebben om een instrumentarium te ontwikkeling voor informatiedeling die breed door de verschillende CSIRT's moet worden ingezet. Maar ook verder zijn er mogelijkheden voor samenwerking waarover in het stelsel verdere afspraken moeten worden gemaakt. Advies is om daarin in elk geval de volgende elementen mee te nemen:

- Het creëren van meer samenhang tussen gebruikte systemen en technologieën, *policies, best practices*, etc.
- Het onderling uitwisselen van best practices
- Het bieden van ondersteuning, bijvoorbeeld door middel van het delen van specifieke kennis van experts, het delen van capaciteit in geval van calamiteiten, etc.
- Het opbouwen van brede expertise op specifieke onderwerpen die meerdere sectorale CSIRT's raken zoals Operational Technogy (OT)
- Het centraal inkopen en waar nodig ontwikkelen van gezamenlijke tools/technologie/infrastructuur die binnen alle sectorale CSIRT's met wettelijke verplichtingen nodig zijn

Advies is om de nationale CSIRT een coördinerende rol te geven in deze activiteiten.

IMPLICATIES WIJZIGINGEN CSIRT-STELSEL

Implementatie van het herontwerp van het CSIRT-stelsel heeft een aantal belangrijke implicaties. Deze implicaties zijn deels een direct gevolg van wettelijke verplichtingen, onder andere door de komst van NIS2.

Voor de CSIRT's die te maken krijgen met wettelijke verplichtingen geldt dat ze voor wat betreft hun kerntaken te maken krijgen met:

- Het CSIRT Services Framework en een nader vast te stellen taakverdeling tussen de nationale CSIRT en de sectorale CSIRT's
- Met eisen aan de taakvolwassenheid, enerzijds vanuit de wettelijke verplichtingen en anderzijds vanuit het ENISA CSIRT Maturity Framework

Het staat sectorale CSIRT's overigens vrij om (via een separate financieringsstroom) andere producten en diensten te leveren, zoals advies op gebied van de implementatie van standaarden, leveranciersmanagement, etc.

Implicaties voor de CSIRT's met wettelijke verplichtingen

Voor het verplichte deel van het CSIRT-stelsel zijn er enkele aanvullende implicaties.

Belangrijk is hier dat de sectorale CSIRT's gezamenlijk alle sectoren moeten bedienen die in de NIS2 zijn aangewezen. Ook moeten de in de NIS2-richtlijn en sectorspecifieke richtlijnen opgenomen taken terugkomen in de taakverdeling tussen de nationale en sectorale CSIRT's. Hierop moet een toets worden gedaan nadat de taken definitief zijn verdeeld.

Als een sector een eigen aparte sectorale CSIRT wil inrichten of handhaven dan zal deze alle verplichte taken waarvan wordt afgesproken dat ze door sectorale CSIRT's worden uitgevoerd op zich moeten nemen. Wel is het mogelijk dat de sectorale CSIRT samen met de andere CSIRT's gezamenlijk over technische capaciteiten kunnen beschikken. Het is niet verplicht dat een CSIRT alle taken zelf technisch uitvoert. Het is bijvoorbeeld mogelijk om voor taken diensten uit de markt te betrekken

Voor bestaande sectorale CSIRT's geldt dat ze in oktober 2024 moeten voldoen aan de eisen die de NIS2 aan hen stelt. Als dit niet haalbaar of wenselijk is, dan moet in gesprek met het NCSC/CSIRT-DSP bekeken worden of de CSIRT-taken door hen kunnen worden overgenomen. Dit impliceert automatisch dat de bestaande sectorale CSIRT ophoudt te bestaan. In alle gevallen moet gezocht worden naar een passende manier om de betreffende sector te bedienen. Als overwogen wordt om een CSIRT te stoppen moet rekening gehouden worden met een overgangstermijn om de continuïteit van de dienstverlening voor de doelgroep te waarborgen. Als in een sector die wordt ondersteund door het NCSC/CSIRT-DSP toch behoefte is aan een entiteit dichter bij de sector zelf kan overwogen worden om in plaats van een CSIRT een eigen weerbaarheidscentrum in te richten. Dat weerbaarheidscentrum heeft dan nadrukkelijk niet de taak om CSIRT-achtige dienstverlening te bieden.

Implicaties voor het vrijwillige deel van het CSIRT-stelsel

Het vrijwillige deel van het CSIRT-stelsel biedt ruimte aan nieuwe CSIRT's. Wel zullen deze aan de beschreven kwaliteitscriteria moeten gaan voldoen. Voor sectoren die buiten de NIS2 vallen is er dus ruimte om te kiezen zelf CSIRT-functionaliteit te ontwikkelen en daarmee aan te sluiten op bredere informatievoorziening, bijvoorbeeld vanuit het Landelijk Dekkend Stelsel. Merk op dat het van belang is om te waken voor eenheid in het stelsel door toepassing van de besproken frameworks, het inrichten van governance en het stellen van eisen zodat het CSIRT-stelsel overzichtelijk blijft.

ADVIES
VERVOLGSTAPPEN

Het in dit document toegelichte herontwerp schetst kaders voor het hernieuwde CSIRT-landschap. Daarmee vormt het een fundament onder het landschap dat in praktische zin daarna concreet zal moeten worden ingekleurd. Er moeten keuzes worden gemaakt die inzicht geven in hoe voor de korte, maar ook langere termijn het landschap er concreet uit komt te zien, binnen de kaders die in dit document zijn geschetst.

Advies is om deze vervolgstappen zo snel mogelijk op te pakken, nadat overeenstemming over het herontwerp is bereikt. Het betreft in elk geval:

1. Juridische context in relatie tot NIS2 en andere sectorspecifieke regelgeving uitwerken
2. CSIRT-ondersteuning borgen voor alle NIS2-doelgroepen
3. Taakverdeling tussen nationale en sectorale CSIRT's vaststellen
4. Bepalen hoe de huidige CSIRT's verder gaan in het CSIRT-stelsel
5. Inrichten van de besturing van het stelsel (governance/toezicht)
6. Koppelen van het landschap aan het Landelijk Dekkend Stelsel
7. Verbeteren van onderlinge samenwerking tussen CSIRT's
8. Onderzoeken hoe een kostprijsmodel kan worden toegepast

Ad.1 Juridische context in relatie tot NIS2 uitwerken

Termijn: zeer korte termijn

Parallel aan het uitvoeren van deze verkenning is onder regie van de NCTV een werkgroep gestart met het vertalen van de NIS2-richtlijn naar Nederlandse wetgeving. Belangrijk is dat in de verdere uitwerking de principes die vanuit het herontwerp zijn gedefinieerd passen binnen de gekozen implementatie. Elementen die hierin moeten worden meegenomen zijn:

- Het in het stelsel aangebrachte onderscheid tussen nationale CSIRT-taken en sectorale CSIRT-taken en de wijze waarop de nationale CSIRT zich tot de sectorale CSIRT's verhoudt
- De dubbelrol die het NCSC/CSIRT-DSP krijgt met aan de ene kant nationale en regietaken en aan de andere kan sectorale taken
- De mogelijkheid om een afgebakend takenpakket te formuleren tussen de nationale CSIRT en de sectorale CSIRT's en dit periodiek te herijken
- Flexibiliteit om bij wijzigingen in inzicht te kunnen kiezen voor het starten of stoppen van een nieuwe of bestaande sectorale CSIRT in het NIS2-domein

Ad. 2 CSIRT-ondersteuning borgen voor alle NIS2-doelgroepen

Termijn: zeer korte termijn

Er moet definitief worden bepaald welke doelgroepen onder de NIS2 vallen en wat een realistische inschatting is voor hun omvang (inclusief onderbouwing daarvoor). Vervolgens moet in overleg worden bepaald welke doelgroepen bediend gaan worden door welke sectorale CSIRT (onderbrengen bij een bestaande sectorale CSIRT of nieuwe CSIRT). Dit moet in onderlinge afstemming plaatsvinden tussen het vakdepartement, het ministerie van Justitie en Veiligheid, het NCSC/CSIRT-DSP en eventueel een betrokken sectorale CSIRT waarvan de overige doelgroepen passen bij de extra doelgroep.

Als entiteiten vallen binnen meer dan één sector kunnen ze in de doelgroep van meerdere CSIRT's vallen. Het is belangrijk dat er helder wordt afgesproken wie er primair aanspreekpunt is voor een entiteit en daarnaast dat er waar nodig tussen de betreffende CSIRT's wordt samengewerkt in geval van een incident.

Ad. 3 Taakverdeling tussen nationale en sectorale CSIRT's vaststellen

Termijn: korte termijn

Op basis van het keuzemodel, zoals dat op pagina 61 is toegelicht moet een eerste verdeling van taken tussen het nationale CSIRT en de sectorale CSIRT's worden vastgesteld. Uitgangspunt zijn de taaksoorten die een primaire verdeling impliceren, maar waarbinnen uitzonderingen denkbaar zijn.

Het is belangrijk om gezamenlijk, onder regie van de NCTV als stelselcoördinator, met experts vanuit de sectorale CSIRT's die in het stelsel NIS2-taken gaan uitvoeren deze indeling te maken, waarbij praktijksituaties moeten leiden tot het definiëren van:

1. Algemene scenario's met een basistaakverdeling
2. Specifieke scenario's die leiden tot uitzonderingen op basis waarvan de taakverdeling moet worden bijgesteld

Hierbij moeten tenminste de geformuleerde randvoorwaarden worden meegewogen, eventueel aangevuld met nieuwe randvoorwaarden zodra die actueel worden.

Ad. 4 Bepalen hoe de huidige CSIRT's verder gaan in het CSIRT-stelsel

Termijn: korte termijn

Voor ieder van de huidige CSIRT's die actief is binnen het NIS2-domein geldt dat zij moeten beoordelen in hoeverre zij aan de wettelijke eisen (onder andere van de NIS2) en het herontwerp van het CSIRT-stelsel kunnen en willen voldoen. Ook zullen zij in gesprek moeten gaan met de betreffende vakdepartementen over de NIS2-verplichtingen in relatie tot hun governance-structuur en de wens die de vakdepartementen hebben over de invulling van de CSIRT-taken. Als het nodig is om taken te verplaatsen naar het NCSC/CSIRT-DSP dan zullen ook zij en de NCTV bij dit gesprek betrokken moeten worden om te bespreken wat de impact hiervan zal zijn.

Als wettelijke taken worden belegd bij een al bestaand CSIRT, moet onderzocht worden op welke wijze de governance moet worden aangepast om het beleggen van wettelijke taken mogelijk te maken (zie pagina 18).

Om te bepalen wat de gap is tot oktober 2024 kan overwogen worden om bij de bestaande sectorale CSIRT's op korte termijn een self-assessment te laten uitvoeren ten aanzien van de taakvolwassenheid in relatie tot het ENISA CSIRT Maturity Model om te bepalen wat er nodig is om het *Intermediate*-niveau te bereiken.

Ad. 5 Inrichten van de besturing van het stelsel (governance/toezicht)

Termijn: middellange termijn

In dit herontwerp zijn de kaders geschetst voor het verder invullen van de besturing van het CSIRT-stelsel. Deze zullen verder moeten worden uitgewerkt in interdepartementaal verband. Hierbij moet zoveel mogelijk worden aangesloten bij al lopende trajecten en structuren die er al zijn. Advies is om de NCTV bij deze actie als regiehouder op te laten treden.

Ad. 6 Koppelen van het landschap aan het Landelijk Dekkend Stelsel

Termijn: middellange termijn

In de NLCS is een actielijn geformuleerd voor het door ontwikkelen van het Landelijk Dekkend Stelsel. Belangrijk onderdeel van dit stelsel is het CSIRT-stelsel. Het is belangrijk dat de resultaten van deze verkenning en de besluiten erover worden ingebracht bij deze actielijn en dat bij eventuele knelpunten in relatie tot het herontwerp van het Landelijk Dekkend Stelsel gezamenlijk naar oplossingen wordt gezocht. Advies is dat de NCTV dit actiepunt bewaakt.

Ad. 7 Verbeteren van onderlinge samenwerking tussen CSIRT's

Termijn: middellange termijn

Zoals op pagina 69 is toegelicht is het van belang de onderlinge samenwerking tussen de sectorale CSIRT's te verbeteren. Advies is om vanuit de nationale CSIRT (in oprichting) deze taak op te pakken en in kaart te brengen welke mogelijkheden er

liggen en welke prioriteiten hierin moeten worden gesteld, mede afhankelijk van beschikbare capaciteit en middelen.

In dit kader is het ook van belang om onderlinge afspraken te maken over kennisborging, en dan specifiek in elk geval voor het OT-domein. In de gesprekken die in het kader van de verkenning zijn gevoerd is meerdere keren gesproken over kennis over Operational Technology (OT) die in meerdere domeinen relevant is. Het is goed om dit te koppelen aan de NLCS-actielijn voor wat betreft de verdere ontwikkeling van de een bredere samenwerking op dit terrein in de zogenaamde IACS-coalitie.

Ad. 8 Onderzoeken hoe een kostprijsmodel kan worden toegepast

Termijn: middellange termijn

Voor vakdepartementen die de sectorale CSIRT-taken beleggen bij het NCSC/CSIRT-DSP moet opdrachtgeverschap nader worden ingericht. Hiervoor is een aparte vervolgactie gedefinieerd (zie governance). Voor de langere termijn is het belangrijk om te onderzoeken welk financieringsmodel/kostprijsmodel hierbij gehanteerd zou kunnen worden. Dit is een complex onderwerp dat aparte aandacht behoeft. Zodoende dat hiervoor een aparte actie is benoemd. De NCTV kan hier regie op voeren.

BIJLAGEN

GERAADPLEEGDE ORGANISATIES

Er zijn tijdens de verkenning meerdere gesprekken gevoerd met de vakdepartementen die betrokken zijn bij het programma Versterkte Aanpak Vitaal en daarnaast met de in Nederland actieve sectorale CSIRT's.

Vakdepartementen

- Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
- Ministerie van Economische Zaken en Klimaat
- Ministerie van Infrastructuur en Waterstaat
- Ministerie van Financiën
- Ministerie van Landbouw, Natuur en Voedselkwaliteit
- Ministerie van Onderwijs, Cultuur en Wetenschap
- Ministerie van Volksgezondheid, Welzijn en Sport

Sectorale CSIRT's

- CERT-WM
- CSIRT-DSP
- IBD
- NCSC
- SURF-CERT
- Z-CERT