Ministerie van Infrastructuur
en Waterstaat

Inzicht in verhouding organisatie (incl. SOC) vs (sectoraal) CSIRT

Luuk Stadhouders (Berenschot), Rianne Zivali-de Kievit (Berenschot)
en Tim Kenter (Berenschot)

Programma
Versterken
Cyberweerbaarheid
in de watersector

17 november 2023

Inleiding

Het ministerie van Infrastructuur en Waterstaat (hierna: IenW) heeft Berenschot gevraagd een beknopt (visueel) overzicht gemaakt van hoe de taken die het sectorale CSIRT Water gaat vervullen zich verhouden tot SOC-taken waarvoor individuele entiteiten verantwoordelijk zijn en blijven. Onderliggende document biedt dit overzicht en is op onderdelen gevisualiseerd.

Eisen

Aan de uitwerking zijn vooraf de volgende eisen meegegeven:

- Dit overzicht sluit aan bij de inrichting van het CSIRT Water die wordt voorzien in de business case die wordt ontwikkeld in het project “Doorontwikkelen CERT stelsel watersector”.
- De taken worden concreet omschreven en geven verdere verdieping aan de taken zoals deze voor CSIRTs in de NIS2 staan omschreven. Hiervoor wordt geput uit de taakinvulling zoals deze wordt uitgewerkt in de sectorale CSIRT werkgroep.
- Het overzicht gaat uit van de situatie waarbij de wettelijke CSIRT-taken van het CERT-WM opgaat in het CSIRT Water en de SOC-taken bij HWH blijven.
- In de taken van het sectorale CISRT Water worden zowel de verplichte CSIRT taken onder NIS2 als weerbaarheidstaken gevoegd.
- In het overzicht worden ook andere voor de sector belangrijke CSIRT’s zoals het nationale CSIRT (NCSC), de IBD en waar mogelijk de provincies meegenomen.
- In het overzicht worden ten minste ook het SOC van Rijkswaterstaat, het beoogde joint SOC van de waterschappen en de situatie waarin organisaties een eigen interne of externe SOC dienst hebben meegenomen.

Randvoorwaarden/beperkingen

- Voor een concreet overzicht van de taken is toegang tot de laatste informatie over taakinvulling door CSIRTs zoals deze wordt besproken in de sectorale CSIRT werkgroep vereist.
- Dit overzicht wordt gelijk opgeleverd met de business cases voor een sectoraal CSIRT Water, hierdoor kan de plaat alleen gebaseerd worden op de uitwerking zoals deze in het project “Doorontwikkelen CERT stelsel watersector” beschikbaar is.

Leeswijzer

Op pagina 3 worden enkele afkortingen en definities toegelicht. Vanaf pagina 5 wordt het cyberstelsel in één oogopslag toegelicht. Vanaf pagina 9 is de verdeling NIS2-taken over organisatie (SOC) en sectoraal CSIRT uitgewerkt. Vanaf pagina 12 zijn de FIRST-area’s en services uitgewerkt.

Gehanteerde definities en afkortingen

CSIRT
De term CSIRT staat voor Computer Security Incident Response Team. Met andere woorden, een CSIRT is een organisatie(unit) die diensten verleent op het gebied van preventie, detectie en afhandeling van cybersecurity incidenten. Met de komst van de NIS2 heeft, in elk geval binnen de EU, de term CSIRT meer lading gekregen voor die CSIRTs die in het kader van de NIS2 landelijke dan wel sectorale taken gaan uitvoeren binnen het CSIRT netwerk. Er zijn voor deze CSIRTs met de komst van de NIS2 namelijk wettelijke taken en eisen gedefinieerd.

CSIRT Water
IenW beoogt een CSIRT voor de watersector op te richten die als sectoraal CSIRT, en daarmee dus conform de wettelijke taken en eisen van de NIS2, gaat functioneren. Het huidige CERT-WM wordt onderdeel van deze nieuwe CSIRT, SOC-taken worden expliciet bij de organisaties binnen de sector zelf belegd (SOCs). Naast de verplichte NIS2 taken zal het CSIRT water ook (mogelijk) aanvullende weerbaarheidstaken gaan uitvoeren die sectorbreed bijdragen aan het vergroten van de weerbaarheid van de individuele organisaties. Het betreft hier taken die door de deelnemers als waardevol zijn geïdentificeerd om gezamenlijk op te pakken bovenop hun eigen inspanningen. De organisaties zelf blijven immers verantwoordelijk voor de eigen informatiebeveiliging.

FIRST CSIRT Services Framework (hierna: FIRST-raamwerk)
Het FIRST-raamwerk is een hulpmiddel voor de inrichting van CSIRTs. Het biedt een overzicht van alle diensten die een CSIRT kán verrichten. Het schrijft niet voor dat een CSIRT ook al die services zou moeten verrichten. Het raamwerk richt zich op het geheel aan incident management, wat ook deels door andere organisatieonderdelen, zoals een SOC ingevuld kan worden. Met andere woorden, het raamwerk maakt het geheel aan services rondom incident management inzichtelijk, maar doet geen uitspraken over óf en waar je deze allemaal moet beleggen. De nationale en sectorale CSIRTS uit de NIS2 zijn binnen het FIRST-raamwerk te definiëren als een coordinating CSIRT.

ISAC
Een Information Sharing and Analysis Centre (ISAC) is een sectoraal overleg over cybersecurity. In een ISAC wordt in een vertrouwde omgeving met organisaties uit dezelfde sector gevoelige en vertrouwelijke informatie over incidenten, dreigingen, kwetsbaarheden, maatregelen en leerpunten op het gebied van cybersecurity gedeeld. Er is geen ‘standaardvorm’ van een ISAC. Een samenwerking in een ISAC kan formeel of informeel zijn; gestructureerd of flexibel; met fysieke vergaderingen, teleconferenties, via een digitaal platform of een mix van deze drie. De deelnemers kiezen zelf de best passende vorm.

SOC
Een Security Operations Centre monitort de computer- en netwerkactiviteiten in (of voor) een organisatie. Zo wordt log-informatie van applicaties en apparaten in het bedrijfsnetwerk verzameld en onderzocht op afwijkende zaken en vaak vindt initiële response bij cyberincidenten hier plaats. Er zijn meerdere varianten: individueel SOC voor een organisatie of een joint-SOC bij meerdere samenwerkende organisaties. SOC-diensten kunnen intern, extern of hybride worden uitgevoerd en (al dan niet gezamenlijk) worden ingekocht (bijvoorbeeld zoals in het geval van HWH/Secura)

Weerbaarheidstaken
Weerbaarheidstaken betreffen niet-wettelijke activiteiten die door de deelnemers als waardevol zijn geïdentificeerd om gezamenlijk op te pakken bovenop hun eigen inspanningen en die de weerbaarheid van de deelnemers vergroot.

Het cyberstelsel in één oogopslag

Programma
Versterken
Cyberweerbaarheid
in de watersector

Het stelsel

Een digitale crisis is vaak niet opzichzelfstaand en raakt veel facetten binnen onze samenleving. Bij de beheersing van een digitale crisis zijn veel actoren betrokken, zowel in het digitale domein als in het fysieke domein. Daarnaast zijn er zowel publieke als private partijen betrokken, die allemaal hun eigen verantwoordelijkheid hebben tijdens een digitale crisis én daarbij ook nauw samenwerken. Vandaar dat het belangrijk is om goed inzichtelijk te hebben op welke manier al deze partijen op elkaar aangesloten zijn, welke taken zij uitvoeren en op welke manier zij met elkaar interacteren. In onderliggend overzicht beperken we ons tot de zogeheten 'functionele keten', oftewel 'het cyberspecifieke stelsel'.
(bron: Landelijk Crisisplan Digitaal)

Er is in Nederland in de loop der jaren een landschap ontstaan waarin verschillende sectorale en niet-sectorale CSIRT's actief zijn. Er is een zestal sectorale CSIRT's 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)
(bron: Onderzoek CSIRT-stelsel, Petra Oldengarm)

In de komende periode ontstaan er diverse nieuwe wettelijke taken op het gebied van ondersteuning door sectorale CSIRT's, met name vanuit de NIS2, 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.
(bron: Onderzoek CSIRT-stelsel, Petra Oldengarm)

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 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.
(bron: Onderzoek CSIRT-stelsel, Petra Oldengarm)

Over de verdeling van de taken tussen nationaal en sectorale CSIRT's vindt op dit moment interdepartementaal afstemming plaats.


Taakniveau
De positionering van een SOC/CSIRT in relatie tot NIS2
Verplicht
Niet verplicht
Nationaal
Regie- en coördinatie taken
Nationaal CSIRT (NCSC)
Taken zoals het organiseren van ISIDOOR als landelijke cyberoefening
Sectoraal
Ondersteunen van organisaties op het gebied van cyberincidenten
Sectoraal CSIRT (NCSC of eigen sectoraal CSIRT)
Gezamenlijke weerbaarheidstaken zoals het opzetten van sectorale projecten, kennisproducten, trainingen, etc.
ISAC overleggremium voor cybersecurity informatie in brede zin
OKTT dat incidenten en dreigings-informatie deelt
Organisatie
Uitvoering geven aan zorgplicht (zoals incidentenbehandeling)
SOC-organisatie (intern of extern) die invulling geeft aan verplichte en niet-verplichte taken
Niet wettelijke weerbaarheidsactiviteiten

Gelaagd CSIRT-landschap

Op de vorige pagina staat een gevisualiseerd, abstract en deels gefingeerd overzicht van het cyberstelsel in relatie tot CSIRTS. We maken hierbij onderscheid naar verplichte en niet-verplichte NIS2-taken en naar nationaal, sectoraal en organisatieniveau:

1. Op **nationaal niveau** bevindt zich het NCSC. Het NCSC is verantwoordelijk voor alle taken uit de NIS2 die niet gedelegeerd zijn aan de sectorale CSIRTs. Het NCSC is tevens een sectoraal CSIRT en bevindt zich daarmee dan ook op zowel nationaal als sectoraal niveau. Het NCSC kan meer taken uitvoeren van verplicht vanuit de NIS2.
2. Op **sectoraal niveau** bevinden zich de sectorale CSIRTs die de door het NCSC gedelegeerde taken van de NIS2 uitvoeren, al dan niet uitgebreid met weerbaarheidstaken op sectoraal niveau. Daarnaast bevinden zich hier ook OKTTs en ISACs:
   - OKTT: een afkorting die het NCSC gebruikt voor een organisatie die 'objectief kenbaar tot taak' heeft om andere organisaties of het publiek te informeren over dreigingen en incidenten met betrekking tot andere netwerk- en informatiesystemen. Hoewel niet per se sectoraal ingericht, richten zij zich op het informeren van een bredere groep organisaties en vinden we daarmee plaatsing op de sectorale laag als passend.
   - ISAC: Binnen vitale sectoren speelt het NCSC een rol voor de organisatie van de ISACs, de inrichting is echter op basis van sector en daarmee vormen ze een organisatie op de sectorale laag. Voor de sector water is er bijvoorbeeld een ISAC 'keren en beheren', een ISAC 'drinkwater', en een ISAC 'OT'.
3. Op **organisatieniveau** is de zorgplicht vanuit de NIS2 aanwezig. Elke organisatie is en blijft (eind-)verantwoordelijk voor de informatiebeveiliging binnen de eigen organisatie en dient dus hiervoor zelf de benodigde zaken zoals een SOC in te (laten) richten. De wijze waarop organisaties hier invulling aan geven verschilt, of anders gezegd is niet voorgeschreven vanuit de NIS2. Een SOC is echter een veelvoorkomende organisatievorm om bij te dragen aan deze zorgplicht. Het kan ook ingevuld worden door een andersoortige security functie binnen de organisatie.

Een taak beleggen is niet elders (geheel) wegnemen

Het beleggen van taken bij een sectoraal of nationaal CSIRT betekent niet dat individuele organisaties geen taak voor hun eigen organisaties hebben op deze vlakken (!). Denk hierbij bijvoorbeeld aan monitoring of bewustwording. De activiteiten van een sectoraal CSIRT kunnen wel versterkend werken voor organisaties, maar vervangen geenszins de eigen verantwoordelijkheid / zorgplicht van organisaties.

NIS2-taken: organisatie (SOC) en (sectoraal) CSIRT

Programma
Versterken
Cyberweerbaarheid
in de watersector

De kern van de opdracht is het inzichtelijk maken van de verhouding in taken van enerzijds individuele organisaties (o.a. in de vorm van SOC's) en anderzijds een sectoraal CSIRT. Een aantal constateringen vooraf:

NIS2-taken

De NIS2 beschrijft verplichte taken voor een land om te organiseren, in 1 (of meerdere) CSIRT's. Dit is aan het land zelf. De verplichte NIS2-taken komen, zo wordt gesteld in het Onderzoek CSIRT-stelsel (deels) overeen met enkele area's en services van het FIRST-raamwerk (bijlage 1, slide 15).

FIRST-raamwerk

Het FIRST-raamwerk beschrijft mogelijke taken die een CSIRT op zich kan nemen, heeft geen dwingend karakter en wordt gezien als leidraad bij het opzetten en verder ontwikkelen van CSIRT's. Of in de woorden uit het FIRST-raamwerk: "The services described are those potential services a CSIRT could provide. No CSIRT is expected to provide all described services. Each team will need to choose services that support their mission and constituents, as described by their mandate".

Het raamwerk voorziet in standaard terminologie die binnen de CSIRT-community kan worden gebruikt en helpt dus bij standaardisatie en vergelijken van werkzaamheden. Het FIRST-raamwerk is in het onderzoek CSIRT-stelsel dan ook geïntroduceerd en omarmd door JenV met als doel 'creëren van gemeenschappelijke taal' voor de verdeling van de NIS2-taken.

FIRST-raamwerk: Beschrijvend, niet gericht op verdeling

Bij het inzichtelijk maken van de taakverdeling tussen organisatie en sectoraal/nationaal is het FIRST-raamwerk beperkt passend. Het is *beschrijvend* en niet bedoeld voor *verdeling* van taken met bijvoorbeeld SOC's. Het beschrijft alle services die op het brede vlak van incident management *ingericht* kunnen worden, ongeacht waar. Daarbij geldt ook dat een sectoraal CSIRT een vorm van een coördinerend CSIRT is. Hierover zegt FIRST: "The Coordinating CSIRT acts as single point of contact for the whole group and is focused on the overall security aspects of these organizations." Hiermee is dus niet gezegd dat daarnaast niet een 'enterprise CSIRT' (op organisatieniveau) kan bestaan. Met andere woorden, het CSIRT neemt geen taken of verantwoordelijkheden van een organisatie weg, maar vult aan / ondersteunt (vanuit breed sectoraal perspectief). Concluderend: alle services uit het FIRST-raamwerk dienen - in meer of mindere mate - ook binnen elke individuele organisaties geborgd te zijn.

Verdeling: NIS2-taken over organisatie en (sectoraal) CSIRT

In de volgende slide verdelen we de NIS2-taken – zoals uitgewerkt in het Onderzoek CSIRT-stelsel – over organisatie en (sectoraal) CSIRT. De verdeling tussen sectoraal en nationaal is buiten scope en onderhevig aan interdepartementale afstemming.

Uit de verdeling blijkt dat (delen van) NIS2-taken zowel op organisatieniveau als op (sectoraal) CSIRT-niveau belegd dienen te worden. Hiertussen dienen afspraken gemaakt te worden, op onderdelen informatie worden uitgewisseld of op andersoortige wijze 'koppelvlakken' te worden georganiseerd. Dit geldt ook voor weerbaarheidstaken.

Verdeling: NIS2-taken over organisatie en (sectoraal) CSIRT

In de volgende slide verdelen we de NIS2-taken – zoals uitgewerkt in het Onderzoek CSIRT-stelsel – over organisatie en (sectoraal) CSIRT. De verdeling tussen sectoraal en nationaal is buiten scope en onderhevig aan interdepartementale afstemming.

Uit de verdeling blijkt dat (delen van) NIS2-taken zowel op organisatieniveau als op (sectoraal) CSIRT-niveau belegd dienen te worden. Hiertussen dienen afspraken gemaakt te worden, op onderdelen informatie worden uitgewisseld of op andersoortige wijze ‘koppelvlakken’ te worden georganiseerd. Dit geldt ook voor weerbaarheidstaken.

Gebieden*	Organisatie**	CSIRT**
Monitoring (en detectie). Hierbij gaat het over het voortdurend monitoren van dreigingen die sectoren kunnen raken: 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)	Monitoring en detectie binnen eigen systemen binnen / van de (samenwerkende) organisatie(s). Dit kan georganiseerd worden binnen een organisatievorm, zoals een SOC.	Monitoring en detectie van de 'sector' / omgeving tot de 'buitenkant' van de organisaties (en mogelijk verdergaand maar onderhevig aan discussie m.b.t. reikwijdte NIS2). Een CSIRT kan bijstand leveren aan het monitoren van netwerken en informatiesystemen bij individuele SOC's, denk bijvoorbeeld aan het faciliteren van knowhow over de (technische) inrichting en het uitwisselen van kennis tussen SOC's.
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)	Kwetsbaarheden nagaan / opvolgen binnen eigen organisatie(s). Organisaties kunnen informatie aanleveren aan het CSIRT, zoals 'indicators of compromise' (IOC's).	• Analyse kwetsbaarheden die sector kunnen raken. • Analyse van dreigingen / fenomenen, op basis van informatie uit de sector en daarbuiten. • Incidentanalyse, inclusief data/forensics.
Meldingen. Belangrijke taak van de CSIRT's is het doen van meldingen aan de doelgroep over de actualiteiten: a. Het afgeven van vroege waarschuwingen en het delen van analyses (11.3b)	Meldingen voor de eigen organisaties vertalen naar actie.	• Afgeven (vroege) waarschuwingen • Delen van analyses
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)	• Regulier Incident Management en evt. opgeschaald Incident Response in lijn met afspraken in betrokken organisatie(s). • Het delen van informatie en medewerking verlenen bij sectorale incidenten. Zorgdragen voor analyse van eigen incidenten inclusief forensics.	• Flexibele ondersteuning: het verlenen van bijstand bij incidenten (24/7) • Coördinatie/duiding op sectoraal niveau, afstemming landelijk • Het bieden van ondersteuning bij forensics • Bijstaan in crisiscommunicatie op verzoek van organisaties
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)	Niet van toepassing.	• Deelnemen aan (inter)nationaal CSIRT-netwerk. • Gecoördineerd bekend maken van kwetsbaarheden. Ontwikkelen van instrumentarium voor informatiedeling. Bevorderen van samenwerking met private sector. Bevorderen van standaardisatie.
Knowledge transfer.	• Trainen en ontwikkelen security-medewerkers. • Oefeningen voor de eigen organisatie(s) organiseren. • Bewustwording creëren.	• Trainen CSIRT medewerkers. • Sectorbrede oefeningen. • Zorgen voor relevante sectorbrede kennisdeling, ook borging programma PVCW.
Artikel 23 en artikel 30. Meldingen op verplichte dan wel vrijwillige basis aangaande incidenten, bijna-incidenten en dreigingen, ook vanuit organisaties die niet onder de richtlijn vallen.	• Verplicht melden van significante incidenten. • Vrijwillig melden van cyberdreigingen en bijna-incidenten.	Het in ontvangst nemen van en afhandelen van alle binnenkomende meldingen, conform de eisen van de NIS2.

De zwarte teksten zijn de NIS2-taken, bovenste vijf zoals verwoord en geclusterd in het onderzoek van Petra Oldengarm.
De rode teksten zijn weerbaarheidstaken die niet direct voortvloeien uit de NIS2.
* Verdeling gebieden op basis van het onderzoek CSIRT-stelsel (Petra Oldengarm, 2023)
** Nadere beschrijving en verdieping op basis van onder meer hetgeen bekend is vanuit de NIS2 dan wel logischerwijs kan/moet worden verwacht op basis van bestaande wet- en regelgeving of best practices.

Beschrijving: FIRST-raamwerk over organisatie en (sectoraal) CSIRT

In de volgende slide hanteren we het FIRST-raamwerk en werken dit uit naar wat een organisatie en (sectoraal) CSIRT zou doen. Ook hier geldt dat de verdeling tussen sectoraal en nationaal buiten scope is en onderhevig aan interdepartementale afstemming.

Uit de beschrijving blijkt dat (delen van) de taken (of services als onderdeel van area's) zowel op organisatieniveau als op (sectoraal) CSIRT-niveau liggen. En ook hier geldt dat hiertussen afspraken gemaakt dienen te worden, op onderdelen informatie worden uitgewisseld of op andersoortige wijze 'koppelvlakken' te worden georganiseerd. Dit geldt ook voor weerbaarheidstaken.

Ook een ISAC – een vertrouwde omgeving met als doel het delen van (vertrouwelijke) informatie omtrent cybersecurity gerelateerde onderwerpen (m.n. dreigingen, kwetsbaarheden, incidenten en evt. crises) – kan op deze area's een rol spelen.

FIRST area's	Services	Organisatie / SOC*	Sectoraal CSIRT**
1. Information Security Incident Management (oftewel Incident management aldus overzicht Gabor)	Information Security Incident Report Acceptance	Organisatie heeft een intern meldpunt, inclusief afspraken over werkwijze. Organisatie is 24/7 beschikbaar (bijv. in wacht- of piketdienst).	Het sectorale CSIRT ontvangt (vrijwillige of verplichte) meldingen van incidenten.
	Information Security Incident Analysis	Organisatie doet analyses conform gestandaardiseerde afspraken.	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)
	Artifact And Forensic Evidence Analysis	Organisatie verzamelt en analyseert forensische gegevens, doet een risico- en incidentanalyse. Organisatie doet dit zelf of laat zich hierbij ondersteunen door externe organisatie(s).	Het bieden van ondersteuning bij forensics (art. 11.3d)
	Mitigation And Recovery	Organisatie zorgt voor mitigatie en recovery, onder meer in het kader van continuïteit van de primaire processen (bedrijfscontinuïteit).	X
	Information Security Incident Coordination	Organisatie zorgt voor een gecoördineerde incident response op security incidenten conform standaarden of best practices.	Het sectorale CSIRT verstrekt relevante informatie over incidenten aan relevante belanghebbende. Het sectorale CSIRT verstrekt informatie over incidenten aan de sector in Nederland. Het sectorale CSIRT coördineert incidenten die (vrijwillig of verplicht) gemeld worden door organisaties binnen een sector: 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)
	Crisis Management Support	Organisatie zorgt voor ingericht en werkend crisismanagement proces die ondersteunend is/kan zijn aan de response op incidenten met als doel beperken schade en zorgen voor bedrijfscontinuïteit.	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)
2. Vulnerability Management	Vulnerability Discovery / Research	Organisatie monitort en analyseert dreigingen en kwetsbaarheden op eigen organisatie (onder meer vulnerabiliyscans, pentesten etc.). Maakt gebruik van kennis en advies van (sectoraal) CSIRT. Kan daarnaast zelf actief onderzoeken, bijvoorbeeld afstruinen darkweb of monitoren van social media.	Het sectorale CSIRT monitort kwetsbaarheden voor de sector in Nederland. Het sectorale CSIRT scant (proactief en niet-intrusief) openbaar toegankelijke netwerken en informatiesystemen. Het sectorale CSIRT analyseert kwetsbaarheden voor de sector
	Vulnerability Report Intake	Idem als bij incidenten.	X
	Vulnerability Analysis	Idem als bij incidenten.	Het sectorale CSIRT maakt op basis van een risico gebaseerde benadering een inschatting van de prioritering van taken in de sector: 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)
	Vulnerability Coordination	Idem als bij incidenten.	Het sectorale CSIRT treedt op als coördinator voor het proces van gecoördineerde bekendmaking van kwetsbaarheden in de sector. 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). Zie raakvlak/overlap met incidenten (sub area 1).
	Vulnerability Disclosure	Organisatie zorgt voor gecoördineerde 'vulnerability disclosure', al dan niet ondersteund door een sectoraal CSIRT. In dit geval: overnemen huidige taak van het CERT-WM.	Het sectorale CSIRT verstrekt vroegtijdige waarschuwingen over kwetsbaarheden aan de sector: a. Het afgeven van vroege waarschuwingen en het delen van analyses (11.3b)
	Vulnerability Response	Idem als bij incidenten.	X

FIRST area's	Services	Organisatie / SOC*	Sectoraal CSIRT**
3. Situational Awareness	Data Acquisition	Organisatie is verantwoordelijk voor (extra) beveiliging van de eigen (security) organisatie.	X (sector-level)
	Analysis And Synthesis	Organisatie doet dit voor eigen organisatie(-onderdelen).	X (sector-level)
	Communication	Organisatie communiceert in eigen organisatie (of onderdelen onder verantwoordelijkheid van de organisatie). Communiceert tevens met peers, leveranciers, (sectoraal)CSIRT etc.	Het sectorale CSIRT verstrekt informatie over dreigingen aan de sector. Het sectorale CSIRT verstrekt relevante informatie over dreigingen aan relevante belanghebbende. Het sectorale CSIRT vergemakkelijkt de verstrekking van doeltreffende en efficiënte informatie met Nationale Security Incident Response teams van derde landen. Zie raakvlak/overlap met coördinatie-taak.
4. Knowledge Transfer	Awareness Building	Organisatie zorgt voor awareness in de organisatie. Desgewenst heeft de organisatie een bredere taakopvatting door bijvoorbeeld de (fysieke) omgeving of keten van de organisatie mee te nemen.	Het sectorale CSIRT zorgt voor situationeel bewustzijn met betrekking tot cyberbeveiliging in de sector.
	Training And Education	Organisatie zorgt voor opleiding en training van de eigen (security) medewerkers, bijvoorbeeld op het gebied van incident response, crisismanagement etc.	X (sector-level)
	Exercises	Organisatie zorgt voor oefeningen in eigen organisatie. Dit kan breed worden opgepakt in de context van 'opleiden, trainen en oefenen' op onder meer rol-, team- en organisatieniveau. Desgewenst kan dit worden uitgebreid met stakeholders, zoals leveranciers of organisaties in de (waarde)keten.	X (sector-level)
	Technical And Policy Advisory	Organisatie doet dit voor eigen organisatie(-onderdelen).	X (sector-level)
5. Information Security Event Management (dreigings-management aldus overzicht Gabor)	Monitoring And Detection	Organisatie monitort dreigingen voor eigen organisatie, zorgt voor eigen dreigingsbeeld (al dan niet op basis van een nationaal of sectoraal dreigingsbeeld).	Het sectorale CSIRT monitort incidenten voor de sector in Nederland: 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)
	Event Analysis		X

* Onder meer de BIO stelt op aspecten normen en een baseline/ondergrens. Uitwerking is niet uitputtend en slechts indicatief. Uitwerkingen als aard en omvang van aspecten als 'toeleveringsketen' in de NIS2 in relatie tot de verantwoordelijkheid van een entiteit kunnen hierop van invloed zijn.

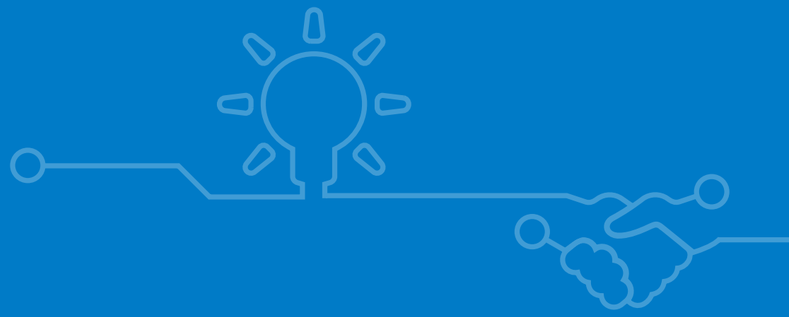
** Verdeling sectoraal/nationaal valt buiten scope van de opdracht. Uitwerking in deze kolom (deels) overgenomen uit de (concept) uitwerking / Excel-bestand via Eva/Gabor. Mogelijke keuzes hierin hebben impact op de taken van het sectorale CSIRT. N.B. de product-groepen uit dat Excel-bestand komen niet geheel overeen met het hier juist toegepaste FIRST-raamwerk!

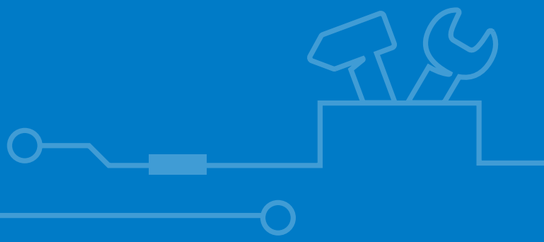
Bijlage 1: Mapping van NIS2-taken op CSIRT Services Framework

 Information security incident management	 Vulnerability management	 Situational awareness	 Knowledge transfer	 Information security event management
1. Information Security Incident ReportAcceptance 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

Bron: Onderzoek CSIRT-stelsel (Petra Oldengarm, 2023)

Ministerie van Infrastructuur
en Waterstaat





Contactgegevens

cyberweerbaarheidwater@minienw.nl

versterkencyberweerbaarheid.nl

Programma
Versterken Cyberweerbaarheid in de watersector