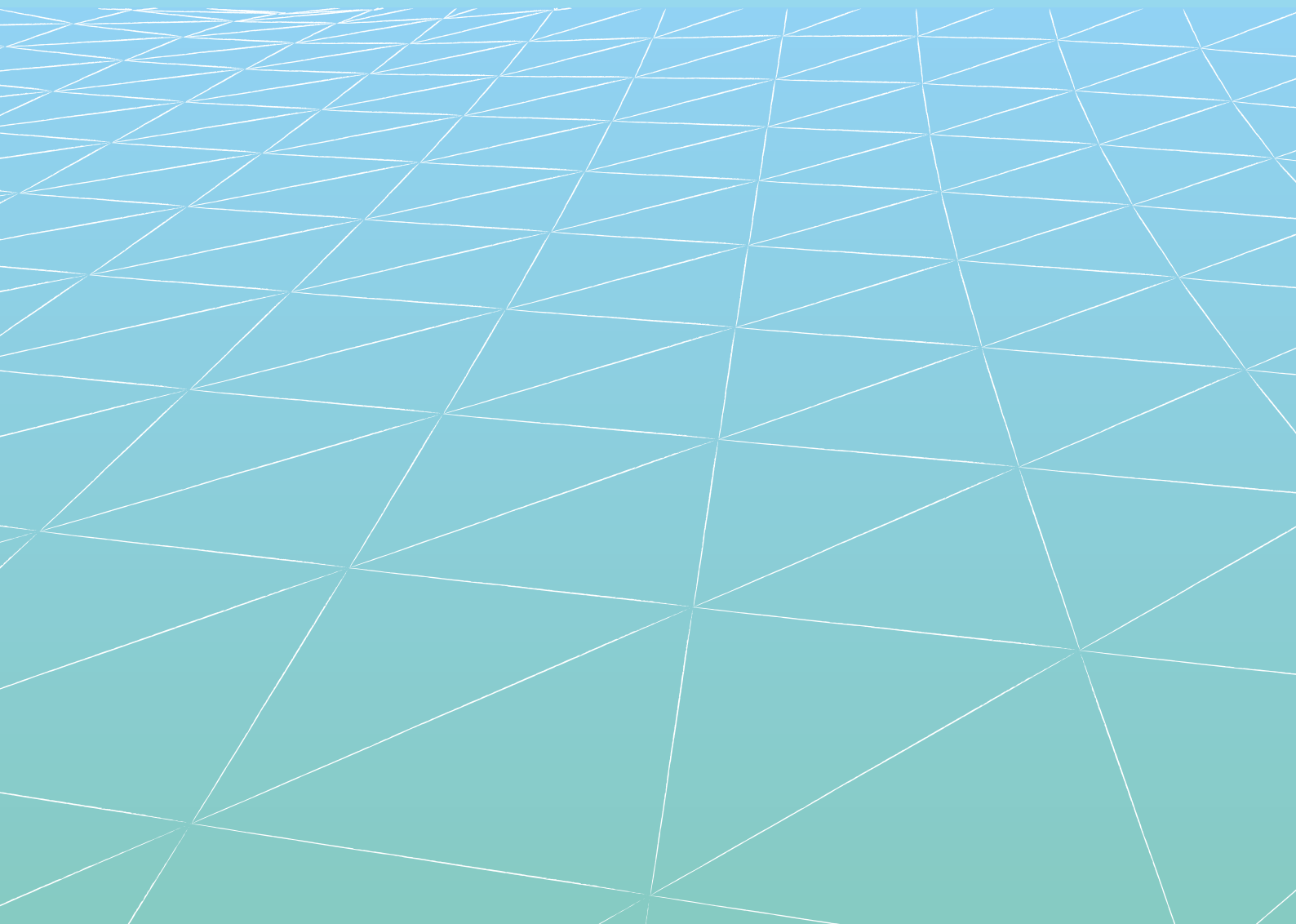
Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Bijlage 3 van het Bouwplan Cyberweerbaarheidsnetwerk (CWN)

Functie Incidentafhandeling

Uitwerking van CWN-functie Incidentafhandeling in publiek-private samenwerking



Inleiding

In de periode september 2024 tot en met mei 2025 is in publiek-private samenwerking gewerkt aan een plan om incidentafhandeling in cybersecurity te versterken. Dit plan is een resultaat van vele overleggen en bijeenkomsten en vormt een gezamenlijk beginpunt voor de functie Incidentafhandeling van het Cyberweerbaarheidsnetwerk. Vanuit dit plan zal onder coördinatie van het Nationaal Cyber Security Center worden gewerkt aan het opzetten van een netwerk en het prioriteren en bereiken van de gestelde doelen.

Dit plan is onderdeel van het bouwplan CWN. Het geeft houvast en richting aan het ontwikkelen van het CWN samen met publieke en private partners. Gedurende de ontwikkeling zal steeds opnieuw bezien moeten worden wat nodig is om het CWN verder uit te bouwen tot een succesvol relevant netwerk, waardoor in de toekomst mogelijk aanpassingen in dit plan nodig zijn.

Definitie en scope van de functie

De noodzaak tot samenwerking

Er is een groep organisaties in Nederland die zich niet of minder goed heeft voorbereid op cyberincidenten. De bedoeling van deze functie is dat ook deze entiteiten via 'schakelorganisaties' ondersteuning krijgen. Dat kan bijvoorbeeld door hen te verwijzen naar relevante informatiebronnen of organisaties die hen verder kunnen helpen. Daarnaast is het belangrijk om informatie over incidenten zoveel mogelijk te delen. Hier kan het CWN een rol spelen door schakels uit het netwerk in te zetten voor het stimuleren van het vrijwillig melding van incidenten of dreigingen. Daarnaast maken we samenwerkingsafspraken met organisaties die incidentresponsediensten leveren in Nederland. Op deze manier borgen we het delen van incidentinformatie.

Het samenwerkingsproces

De interactie in het CWN-netwerk voor deze functie begint met voorbereiden in de 'koude fase'. Daadwerkelijke interactie speelt zich met name af tijdens de 'lauwe en warme fases' van incidenten en crises. In de warme fase moet een organisatie de ondersteuning kunnen vinden die haar kan helpen bij de afhandeling van het incident. Iedere organisatie in Nederland moet hiervoor over de juiste kennis en informatie kunnen beschikken.

Scope van de functie

De functienaam 'Incidentafhandeling' kan ten onrechte de indruk wekken dat deze functie incidenten gaat afhandelen. Dat is niet het geval; iedere organisatie in Nederland is én blijft zelf verantwoordelijk voor het afhandelen van een incident. Deze CWN-functie zorgt ervoor dat organisaties, als zij daar belangstelling voor hebben, tijdens een incident kunnen worden ondersteund bij de afhandeling van dat incident. Het betekent dat je als organisatie beter in staat bent om te reageren op een incident omdat je de weg kunt vinden naar partners die jou daarbij kunnen helpen.

De volgende onderwerpen vallen buiten de scope van deze functie:

- Het managen of afhandelen van actuele incidenten of crises; hiervoor zijn organisaties zelf verantwoordelijk;
- Het uitwisselen van operationele informatie tijdens incidenten of crises. Dit wordt gedaan vanuit de functie Informatiedeling. Het in kaart brengen van welke partijen beschikking hebben over incident-informatie, hoort uiteraard wel bij de functie Incidentafhandeling;
- Het verspreiden van informatie- of kennisproducten. Hiervoor wordt gebruikgemaakt van de functie Kennisuitwisseling.

Huidige situatie

Bestaande organisaties

Binnen het huidige LDS is incidentafhandeling geen functie. Er zijn echter al veel organisaties, samenwerkingsverbanden en programma's die zich op de een of andere wijze bezighouden met incidentafhandeling. Voorbeelden hiervan zijn: MSSPs, MSPs CSIRTs, brancheverenigingen, (regionale) initiatieven, programma's (zoals Cyclotron) en ISACs[1].

Bestaande initiatieven

In de tabel op pagina 5 staan initiatieven binnen Nederland die al als doelstelling hebben om organisaties te ondersteunen bij het vinden van de weg naar de juiste partij. Deze initiatieven kennen geen gestructureerde, onderlinge samenwerking of informatie-uitwisseling. Mede daarom is het lastig voor een individuele organisatie in Nederland om de juiste informatie over een incident te vinden, danwel relevante organisaties te vinden die ondersteuning kunnen bieden tijdens de incidentafhandeling. Het CWN streeft ernaar om deze initiatieven bij elkaar te brengen of te omarmen. Dit maakt het, naar verwachting, mogelijk om snel stappen te zetten voor deze functie omdat er al (op kleinere schaal) aan dit probleem wordt gewerkt. In de tabel op pagina 5 staat een opsomming van verschillende initiatieven die aansluiten bij het invullen van de behoefte aan een gidsfunctie ten behoeve van incidentafhandeling voor organisaties in Nederland.

[1] Zie voor een overzicht Bijlage 1: Functie Informatiedeling.

Naam initiatief	Doelstelling
Platform Veilig Ondernemen – De HackHelpdesk	De HackHelpdesk is een initiatief van diverse partijen dat zich richt op het ondersteunen van ondernemers die geconfronteerd worden met cybercriminaliteit. Om zo gericht mogelijk advies te geven kunnen ondernemers hun vraag voorleggen aan de AI-gedreven chatbot Cyberwijzer of een makkelijk keuzemenu doorlopen om schriftelijke informatie te vinden over hun situatie.
Saxion Hogeschool – CyberCavalerie Incident response keten voor mkb	Het doel van het project is om incidentafhandeling voor het mkb efficiënter in te richten. Dit platform koppelt het getroffen mkb, na een korte triage, aan een 'private incident responder'. Het bedrijf kan rechtstreeks contact opnemen met het platform. Een belangrijk onderdeel is ook het contact via zogeheten first level responders.
Centrum voor Criminaliteitspreventie en Veiligheid (CCV) – Keurmerk Incident Response	Het Centrum voor Criminaliteitspreventie en Veiligheid (CCV) is bezig om een keurmerk op te richten voor partijen die incidentresponse diensten aanbieden. Het doel is om opdrachtgevers een bepaalde mate van zekerheid te geven dat een aanbieder aan minimumeisen voldoet en een basiskwaliteit levert. De aanbieder met het keurmerk werkt systematisch volgens de geldende spelregels. Hier is ook onafhankelijk toezicht op.
Nationaal Response Netwerk	Het Nationaal Response Netwerk is een netwerk van organisaties die hebben afgesproken elkaar te helpen bij hun incident response als de capaciteit of kennis van een organisatie niet afdoende is om het incident zelf af te handelen. De basis van het NRN is een convenant waarin deze afspraken zijn opgenomen.

Lopende programma's

Naast de verschillende organisaties en initiatieven zijn er ook programma's begonnen om de operationele publiek-private samenwerking tussen organisaties tijdens incidenten te verbeteren. Een voorbeeld hiervan is het programma Cyclotron. Dit programma heeft onder andere als doel om ten tijde van een cybersecurity-incident, tijdig en geanonimiseerd, dreigingsinformatie uit te wisselen tussen publieke en private partners. Het lijkt voor de hand te liggen om resultaten van het programma Cyclotron op te nemen in het CWN. In dit programma worden informatie-uitwisselingsplatforms gebruikt zoals MISP, Mattermost en OpenCTI. Deze succesvolle aanpak lijkt toepasbaar voor de CWN-functie Informatie-uitwisseling.

Doel(en) binnen het bouwplan

In de visie op het CWN valt te lezen dat organisaties door een sectorale CSIRT in het kader van de NIS2 ondersteuning krijgen. Daarnaast is er een grote groep organisaties die niet direct hulp krijgt bij incidentafhandeling en dat wel nodig heeft vanuit het CWN. Het belangrijkste doel van de functie Incidentafhandeling is ondersteuning leveren aan organisaties ten tijde van een incident.
Deze ondersteuning bestaat primair uit.

Subdoel	Beschrijving	Prio	Oplossing
Doorverwijzing naar juiste informatie	Organisaties moeten goed worden doorverwezen naar relevante informatie. Het doel is dat organisaties met behulp van een gidsfunctie toegang krijgen tot informatie/kennisproducten/ handelingsperspectieven die zij kunnen gebruiken om zich voor te bereiden op incidenten. Met behulp van de functie Incidentafhandeling wordt dit gerealiseerd in samenwerking met de functies Kennisuitwisseling en Opleiding, trainen en oefenen.	Zeer hoog	Ontwikkelen van omgeving binnen de 'centrale hal' van kennisuitwisseling voor relevante incidentafhandelings informatie.
Doorverwijzing naar juiste partijen	Organisaties moeten kunnen worden doorverwezen naar organisaties die hen kunnen helpen tijdens hun incidentafhandeling. Binnen deze functie van het CWN wordt dit gerealiseerd met behulp van de gidsfunctie. Deze functionaliteit moet organisaties helpen bij het vinden van informatie over andere organisaties die hen kunnen bijstaan bij hun incidentafhandeling.	Midden	Ontwikkelen van omgeving binnen de 'centrale hal' van kennisuitwisseling voor relevante incidentafhandelings informatie.
Delen van informatie over incidenten	Informatie over incidenten moet zoveel mogelijk worden gedeeld. Voor het delen van informatie tijdens incidenten wordt binnen het CWN de functie Informatiedeling opgezet. Deze functie zorgt er tijdens incidenten dus voor dat deelbare informatie over incidenten zoveel mogelijk wordt verzameld en gedeeld binnen het CWN. Dit heeft ook een sterke relatie met de doelstellingen die binnen het programma Cyclotron worden gerealiseerd.	Hoog	Informatiedelingsafspraken voor en over incidenten.
Opstellen kennisproducten voor incident-afhandeling	De functie Incidentafhandeling heeft als doel om, wanneer een incident achter de rug is, inzichten te verzamelen en te analyseren. Hiervoor wordt gebruikgemaakt van de samenwerkings-verbanden die voor deze functie worden vormgegeven. De resultaten worden aangeboden aan de functie Kennisuitwisseling voor het opstellen van kennisproducten ter verbetering en voorbereiding van incidentafhandeling.	Midden	Afspraken over incidentafhandeling en kennisproductontwikkeling.

Samenhang en afhankelijkheden

Samenhang met Kennisuitwisseling

De functie Incidentafhandeling kent een nauwe samenwerking met de functie Kennisuitwisseling. Kennisproducten en handelingsperspectieven ondersteunen organisaties in de voorbereiding op incidentafhandeling. Incidenten zijn een bron van informatie voor het opstellen van nieuwe, aangepaste kennisproducten. Daarom zal de functie Incidentafhandeling een nauwe uitwisseling van informatie kennen met de functie Kennisuitwisseling. Het is van belang dat er een mechanisme is om vanuit incidentinformatie trends, ontwikkelingen, en behoeften te extraheren die kunnen worden gebruikt om kennisproducten op te stellen.

Het helpt organisaties (juist tijdens een incident) om een incidentafhandeling goed uit te voeren, als zij kunnen beschikken over eenvoudig vindbare kennisproducten.

- Voorafgaand aan een incident is er een behoefte aan kennis- en informatieproducten die bijdragen aan preventie. Deze producten worden verwacht vanuit de functie Kennisuitwisseling.
- Nadat een incident is afgehandeld, is het van belang om informatie en kennis te vergaren en deze om te zetten naar kennisproducten. Deze producten worden verwacht vanuit de functie Kennisuitwisseling.

De samenhang tussen de functies Kennisuitwisseling en Incidentafhandeling bestaat uit het delen van lessons learned en evaluaties over incidenten die hebben gespeeld.

Samenhang met andere functies binnen het CWN

- Informatiedeling levert essentiële input voor de gidsfunctie die is opgezet. Door het delen van IOC's en TTPs ten tijde van incidenten, draagt informatiedeling bij aan incidentafhandeling. Het programma Cyclotron draagt vanuit informatiedeling bij aan realtime ontsluiting van incidentinformatie. Het onderwerp dreigingsinformatie wordt binnen de functie Incidentafhandeling achterwege gelaten; dit is namelijk onderdeel van de functie Informatiedeling. In tegenstelling tot te functie Informatiedeling is de functie Incidentafhandeling specifiek gericht op procesondersteuning tijdens de lauwe en warme fase van een incident. Tijdens de incidentafhandeling zal er (technische) informatie worden gedeeld door middel van de functie Informatiedeling in het CWN.
- Er is sprake van een natuurlijke samenhang met Opleiding, trainen en oefenen. De werking van instrumenten, werkwijze en afspraken kunnen in de OTO-functie worden opgepakt.

Netwerkkaart

In de visie wordt de volgende scope genoemd voor partijen die ondersteund worden vanuit de functie Incidentafhandeling: organisaties die te maken hebben met cyberincidenten, worden ondersteund door sectorale CSIRTs in het kader van de NIS2. Dit geldt ook voor partijen die deze ondersteuning niet krijgen, maar wel ondersteuning nodig hebben. De netwerkkaart voor incidentafhandeling zal verder worden uitgewerkt, aangescherpt en aangevuld bij het bouwen van het netwerk.

In de visie is een netwerkkaart opgenomen voor Incidentafhandeling. Het gedetailleerde overzicht van de rollen en samenhang tussen de organisaties binnen deze functie staat op pagina 14.

Activiteiten en deliverables

Op basis van de eerder beschreven (sub)doelen is hieronder een aantal deliverables en activiteiten beschreven.

Subdoel	Prio	Deliverable	Activiteit
Inzicht in de organisaties	Zeer hoog	• Aangepaste topologie, • Aangepaste netwerkkaart.	• Updaten van de netwerkkaart van organisaties d.m.v. het in kaart brengen van de spelers en de verhoudingen onderling. • Inzichtelijk maken van rollen en functies bij organisaties. • In kaart brengen van de verschillende persona's bij organisaties. • Inzichtelijk maken van netwerkpartners, rol in het netwerk en verantwoordelijkheid binnen het netwerk.
Doorverwijzing naar juiste informatie	Zeer hoog	Gidsfunctie in de 'centrale hal' (wordt ontwikkeld binnen de functie Kennisuitwisseling) voor de doorverwijzing naar de juiste informatie.	• Overzicht van beschikbare en relevante informatie voor Incidentafhandeling en over handelingsperspectieven gericht op het bestrijden van het opstellen van een incident . • Het beschikbaar maken van het overzicht binnen de 'centrale hal'. • Opzetten van een overzicht met informatie over verplichtingen die worden opgelegd vanuit wet- en regelgeving.
Doorverwijzing naar juiste partijen	Midden	Gidsfunctie in de 'centrale hal' voor doorverwijzing naar de juiste/ relevante partijen.	• Overzicht van groepen organisaties waar naar kan worden doorverwezen. • Opzetten van een overzicht over de incidentketen, met informatie over beschikbare en relevante hulpverlening. • Beschikbaar stellen van dit overzicht in de 'centrale hal'.
Delen van informatie over incidenten	Hoog	Informatiedelings-afspraken voor en over incidenten inrichten.	• Bijeenkomsten organiseren om best practices te delen en adviezen te krijgen en te geven. • Overzicht van bestaande informatiedelingsinitiatieven over incidentafhandeling. • Overzicht van 'witte vlekken' voor incidentafhandeling. • Samenwerkafspraken voor informatiedeling over incidenten. • Overzicht opstellen en beschikbaar maken in de 'centrale hal' over het aanhaken bij bestaande initiatieven waar kennisuitwisseling- en informatiedeling plaatsvindt over afgelopen incidenten. • Blauwdruk opstellen en beschikbaar maken van een incidentendraaiboek.
Opstellen kennisproducten voor incidentafhandeling	Midden	• Samenwerkingsafspraken, • Lijst met incidentafhandelings-onderwerpen, • Handelingsperspectieven voor incidenten.	• Plan opstellen en samenwerkingsafspraken maken om binnen het netwerk inzichten over incidenten te verzamelen en te analyseren om vervolgens om te kunnen zetten naar een kennisproduct. • Lijst opstellen van incidentafhandelings onderwerpen waarvoor handelingsperspectief moet worden opgesteld. • Kennisproducten die handelingsperspectief voor incidentafhandeling beschrijven.

De gidsfunctie

De functie Incidentafhandeling levert een gids om organisaties te helpen de voor hen relevante bronnen en ketenpartners te vinden, zodat zij kunnen voldoen aan hun wettelijke, contractuele en/of maatschappelijke verplichtingen op dit vlak. Om deze gidsfunctie te vervullen en verbeteren, is het de bedoeling dat CWN-samenwerkingspartners bijeenkomen om te leren van ervaringen en deze te vertalen in bruikbare best practices en adviezen. De opgedane inzichten en ervaringen worden vervolgens geborgd in de kennisdelingsfunctie van het CWN, en waar relevant ook ingezet ten behoeve van de OTO- en informatiedelingsfuncties. Als uitgangspunt wordt in het CWN gebruikgemaakt van bestaande succesvolle initiatieven, want: wat goed is, hoeft niet vervangen te worden.

De gidsfunctie is een centrale en vanzelfsprekende plek voor organisatie om hulp te vinden bij hun incidentafhandeling. De gids zal de weg wijzen naar relevant handelingsperspectief en naar organisaties die bijvoorbeeld incidentresponse diensten leveren.

De gidsfunctie geeft een overzicht van verschillende groepen organisaties. De volgende groepen organisaties worden nu voorzien:

- De sectorale CSIRTs en hun doelgroepen.;
- De verschillende brancheverenigingen en de ondersteuning/ informatie die zij of hun deelnemers bieden (denk aan o.a. MSSPs en MSPs);
- De (semi-) overheidsorganisaties zoals de fraudehelpdesk en Slachtofferhulp.
- Organisaties die advies kunnen geven op het juridische en communicatieve vlak van cybersecurity;
- Bestaande initiatieven die behulpzaam zijn bij incidentafhandeling zoals lokale of regionale initiatieven.

De gidsfunctie geeft overzicht om de weg naar de politie te vinden voor het doen van aangifte en adviezen voor aangifte.

Voor de gidsfunctie creëren we een centrale, digitale plek als ingang voor de ontsluiting van deze informatie. De gidsfunctie brengen we onder bij de functie Kennisuitwisseling zodat er één centrale plek is voor alle informatie.

Handelingsperspectieven

Tijdens incidentafhandeling is het van belang dat organisaties weten hoe ze moeten handelen. De functie Incidentafhandeling stelt handelingsperspectieven ter beschikking aan organisaties. Daarvoor is het noodzakelijk om in de koude fase vanuit samenwerkingsverbanden en incidentrapportages de onderwerpen te identificeren waaruit handelingsperspectief kan worden afgeleid en waarvoor kennisproducten moeten worden gemaakt. Deze onderwerpen en inzichten dienen als input voor de functie Kennisuitwisseling die de perspectieven vervolgens ter beschikking kan stellen aan de doelgroep.

Voortbouwen op bestaande initiatieven voor incidentafhandeling

Binnen de functie Incidentafhandeling dienen bestaande initiatieven in kaart te worden gebracht. Door het samenbrengen, en het aan elkaar verbinden, van de organisaties achter deze initiatieven, vindt een versterking plaats op kennis- en informatiedeling voor incidentafhandeling doordat:

- Netwerken leunen op vertrouwen, mensen dienen elkaar te kennen voordat ze elkaar helpen.
- De gezamenlijke verantwoordelijkheid voor de gidsfunctie in het netwerk hiermee kan worden gecreëerd, door het maken van samenwerkingsafspraken over de inrichting en het onderhoud van de gidsfunctie.
- Gezamenlijk inzicht zorgt dat de 'witte vlekken' kunnen worden geïdentificeerd en bespreekbaar worden gemaakt voor deze functie.
- Het delen van informatie en ervaringen over incidentafhandeling binnen het netwerk bijdraagt aan de verbetering van handelingsperspectief. Partijen die incidentresponse diensten leveren bij Nederlandse bedrijven en organisaties moeten in vertrouwen, laagdrempelig en geanonimiseerd, ruwe dreigingsinformatie kunnen delen binnen het CWN. Het programma Cyclotron en het project Melissa leveren een blauwdruk voor deze samenwerkingsverbanden.

Randvoorwaarden

Voor een succesvolle implementatie van de bovenstaande activiteiten en daarmee een succesvolle inrichting en werking van de functie Incidentafhandeling van het CWN zijn de onderstaande functiespecifieke randvoorwaarden noodzakelijk:

- Het is van belang om in het ontwerp en de implementatie van de gidsfunctie rekening te houden met een aantal zaken:
  - De gidsfunctie mag niet marktverstorend werken en kan dus geen voorkeur geven aan specifieke dienstverleners.
  - Goed onderhoud en beheer van de gidsfunctie is cruciaal. De gidsfunctie is een dynamische plek van informatie. Dat betekent dat de gidsfunctie moet worden beheerd en actueel moet worden gehouden zodat deze ook van nut is - en blijft - voor incidentafhandeling. Het is daarom van belang om, naast het ontwerp van de gids zelf, de onderhoud- en beheerprocessen vorm te geven en ook hierin de rol van schakelorganisaties duidelijk te maken.
  - Het bestaan van een centrale, online plek moet ook bekend zijn bij organisaties die doorgaans initieel bij incidenten worden benaderd zoals lokale politiebureaus, verzekeraars en diverse centrale overheidswebsites.
- Om informatie-uitwisseling over incidenten structureel vorm te geven, zullen er samenwerkingsafspraken moeten worden gemaakt met de commerciële dienstverleners die incidentresponse uitvoeren bij slachtoffers. Deze partijen zullen hier ook afspraken over moeten maken met hun klanten, zoals aanpassing van een eventuele NDA waarin is opgenomen dat technische incidentinformatie (TTP's, IOC's) geanonimiseerd zal worden gedeeld binnen het CWN.

Functiecanvas

Incidentafhandeling

Doelen

(Deel)opgave

Het doel van de functie Incidentafhandeling is ondersteuning leveren aan organisaties ten tijde van een incident. Deze ondersteuning bestaat uit:

- Doorverwijzing naar juiste informatie;
- Doorverwijzing naar juiste partijen;
- Delen van informatie over incidenten;
- Opstellen kennisproducten voor incidentafhandeling.

Buiten scope

Samen coördineren en regie voeren

- Het managen/afhandelen van actuele incidenten of crises, hiervoor zijn organisaties zelf verantwoordelijk.
- Het oplossen van een mogelijk te ontstaan “verdringingseffect”.
- Het uitwisselen van operationele informatie tijdens incidenten of crises.
- Het verspreiden van informatie- of kennisproducten, hiervoor wordt gebruikgemaakt van de functie Kennisuitwisseling.

Randvoorwaarden uitvoering

Samen coördineren en regie voeren

- Niet marktverstorend werken en geen voorkeur geven voor specifieke dienstverleners.
- Goed onderhoud en beheer en actualiteit van de gidsfunctie.
- Bekendheid.
- Samenwerkingsafspraken met de commerciële dienstverleners.

Activiteiten

Samen creëren

1. Inzichtelijk maken van de organisaties
   - Updaten van de netwerkkaart van organisaties;
   - Inzichtelijk maken van rollen en functies;
   - In kaart brengen verschillende persona’s;
   - Inzichtelijk maken van netwerkpartners.
2. Doorverwijzen naar de juiste informatie
   - Overzicht van beschikbare/relevante informatie voor incidentafhandeling en over handelingsperspectieven;
   - Het beschikbaar het overzicht binnen de ‘centrale hal’;
   - Opzetten van een overzicht over verplichtingen die worden opgelegd vanuit wet- en regelgeving.
3. Delen van informatie over incidenten
   - Bijeenkomsten organiseren;
   - Overzicht bestaande informatiedelingsinitiatieven over incidentafhandeling;
   - Overzicht ‘witte vlekken’ voor incidentafhandeling;
   - Samenwerkafspraken informatiedelingincidenten;
   - Overzicht initiatieven waar kennisuitwisseling- en informatiedeling plaatsvindt over incidenten;
   - Blauwdruk opstellen en beschikbaar maken van een incidentendraaiboek.
4. Opstellen kennisproducten voor incidentafhandeling
   - Plan opstellen en samenwerkingsafspraken maken;
   - Lijst opstellen van incidentafhandelings onderwerpen;
   - Kennisproducten die handelingsperspectief voor incidentafhandeling beschrijven.

Deliverables

Samen creëren

- Aangepaste topologie;
- Aangepaste netwerkkaart;
- Gidsfunctie in de ‘centrale hal’ voor de doorverwijzing naar de juiste informatie;
- Gidsfunctie in de ‘centrale hal’ voor doorverwijzing naar de juiste/relevante partijen;
- Informatiedelingsafspraken voor en over incidenten inrichten;
- Samenwerkingsafspraken;
- Lijst met incidentafhandelingsonderwerpen;
- Handelingsperspectieven voor incidenten.

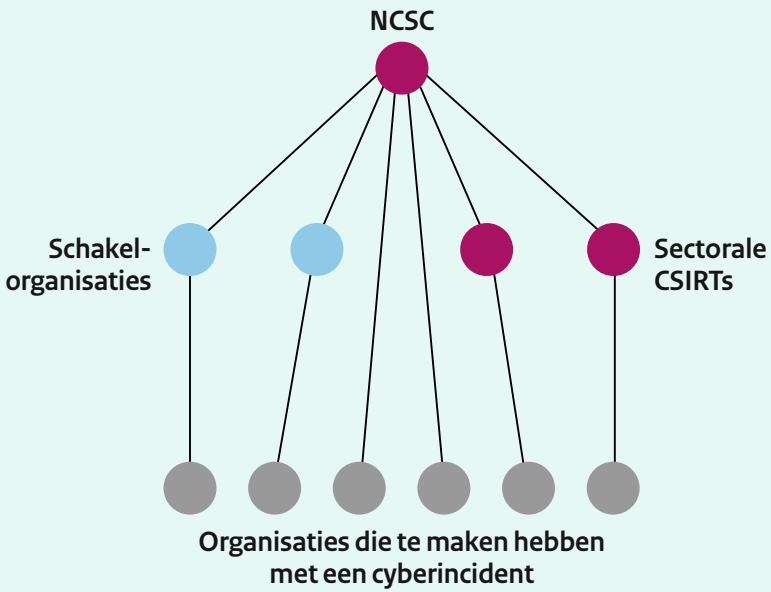
Netwerkkaart

Ontmoeten

De functie ondersteunt:

- Organisaties die te maken hebben met cyberincidenten, die worden ondersteund door sectorale CSIRTs;
- Partijen die geen ondersteuning krijgen, maar wel ondersteuning nodig hebben;
- De netwerkkaart voor incidentafhandeling zal verder worden uitgewerkt, aangescherpt en aangevuld bij het bouwen van het netwerk.

Incidentafhandeling netwerkkaart



	Rollen	Organisaties
	Centraal knooppunt	NCSC en de sectorale CSIRTs
	Organisaties die fungeren als schakel naar organisaties die weerbaar kunnen maken	Koepelorganisaties, branche-organisaties, coalities, samenwerkingsverbanden, (sectorale) CSIRTs, etc.
	Organisaties die weerbaar kunnen maken en dus informatie moeten ontvangen	Leveranciers van IT-oplossingen, zoals ISPs, MSPs en MSSPs, maatwerkleveranciers.
	Organisaties die weerbaar willen worden en te maken hebben met een cyberincident. Sommige van deze organisaties hebben een meldplicht, andere niet.	Midden- en hoogvolwassen organisaties vallende onder Vitale en/of NIS2-sectoren of buiten de NIS2. Doelwit- en slachtoffernotificaties kunnen hier direct of via netwerkeigenaren worden verstrekt maar ook aan burgers. Organisaties met een hogere mate van volwassenheid kunnen rechtstreeks en via schakelorganisaties worden geïnformeerd.

Opgesteld door
CWN publiek-private werkgroep
Incidentafhandeling

Uitgave
Nationaal Cyber Security Centrum (NCSC)
Postbus 117, 2501 CC Den Haag
Turfmarkt 147, 2511 DP Den Haag
070 751 5555

Meer informatie
www.ncsc.nl
info@ncsc.nl
@ncsc_nl

September 2025