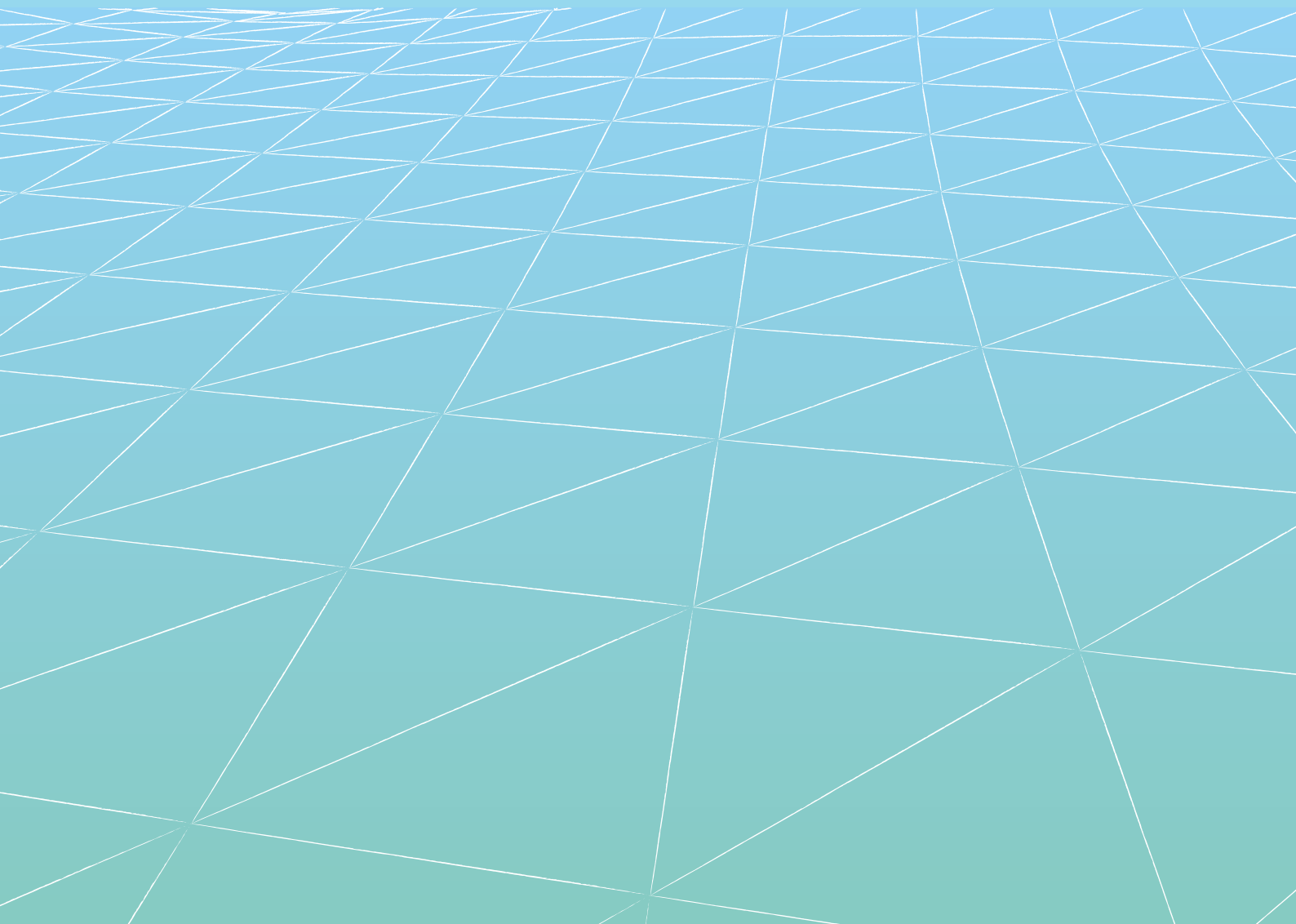
Nationaal Cyber Security Centrum
*Ministerie van Justitie en Veiligheid*

**Bijlage 2** van het Bouwplan Cyberweerbaarheidsnetwerk (CWN)

# Functie Doelwit- en slachtoffernotificatie

*Uitwerking van CWN-functie Doelwit- en slachtoffernotificatie in publiek-private samenwerking*



# Inleiding

Sinds januari 2023 werken het NCSC, het DTC en het CSIRT-DSP, vooruitlopend op de integratie, intensief samen op het gebied van de mens, het proces en de technologie binnen de drie stappen in het Doelwit- en slachtoffernotificatieproces: informatie vergaren, verwerken en verspreiden. Sindsdien zijn er meerdere bijeenkomsten geweest met stakeholders. Die hebben er onder andere toe geleid dat de functie Doelwit- en slachtoffernotificatie (DSN) al in een ver stadium van realisatie is en vanuit één loket informatie over doelwitten en slachtoffers van cyberaanvallen kan verzamelen, verwerken en verspreiden. Dit plan vormt een basis voor het continue verbeterproces van de DSN-functie.

# Definitie en scope van de functie

De functie Doelwit- en slachtoffernotificatie (DSN) betreft een specifieke vorm van de functie informatiedeling in het CWN. Binnen deze functie ligt de nadruk op het waarschuwen van organisaties die (potentieel) kwetsbaar zijn voor aanvallen (doelwit) of al gecompromitteerd zijn (slachtoffer). Daarmee speelt de functie DSN een rol tijdens de gehele lifecycle van incidenten: vanaf het moment van dreiging tot aan het optreden bij incidenten.

Vanuit de eigen taken van het NCSC, het CSIRT-DSP en het DTC vinden er versnipperd notificatie-activiteiten plaats, bijvoorbeeld gericht op specifieke doelgroepen. Zo stuurt het NCSC notificaties naar vitale organisaties, de Rijksoverheid en de schakelorganisaties in het Landelijk Dekkend Stelsel (LDS). Het CSIRT-DSP stuurt notificaties naar digitale diensten en het DTC naar het niet-vitale bedrijfsleven. De Nederlandse Cybersecuritystrategie (NLCS) stelt dat iedereen in Nederland gewaarschuwd moet kunnen worden wanneer ze (mogelijk) slachtoffer of doelwit zijn van een cyberaanval. Daarom is er één loket nodig waar informatie over slachtoffers en doelwitten van cyberaanvallen wordt verzameld, verwerkt (o.a. verrijkt) en verspreid.

De functie DSN richt een loket in waardoor organisaties (publiek en privaat, vitaal en niet-vitaal en groot en klein) beter in staat zijn om hun digitale weerbaarheid te vergroten.

# Huidige situatie

Het NCSC en het CSIRT-DSP voeren de DSN-functie uit op basis van de Wet beveiliging netwerk- en informatiesystemen (Wbni) die zal overgaan in de Cyberbeveiligingswet (Cbw), die nog in werking treedt. Het DTC voert de DSN-functie uit op basis van de Wet bevordering digitale weerbaarheid bedrijven (Wbdwb).

Sinds januari 2023 werken het NCSC, het DTC en het CSIRT-DSP, vooruitlopend op de integratie, intensief samen op het gebied van de mens, het proces en de technologie binnen de drie stappen in het DSN-proces: informatie vergaren, verwerken en verspreiden. Dit heeft er onder andere toe geleid dat de functie DSN al in een ver stadium van realisatie is en vanuit één loket informatie over slachtoffers en doelwitten van cyberaanvallen kan verzamelen, verwerken en verspreiden. Sinds eind 2024 notificeert de functie DSN vanuit één technisch geautomatiseerde oplossing, op basis van bekende assets, over dreigingsinformatie. In 2025 zal het NCSC vanuit deze oplossing ook ongevraagd notificaties uitsturen. Organisaties en hun assets die niet bekend zijn met deze oplossing, worden eerst in kaart gebracht en ontvangen via het technisch geautomatiseerde systeem notificaties en eventueel aanvullende berichtgeving per e-mail of telefoon.

Organisaties die op eigen verzoek notificaties ontvangen, kunnen in het MijnNCSC-portaal hun assets en notificatievoorkeur zelf regelen. Met de komst van de Cbw zal het aantal organisaties dat van MijnNCSC gebruik kan maken, exponentieel groeien. Hiermee zal de reikwijdte van de DSN vergroten en de informatie sneller kunnen worden gedeeld. Om met de DSN-functie (meer) organisaties op verzoek te notificeren, is het belangrijk dat alle (NIS2-)organisaties bereid zijn zich te registreren met hun assets in MijnNCSC.

De ruim twee miljoen Nederlandse bedrijven die hun assetinformatie niet hebben doorgegeven, kunnen wel ongevraagd notificaties krijgen. De uitdaging bij dit ongevraagd notificeren, zit vooral in het herleiden van assets naar een organisatie en het traceren van de juiste contactpersoon.

# Doel(en) binnen het bouwplan

Het doel van de functie DSN in het CWN is om organisaties binnen de doelgroep van het NCSC, CSIRT-DSP en DTC tijdig en effectief te notificeren over dreigingsinformatie zodat zij maatregelen kunnen treffen om mogelijke schade te detecteren, te beperken of te voorkomen. Het bereiken van een dermate omvangrijke doelgroep zal zoveel mogelijk gestandaardiseerd en geautomatiseerd verlopen. Dat geldt voor het vergaren van informatie, maar ook voor het verwerken en verspreiden ervan.

Een continu verbeterproces is belangrijk om het doel van de functie DSN te kunnen nastreven. Er zullen wellicht op verschillende vlakken aanpassingen of extra functionaliteiten nodig zijn. Hierbij valt te denken aan de toepasbaarheid en het begrijpelijk maken van een handelingsperspectief voor een diverse doelgroep, het herleiden van assets naar de juiste organisatie tot het kunnen bereiken van dé persoon of partij die daadwerkelijk met de dreigingsinformatie de juiste vervolgstappen kan nemen.

Daarnaast haalt de functie structureel feedback op bij stakeholders om op die manier geschikte aanpassingen te doen of nieuwe functionaliteiten toe te voegen. Hier kan in het bijzonder worden gedacht aan ‘personalisatie’ of organisatie specifieke inrichting voor DSN-activiteiten. Ook is er een noodzaak om afspraken te maken over de verspreiding van DSN-informatie met afnemers zoals sectorale CSIRTs en leveranciers van IT-oplossingen zoals ISPs, MSPs (IT-dienstverleners) en MSSPs.

# Samenhang en afhankelijkheden

## Samenhang met Informatiedeling

De DSN-functie is een vorm van informatiedeling en heeft daardoor automatisch een samenhang met de functie Informatiedeling. De Toekomstvisie op het CWN definieert de DSN ook als een bijzondere vorm van informatiedeling. Organisaties met systemen die kwetsbaar zijn voor aanvallen (doelwit) of al gecompromitteerd zijn (slachtoffer), worden gewaarschuwd zodat zij in staat zijn om gepaste maatregelen te nemen. Bij Informatiedeling gaat het om technische gegevens en geanalyseerde informatie voor schakelorganisaties, leveranciers en CSIRTs die deze informatie kunnen gebruiken om met hun achterban en klanten te delen. Het netwerk zorgt ook voor operationeel contact tussen de verschillende schakels voor het geval dat informatie snel moet worden gedeeld op operationeel niveau. Echter, bij de bouw van het CWN is voorzien dat DSN onder de functie Informatiedeling zal vallen en daar als bijzondere vorm van informatiedeling nadere invulling krijgt, naast projecten zoals Melissa en programma Cyclotron.

## Samenhang met Kennisuitwisseling

Als bijzondere vorm van de functie Informatiedeling heeft ook de functie DSN een relatie met de functie Kennisuitwisseling. Inzichten vanuit DSN, zoals aantallen notificaties en terugkerende (bekende) kwetsbaarheden of configuratiefouten binnen de doelgroep die op een andere manier (extra) aandacht verdienen, kunnen als input fungeren voor de creatie van kennisdocumenten. Deze gaan vervolgens naar de functie Kennisuitwisseling.

# Netwerkkaart

In de visie is de typologie van Doelwit- en slachtoffernotificatie weergegeven. Dit is ook voor de bouw van het CWN de juiste weergave van het netwerk.

Voor een gedetailleerd overzicht van de rollen en samenhang tussen de organisaties binnen deze functie, zie de netwerkkaart op pagina 10.

# Activiteiten en deliverables

Het CWN kan voor DSN een katalysator zijn voor het ophalen van feedback vanuit stakeholders voor het verbeteren van de huidige, operationele functionaliteit, de werkwijze en communicatie over de DSN. Het doel dat hiermee wordt bereikt is het verbeteren van de dienstverlening, zodat deze beter aansluit op de wensen, (informatie)behoeften en gedrag van de doelgroep.

| Activiteit | Planning | Deliverables |
|---|---|---|
| **Inrichten feedback DSN**<br><br>Voor de functie DSN is het doel om structureel feedback op te halen bij stakeholders om op die manier de juiste aanpassingen te doen of nieuwe functionaliteiten toe te voegen. | Q3-Q4 2025 | • Feedbacksessie organiseren met stakeholders.<br>• Feedback verwerken:<br>  • aanpassingen maken in huidige DSN;<br>  • functionele aanpassingen doorvoeren;<br>  • communicatie verbeteren.<br>• Stakeholders informeren over aanpassingen en functionele verbeteringen.<br>• Feedback opnemen in DSN-user stories. |
| **Opstellen van DSN Distributiestrategie** | Q1 2026 | Distributiestrategie. |
| **Afspraken maken met sectorale CSIRTs en leveranciers zoals ISPs** | 2025-2026 | Afspraken over distributienotificaties. |
| **Situationeel beeld van Nederland** | Doorlopend | • Feedbacksessies voor ophalen beeld.<br>• Situationeel beeld opstellen. |

# Functiecanvas

## Doelwit- en slachtoffernotificatie

**Doelen** (Deel)opgave

Het op een zo veel mogelijk gestandaardiseerde en geautomatiseerde wijze tijdig en effectief notificeren van de doelgroep van het NCSC, CSIRT-DSP en DTC over dreigingsinformatie, zodat zij maatregelen kunnen treffen om mogelijke schade te detecteren, beperken of te voorkomen. Daarnaast is het doel om structureel feedback op te halen bij de doelgroep om zo de juiste aanpassingen te doen en afspraken te maken over de verspreiding van DSN informatie met afnemers.

**Buiten scope** Samen coördineren en regie voeren

- Het waarschuwen van organisaties die potentieel kwetsbaar zijn voor aanvallen of al gecompromitteerd zijn.
- Het vervullen van de rol van één loket waar informatie over slachtoffers en doelwitten van cyberaanvallen wordt verzameld, verwerkt en verspreid.
- Het leveren van informatie in de lifecycle van incidenten vanaf het moment van dreiging tot aan het optreden van een incident.

**Binnen scope** Samen coördineren en regie voeren

- Spelen van een rol na het optreden van een incident.
- Geen meld- of aangifteplatform voor incidenten.

**Activiteiten** Samen creëren

Het fungeren als loket voor de vergaring, verspreiding en verwerking van dreigingsinformatie:

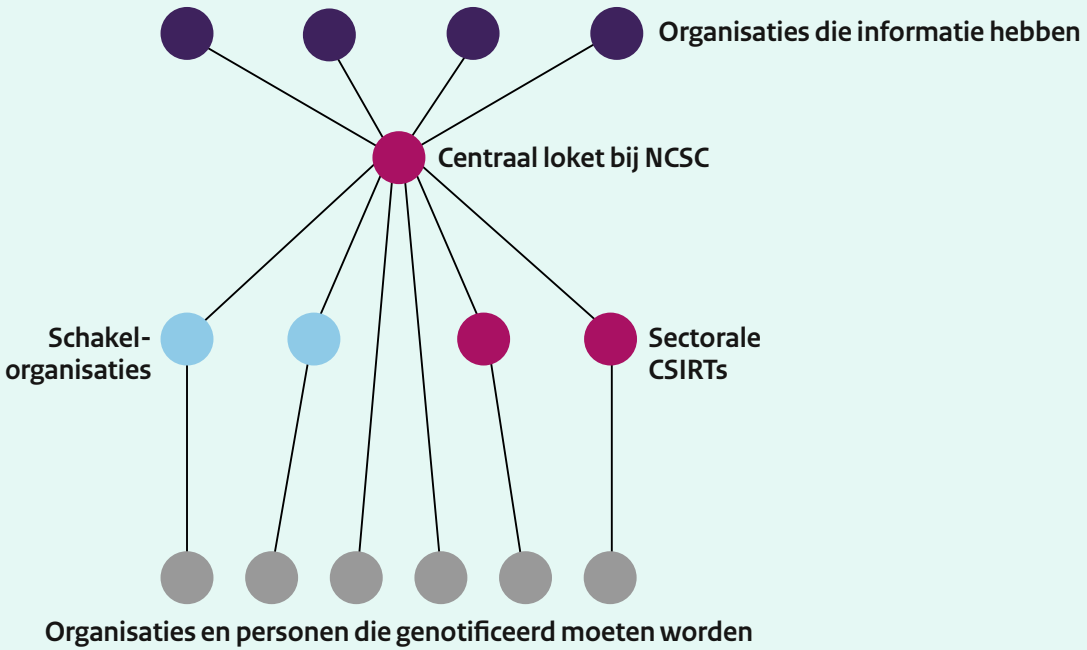
- Het zoveel mogelijk standaardiseren en automatiseren van het vergaren, verwerken en verspreiden van dreigingsinformatie.
- Door feedback gestuurde aanpassingen doorvoeren en/of nieuwe functionaliteiten toevoegen in DSN.
- Opstellen van een DSN-distributiestrategie.
- Afspraken maken met sectorale CSIRTSs en leveranciers zoals ISPs.
- Een situationeel beeld schetsen van cybersecuritydreigingen in Nederland.

**Deliverables** Samen creëren

Opleveren van het volgende:

- Feedbacksessie met stakeholders en deze vervolgens verwerken door aanpassingen te maken in huidige DSN, functionele aanpassingen door te voeren en communicatie te verbeteren. Vervolgens dienen stakeholders geïnformeerd te worden over aanpassingen en functionele verbeteringen en wordt de feedback opgenomen in DSN-user stories.
- Distributiestrategie DSN.
- Gedocumenteerde afspraken over distributienotificaties.
- Een situationeel beeld van cybersecuritydreigingen in Nederland..

# Doelwit- en slachtoffernotificatie netwerkkaart




| | Rollen | Organisaties |
|---|---|---|
| | Informatieknooppunt | NCSC: loket voor doelwit- en slachtoffernotificatie |
| | Organisaties die fungeren als informatiedeelplatform voor andere (groepen) organisaties | Organisaties die als contactpunt dienen voor te informeren organisaties en personen (zoals ISPs), |
| | Organisaties die over relevante informatie beschikken | Organisaties die over relevante (dreigings)informatie beschikken, veelal hoog volwassen publieke en private bronorganisaties, zoals politie, AIVD, DIVD en securitybedrijven. |
| | Organisaties die weerbaar willen worden | Organisaties waarvan vastgesteld is dat ze doelwit en/of slachtoffer zijn (heel ondernemend Nederland). |

**Opgesteld door**
CWN publiek-private werkgroep
Doelwit- en slachtoffernotificatie

**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