# Metrokaart en knelpunten Abuse Informatie – 12-2020

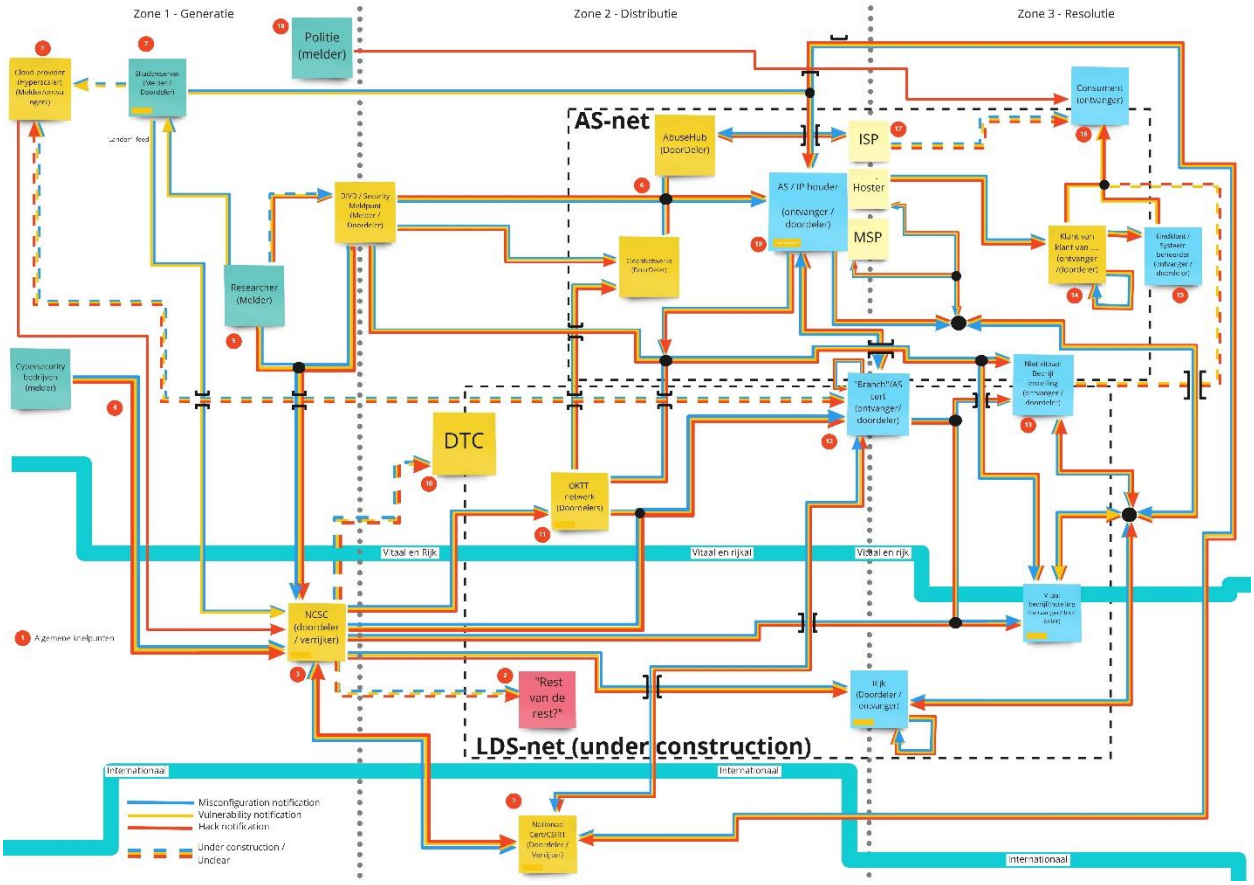
Voor u ligt de tweede versie **De Metrokaart van Abuse gerelateerde informatie inclusief de lijst van geconstateerde knelpunten**. Deze kaart is samengesteld door de leden van het Anti Abuse Netwerk (AAN) dat zich ten doel stelt het Nederlandse internet veiliger te maken door ervoor te zorgen dat informatie over daadwerkelijk onveilige configuraties, kwetsbaarheden en misbruik terecht komt bij diegenen die daar iets aan kunnen doen.

Deze kaart is tot stand gekomen door zeer systematisch te werk te gaan. Eerst hebben we een overzicht gemaakt van welke soorten informatie relevant zijn. Vervolgens is er een overzicht gemaakt van alle betrokken partijen die wij kennen in deze arena, veelal aangesloten bij ons netwerk. Daartussen hebben wij de informatiestromen in kaart gebracht die ons bekend zijn. Dit document is een momentopname op basis van de parate kennis in ons netwerk. Door de breedte van ons netwerk en de tijd en aandacht die wij hier als collectief aan geschonken hebben, hebben wij vertrouwen in de kwaliteit van het resultaat.

Dit document is de tweede iteratie van een dynamisch document.  Aan deze iteratie is een knelpuntenlijst toegevoegd om de kaart wat inzichtelijker te maken. Daarnaast is de feedback naar aanleiding van de eerste iteratie verwerkt. Wij nodigen nog steeds eenieder uit om onze kennis aan te vullen en feedback te geven op dit document. Op die manier kunnen we een kaart maken die de werkelijkheid zo goed mogelijk benadert. Bij significante wijzigingen zullen wij een nieuwe versie publiceren.

Deze metrokaart laat al een paar knelpunten zien. Zo wordt helder dat een deel van de informatie over dreigingen niet de juiste bestemming bereikt, een deel wordt weggegooid en een deel wordt alleen met een selecte groep gedeeld, waar een bredere, gerichte verspreiding wenselijk zou zijn. Dit komt deels door juridische obstakels, deels omdat partijen dit niet tot hun taak rekenen. In de komende tijd willen we samen met de betrokken partijen deze knelpunten zo scherp mogelijk in beeld krijgen. Zodra dat overzicht er is, zullen we dat ook publiceren en opnieuw een beroep doen op u om mee te denken.

## De Metrokaart




Een interactieve versie is te bekijken via: [https://miro.com/app/board/o9J_lbn-wMQ=/](https://miro.com/app/board/o9J_lbn-wMQ=/)

## Voorlopige conclusies

De Metrokaart is een document waarin de leden van AAN, gezamenlijk en overzicht hebben gemaakt van de berichtenuitwisseling die gebruikt wordt bij het bestrijden van onveilig geconfigureerde, kwetsbaarbare of gehackte systemen.

Op basis van De Metrokaart zelf, het onderliggende onderzoek en gesprekken en de lijst van geïdentificeerde knelpunten komen we tot de volgende voorlopige conclusies:

1) De kaart is ingewikkeld omdat het landschap ingewikkeld is, de digitale weerbaarheid zou gebaat zijn bij een eenvoudiger stelsel.
2) Momenteel is er geen enkele partij die effectief in staat is alle ontvangers te bereiken. Hierdoor missen melders een duidelijk “loket” waar zij informatie die breed verspreid moet worden kwijt kunnen.
3) Het NCSC lijkt de rol van Centraal Station te vervullen aangezien hier veel lijnen samenkomen, zij heeft echter te maken met restricties waardoor zij niet alle ontvangers kan bereiken.
4) Naast het bestaande AS-net wordt er gewerkt aan het LDS-net (het Landelijk Dekkend Stelsel). Dit LDS maakt nauwelijks gebruik van het al bestaande stelsel van CERTs en AS-en (AS-net)

5) Het DTC dat vaak nadrukkelijk naar voren geschoven wordt als “het tussenstation voor de rest”, is nog niet aangesloten op het LDS en is nog niet voldoende ingericht op deze taak.
6) Aan veel van deze genoemde knelpunten ligt de “status” van een IP -adres als persoonsgegeven ten grondslag.
7) Binnen de huidige wettelijke grenzen is het voor overheidspartijen niet mogelijk op korte termijn deze problematiek fundamenteel aan te pakken.

## Knelpunten

In de kaart zijn clusters van knelpunten aangegeven met een genummerde cirkel. In onderstaande tabel zijn deze opgenomen met een korte toelichting.

| Nr | Knelpunt | Omschrijving |
|---|---|---|
| | | **Cluster 1: Algemeen** |
| **1a** | Bepalen van de "Nationaliteit" van IP-adressen / AS nummers / domeinen is moeilijk. | Het internet kent geen landsgrenzen, maar de fysieke wereld wel. Discussie rondom de afhandeling van “abuse” richten zich vaak op Nederland, maar welk stukje van het internet is nu eigenlijk Nederlands? Is een domein dat eindigt op .nl per definitie Nederlands? Hoe zit dat dan met Nederlandse sites van multinationals? Hoe gaan we om met Nederlandse internetproviders die ook in het buitenland opereren en hiervoor een en hetzelfde AS gebruiken? |
| **1b** | IP-adres als persoonsgegeven | Binnen de kaders van de AVG is een IP-adres een persoonsgegeven. Dit betekent dat organisaties bij het verwerken van IP-adressen gehouden zijn aan de bepalingen in de AVG.<br><br>Binnen de AVG is bijvoorbeeld bepaald dat je niet zonder meer persoonsgegevens met andere partijen mag delen.<br><br>Dit maakt het uitwisselen van IP-adres informatie lastiger, zeker voor overheidsorganisaties die zich niet op alle grondslagen in de AVG kunnen beroepen, maar vooral moeten steunen op wettelijke kaders en/of algemeen belang.<br><br>Hierdoor zijn partijen als het NCSC en DTC niet vrij lijsten met IP-adressen met andere organisaties als hun wettelijke achterban te delen. |
| **1c** | In geval van (potentiële) slachtoffer notificaties wordt IP-adres door overheidspartijen geclassificeerd als “vertrouwelijke gegevens die herleid kunnen worden tot een aanbieder” | Voor dit soort gegevens gelden in de WBNI extra beperkingen wat betreft het verder verstekken aan derde partijen. Zo is bijvoorbeeld het aantal partijen waar het NCSC deze informatie aan mag verstrekken beperkt. |
| **1d** | Slachtoffernotificatie bevat vaak gevoelige data zoals wachtwoorden. | Als er sprake is van een bericht dat een systeem of persoon slachtoffer geworden is van computercriminaliteit (hack-notificatie), dan is dit bericht op zich vaak al gevoelig.<br>Maar vaak bevat de dataset waaruit deze notificatie is ontstaan extra informatie die betrekking heeft op de ernst van het incident. Deze informatie is extra gevoelig, denk bijvoorbeeld aan (al dan niet versleutelde) wachtwoorden, gestolen documenten of cryptografische sleutels, etc. Deze informatie kan, indien ze in de verkeerde handen komt, tot grote schade leiden. |

| Nr | Knelpunt | Omschrijving |
|---|---|---|
| **Cluster 2: “Rest van de rest”** | | |
| **2a** | Wat gebeurt en met de “Rest van de rest” | Het NCSC kan, op dit moment, op basis van haar mandaat en de inhoud van de WBNI en AVG bepaalde informatie niet verwerken en/of met bepaalde partijen delen. Deze “rest van de rest” is informatie die niet valt binnen de achterban van het NCSC zelf (Rijk en Vitaal). En kan ook niet als “restdata” worden doorgezet naar de bij haar aangesloten CERTS en OKTT’s. Op dit moment belandt deze informatie bij het NCSC op een dood spoor. |
| **Cluster 3: NCSC** | | |
| **3a** | Door restricties in mandaat, doelgroep en de interpretatie van de AVG door het Ministerie van Justitie & Veiligheid kan het NCSC enkel haar doelgroep en de deelnemers in het LDS (aangewezen OKTTs/Certs/etc.) deze informatie verstrekken. | Het NCSC verwerkt slechts gegevens voor een beperkt deel van Nederland. |
| **3b** | Niet altijd voldoende duidelijk dat NCSC selecteert. | Zoals bij knelpunt 2a aangegeven, kan het NCSC niet alle aan haar verstrekte informatie verwerken. Dit is echter niet voor alle melders duidelijk. |
| **3c** | Feedback loop niet gesloten | Het NCSC geeft melders geen feedback over welk gedeelte van de informatie zij wel en welk deel van de informatie zij niet kan verwerken. Dit is deels te verklaren vanwege de achterban van het NCSC, namelijk Rijk en vitaal. Door het geven van deze feedback zou het NCSC impliciet verraden in welke systemen van de rijksoverheid en vitale sectoren problemen zitten.<br>Hiermee wordt een melder dus opgezadeld met een probleem. Hij weet nu immers niet of zijn melding geheel, gedeeltelijk of helemaal niet door het NCSC wordt opgepakt. |
| **3d** | NCSC systemen kunnen overlappende "scopes" (1 IP, N ontvangers) niet aan | In de beoogde opzet van het Landelijke Dekkend Stelsel (LDS) is het onvermijdelijk dat meerdere partijen claimen dat een IP-adres bij hen hoort. Laten we het voorbeeld nemen waarin een logistiek bedrijf een stukje IT dienstverlening heeft uitbesteed aan een IT-dienstverlener, die deze dienstverlening vervolgens heeft geïmplementeerd in een publieke cloud provider. Zowel de logistieke dienstverlener, als de IT dienstverlener als de cloud provider kunnen het IP-adres claimen.<br>De huidige systemen bij het NCSC gaan uit van een 1-op-1 verband tussen IP-adres en bestemming van het bericht. |
| **Cluster 4: Cybersecurity Bedrijven** | | |
| **4a** | Niet alle cybersecurity bedrijven hebben een warme relatie met het NCSC | Cybersecurity bedrijven hebben een goede informatiepositie en doen ook onderzoek naar bedreigingen en kwetsbaarheden.<br>Voor het melden bestaat geen formeel proces, dit is afhankelijk van persoonlijke relaties. |
| **4b** | Alternatieven onvoldoende bekend | Niet alle Cybersecurity bedrijven zijn bekend met de restricties van het NCSC en alternatieve manieren om informatie op de juiste plek te krijgen. |
| **Cluster 5: Security Researchers (melders)** | | |
| **5a** | Soms mismatch tussen de verwachting van de melder en daadwerkelijke rol van het NCSC. | Binnen de security researchers gemeenschap is niet altijd duidelijk wat ze wel en niet kunnen verwachten van het NCSC. Deze verwachtingen zijn soms onrealistisch hoog, hetzij door te hoge verwachtingen aan de kant van de onderzoekers, hetzij door gebrekkige communicatie over realistische beperkingen aan de kant van het NCSC. |
| **5b** | Researchers zijn niet altijd goede melders | Researchers zijn goed in het vinden van kwetsbaarheden en andere securityproblemen. Het opvolgen van meldingen is een minder sterke kant.<br>Sommige researchers zien in het NCSC een partij om deze taak te “outsourcen”. Soms zijn ze onbekend met de andere partijen zoals Security Meldpunt en (NBIP) Cleannetworks. |

| Nr | Knelpunt | Omschrijving |
|---|---|---|
| **Cluster 6: DIVD/Security Meldpunt/Cleannetworks/AbuseIX** | | |
| **6a** | DIVD/Meldpunt is een vrijwilligersorganisatie met beperkte capaciteit | Tijdens de Citrix crisis heeft het DIVD met haar Security Meldpunt zich opgesteld als een alternatief verspreidingspunt voor vulnerability-notifications omtrent Citrix. Deze werkzaamheden zijn na de Citrix crisis voorgezet.<br>DIVD is echter een vrijwilligersorganisatie met een beperkte capaciteit en budget. Is het wenselijk dat deze taak uitgevoerd wordt door deze vrijwilligersorganisatie? Kan DIVD duurzaam blijven uitvoeren als er meer vraag komt naar hun diensten? |
| **6c** | Cleannetworks/AbuseIX ontvangen niet de “restdata” | Het Cleannetworks initiatief van NBIP en het initiatief AbuseIX hebben sinds medio 2019 de OKTT status. Hoewel beiden samen vrijwel alle IP/AS-houders in Nederland kunnen adresseren (informeren), ontvangen zij, van het NCSC, op dit moment niet zondermeer de “restdata” die bestemd is voor deze partijen. |
| **6d** | Niet alle IP/AS-houders zijn aangesloten op Cleannetworks | Het Cleannetworks initiatief is in wording en kent, op basis van de achterban van de NBIP, op dit moment 160 deelnemers. Nog niet alle AS/IP houders hebben zich aangesloten bij de NBIP.Hierdoor is het bereik nog niet dekkend.<br><br>Daarnaast speelt hier ook dat meerdere partijen de abuse informatie voor een IP willen ontvangen (zie punt 3d). Cleannetworks laat op basis van de autorisatie door de houder van de IP-registratie wel toe dat meerdere (tegelijk) partijen kunnen worden geïnformeerd over abuse voor een IP/AS. |
| **6e** | Wat nu naar AbuseIX en wat naar CleanNetworks? | AbuseIX richt zich op de access providers en Cleannetworks op hosting providers. Het is voor een melder niet altijd duidelijk of een IP adres bij een provider hoort die aan hosting doet, access verleent of beiden doet. |
| **Cluster 7: Shadow server** | | |
| **7a** | Voortbestaan van ShadowServer staat op de tocht | Het ShadowServer project[1] is ongelofelijk belangrijk als het gaat om *misconfiguration notifications* en bepaalde *vulnerability notifications*. Door omstandigheden wordt het voortbestaan van ShadowServer op dit moment bedreigd. Zie: https://www.shadowserver.org/news/saving-shadowserver-and-securing-the-internet-why-you-should-care-how-you-can-help/ |
| **7b** | Feeds voor ASen zijn beschikbaar, maar niet iedereen krijgt hiervoor de Shadowserver informatie | ShadowServer verstrekt zijn informatie aan iedereen die er om vraagt en kan bewijzen dat hij houder is van de IP-adressen. De meeste netwerk beheerders hebben dan ook een ShadowServer abonnement, maar zeker niet iedereen.<br>Daarbij zijn er onbewust onbekwame partijen die het aan kennis ontbreekt en partijen die deze informatie bewust niet willen verwerken. Bullet proof hosters vallen in deze laatste categorie. |
| **7c** | Deze "country-feed" is exclusief voor nationale CERTs | ShadowServer heeft exclusieve dienstverlening voor “National CSIRTS”[2]. Deze dienstverlening bevat o.a. de zogenaamde “landen feed”, een informatiestroom met alle door ShadowServer gedetecteerde kwetsbare en verkeerd geconfigureerde systemen in een land.<br>Op dit moment is het NCSC de enige partij in Nederland die deze feed kan ontvangen. NCSC kan deze feed slechts beperkt doordelen. |

[1] Zie https://www.shadowserver.org/who-we-are/
[2] Zie https://www.shadowserver.org/who-we-serve/national-csirts/

| Nr | Knelpunt | Omschrijving |
|---|---|---|
| **Cluster 8: Cloud providers** | | |
| **8a** | Rol hyperscalers niet duidelijk | Steeds meer IT-functionaliteit gaat naar “de cloud”. De rol van de grote cloud providers (hyper-scalers) in deze Metro kaart is echter onvoldoende duidelijk. Hoe kunnen bv. de klanten van deze hyper-scalers bereikt worden? |
| **8b** | Relatie shadowserver / hyperscalers onduidelijk | Worden berichten over kwetsbare systemen in de cloud, die van ShadowServer naar de hyper-scalers gestuurd worden, ook doorgestuurd naar de klanten van de hyper-scalers? |
| **8c** | Exclusieve feed naar landen CERTs | De hyper-scalers hebben, door o.a. hun schaal, een uniek inzicht in de veiligheid van het internet. Een gedeelte van deze informatie, bv. van Microsoft over spammende systemen, is beschikbaar voor nationale CERTS. In Nederland is deze informatie exclusief beschikbaar voor het NCSC, maar net als bij 7c is doordelen van deze informatie momenteel niet geheel mogelijk. |
| **8d** | CSIRT-DSP | De cloud providers vallen onder de digitale services providers (DSPs). Voor DSPs geldt, net als voor andere sectoren, vanuit de WBNI een meld- en zorgplicht en het CSIRT-DSP is voor deze sector het nationale cert. Daar waar in andere sectoren “meld- en zorgplichtigen”via een ministeriele aanwijzing worden aangewezen, geldt dat niet voor de DSPs. Of een bedrijf aan de wettelijke definitie van een DSP voldoet is open voor interpretatie. Deze onduidelijkheid heeft een negatieve impact op de informatie-uitwisseling. |
| **Cluster 9: Landen CERTs/CISRTs community** | | |
| **9a** | Niet alle internationale kruisverbanden NCSC wettelijk afgedekt | Het NCSC vertegenwoordigt Nederland (formeel en informeel) in de internationale community van nationale CERTs. De beperkingen die gelden voor het nationaal uitwisselen van informatie (IP-adressen) gelden ook voor het internationaal uitwisselen van informatie. Voor de landen die deelnemen aan het CSIRT-netwerk, is dit afgedekt in de WBNI, maar niet voor andere landen. Hierdoor kan het NCSC in deze community wel veel ontvangen, maar niet veel zenden. |
| **Cluster 10: het Digital Trust Center (DTC)** | | |
| **10a** | DTC is niet ingericht om het “NCSC voor de rest” te zijn | Het DTC is nadrukkelijk opgezet om de cyberweerbaarheid van bedrijven te verhogen. Hiermee zou het DTC die bedrijven die niet in de vitale sector vallen, en dus niet tot de achterban van het NCSC behoren, van informatie kunnen voorzien.<br>Het DTC is echter in alle opzichten kleiner dan het NCSC, er werken minder mensen, er is minder kennis voorhanden en minder budget om een grotere doelgroep te bedienen. |
| **10b** | DTC is (nog) geen OKTT | Het DTC heeft geen status binnen het LDS (landelijk dekkend stelsel), hetzij OKTT of anders. Deze status is rand voorwaardelijk voor het uitwisselen van misconfiguratie-, kwetsbaarheids- of hack-notificaties tussen het NCSC en het DTC. |
| **10c** | Wettelijke grondslag voor het delen van persoonsgegevens door DTC is niet geregeld | Binnen de WBNI of andere wetten is op dit moment geen grondslag voor het DTC op persoonsgegevens te verwerken.<br>Deze grondslag is noodzakelijk om misconfiguratie-, kwetsbaarheids- of hack-notificaties te ontvangen, verwerken en door te delen. |
| **10d** | Moeilijk voor DTC om achterban aan te geven | Het NCSC stuurt, met het oog op de wbni en AVG, alleen berichten met IP adressen naar LDS deelnemers als deze kunnen aangeven wie hun achterban is en welke IP-adressen daartoe behoren. Hiermee wordt het DTC voor een enorm probleem gesteld, zij zal namelijk met ieder bedrijf wat zij vertegenwoordigt een relatie aan moeten gaan en vervolgens moeten identificeren van welke IP-adressen deze organisaties allemaal gebruik maken, inclusief een proces om deze informatie actueel te houden. |
| **Cluster 11: Het OKTT netwerk** | | |

| Nr | Knelpunt | Omschrijving |
|---|---|---|
| **11a** | Hoe kan een OKTT scope van hun achterban bijhouden? | Voor ieder (beoogd) OKTT bestaat de voorwaarde dat er een overeenkomst is met hun doelgroep wat een enorme klus is, zie knelpunt 10c (geldt ook voor de “restdata”, zie 2a). Hierdoor wordt een groot netwerk van allerlei OKTTs een zeer grote taak gegeven. |
| **11b** | Theoretische structuur LDS sluit niet aan bij de werkelijkheid van het internet. IP-adressen horen niet bij één organisatie / OKTT / groep | Parallel aan punt 3d. Het LDS lijkt gebaseerd op de aanname dat één IP-adres maar bij één OKTT hoort. Niets staat organisaties echter in de weg zich bij meerdere OKTTs aan te melden. En kan (o.a. door leverancier/klant relaties) een IP-adres bij meerdere partijen horen. |
| **11c** | Feedback loop niet gesloten | In het LDS is geen rekening gehouden met een feedback loop. Hierdoor is niet duidelijk hoe landelijk dekkend het stelsel daadwerkelijk is. |
| **Cluster 12: Netwerk van CERTs** | | |
| **12a** | NCSC beperkt de informatie die zij CERTs stuurt strikt tot de doelgroep van het CERT. Hierdoor is het bestaande CERT netwerk buitenspel gezet. | Dit punt is vergelijkbaar met knelpunt 10c en 11a. CERTS zijn in de regel aardig in staat hun achterban te definiëren. Binnen het LDS zijn slechts een beperkt aantal CERTs aangewezen die alleen informatie krijgen voor hun eigen achterban.<br>De CERTs in Nederland (en wereldwijd) hebben echter al een bestaand netwerk (op de kaart AS-net genoemd). De CERTs zouden in de basis de rest van Nederland kunnen informeren, maar door de beperking van de informatie vanuit het NCSC kunnen zij dit netwerk niet voeden vanuit deze bron. |
| **12b** | Scope van een "branch" is (vaak) lastig te bepalen (IPs / ASen / domeinen) | Traditioneel zijn (netwerk-)CERTs georganiseerd rond een of meerdere AS-en. Binnen het LDS ontstaan nu ook sector CERTs zoals Z-CERT. Deze hebben (analoog met knelpunt 10c en 11a) een behoorlijke taak aan het inventariseren en accuraat houden van de IP-adressen en domeinen van hun achterban. |
| **12c** | Scope van een "branche" is (vaak) niet beperkt tot Nederland | Branches houden zich niet aan landsgrenzen. |
| **Cluster 13: Niet vitaal bedrijfsleven** | | |
| **13a** | Oneerlijke voorsprong vitaal | Het niet-vitaal bedrijfsleven voelt zich in de informatiepositie behoorlijk achtergesteld t.o.v. die bedrijven die (toevallig) wel vitaal zijn. |
| **13b** | Uitlegbaarheid scheiding vitaal/niet-vitaal | De scheiding tussen vitaal en niet-vitaal is steeds moeilijker uitlegbaar door keten-afhankelijkheden. Bedrijven met een groot (vitaal?) economisch belang zijn nu niet als vitaal aangemerkt. |
| **13c** | Verantwoordelijkheid bedrijf/consument niet altijd duidelijk | Het is onvoldoende duidelijk welke verantwoordelijkheden een bedrijf heeft ten opzichte van zijn klanten als de issue zich binnen het verantwoordelijkheidsgebied van de klant bevindt. |
| **Cluster 14: Klanten in hosting** | | |
| **14a** | Complexe keten | Hosting bedrijven hebben vaak te maken met klanten van klanten van klanten. B.v. een bedrijf huurt rack-ruimte en IP-adressen bij een hoster en levert daar zelf weer managed services op aan een bedrijf wat weer eindklanten heeft. |
| **Cluster 15: Eindklanten/systeem beheerders** | | |
| **15a** | Niet iedere ontvanger heeft de capaciteit om "iets" met een melding te doen | Hoewel er heel veel bekwame partijen zijn met goede intenties heeft niet ieder bedrijf de competenties in huis om de melding goed op te volgen. |
| **Cluster 16: Consumenten** | | |
| **16a** | Niet iedere ontvanger heeft de capaciteit om "iets" met een melding te doen | Veel consumenten hebben niet de kennis om meldingen op te lossen. |
| **Cluster 17: ISPs** | | |
| **17a** | Verantwoordelijkheden ISP t.o.v. consument niet duidelijk | In welke mate is de ISP verantwoordelijk om meldingen door te zetten naar de consument? |

| Nr | Knelpunt | Omschrijving |
|---|---|---|
| | | **Cluster 18: Politie** |
| **18a** | Mismatch tussen aandacht en capaciteit voor slachtoffernotificatie | De politie heeft de wettelijke taak om zorg te dragen voor slachtoffers. Door (onbewuste) slachtoffers van cybercrime te notificeren, wordt herhaald slachtofferschap voorkomen. Hier is steeds meer aandacht voor, maar de capaciteit is hiervoor niet altijd beschikbaar. |
| | | **Cluster 19: AS / IP houders** |
| **19a** | Bullet proof holsting | Er zijn AS / IP houders die bewust niet reageren op abuse meldingen van welke soort dan ook. |
| **19b** | Niet iedereen is goed bereikbaar | Niet alle AS / IP houders zijn goed bereikbaar voor de kanalen die daarvoor zijn. Dit komt door problemen in de registratie, maar ook doordat sommige organisaties niet bekwaam zijn om deze meldingen af te vangen. |

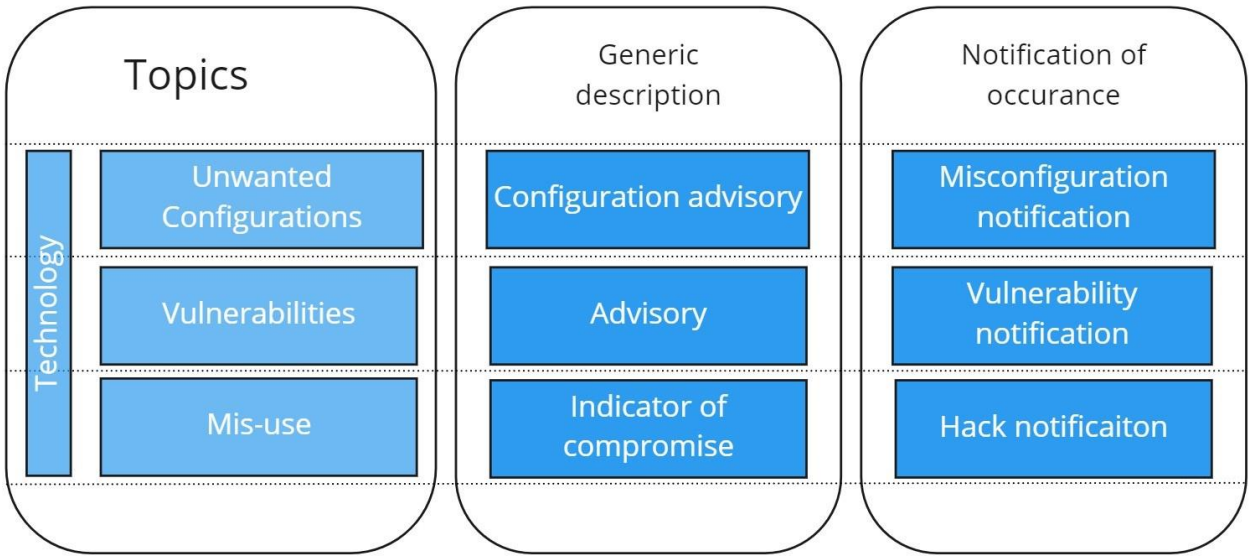
# Nadere toelichting op De Metrokaart

Hoewel De Metrokaart een versimpeling is van de werkelijkheid, geeft ze nog steeds een complex beeld van een complexe situatie.

## Taxonomie

De Metrokaart richt zich alleen op technisch misbruik van de internet infrastructuur, onrechtmatige content of datalekken worden niet behandeld.

In deze Metrokaart hebben we advisories buiten beschouwing gelaten. Een advisory is een niet algemene  melding van het bestaan van een kwetsbaarheid, ongewenste configuratie en/of een methode van misbruik van systemen, dat geen IP adres, url of andere specifieke duiding van het betreffende systeem bevat. Het advisory proces wordt door de leden van AAN als relatief soepel ervaren. De metrokaart richt zich op notificaties, mededelingen over het specifiek voorkomen van ongewenste configuraties, kwetsbaarheden en/of daadwerkelijk misbruik.




Deze taxonomie is verder uitgebreid terug te lezen via [https://www.abuse.nl/publicaties/taxonomie-techniek.html](https://www.abuse.nl/publicaties/taxonomie-techniek.html)

## Zones

De Metrokaart is onderverdeeld in drie zones:

1. Generatie
2. Distributie
3. Resolutie

In het proces is het doel om informatie zo effectief mogelijk van de plek waar zij ontstaat in zone 1 naar dat station in zone 3 te krijgen dat er daadwerkelijk iets aan kan doen. De partijen in zone 2 dienen hierbij als tussenstations.

## Stations

Stations zijn in De Metrokaart aangegeven als gekleurde vierkanten. Ieder vierkant heeft een naam en één of meerdere rollen. Deze rollen variëren tussen:

- Melder (groen), een partij die risico's detecteert en deze als notificaties aanbiedt aan de andere partijen in het stelsel.
- Doordeler (geel), een partij die notificaties ontvangt en deze, eventueel na verrijking, ontdubbeling en/of bundeling doorstuurt naar andere ontvangers of andere doordelers.
- Ontvanger (blauw), een partij die notificaties ontvangt en in staat is of zou moeten zijn om met deze informatie de risico's te verminderen, weg te nemen of doelbewust te accepteren.
- Verrijker, een partij die notificaties en andere informatie ontvangt en verwerkt tot een andere type informatie. Een bekend voorbeeld hiervan is het NCSC dat ieder jaar, samen met het NCTV, op deze manier het Cyber Security Beeld Nederland (CSBN) samenstelt.

## Rivieren

Op de kaart staan twee rivieren die duidelijke barrières zijn in het proces. Het oversteken van de rivier "Internationaal" zorgt voor belemmeringen aangezien er naast de Nederlandse wet- en regelgeving nu ook rekening gehouden moet worden met buitenlandse wet- en regelgeving. Daarnaast is het binnenland verdeeld door de rivier "Rijk en vitaal". Deze rivier scheidt de Rijksoverheid en vitale sectoren van de rest van het binnenland. Informatie die via het station NCSC reist kan deze rivier slechts onder bepaalde condities oversteken.

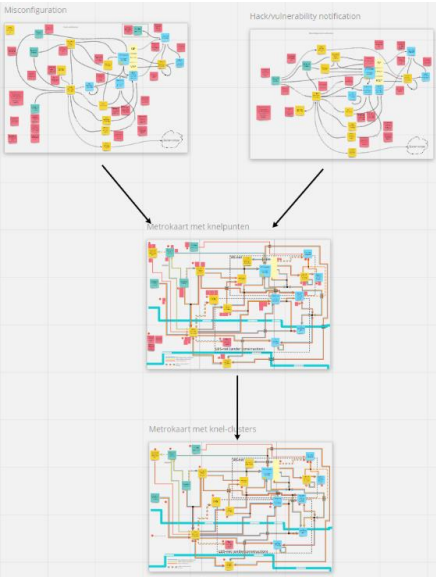
## Netten

Op De Metrokaart zijn twee aparte "netten" omkaderd, het "AS-net" en "LDS-net". AS-en is een reeds bestaand, oud stelsel van afspraken tussen partijen die een zelfstandige IP-adresreeks op het internet beheren. Zo'n IP-adresreeks wordt in jargon ook wel een AS, of Autonomous System genoemd.

Het nieuwe "LDS-net" is een nieuw stelsel van afspraken tussen partijen. LDS staat voor Landelijk Dekkend Stelsel, er wordt hard gewerkt om dit stelsel inderdaad landelijk dekkend te maken, maar dit is nog niet gelukt.

## Knelpunt-clusters

De rode bolletjes met nummers geven gebieden op De Metrokaart waar zich één of meerdere knelpunten bevinden. Deze zijn in de knelpuntenlijst verder uitgewerkt.




## Onderzoeksmethode

De Metrokaart is in een aantal verschillende ronden, met de inbreng van zoveel mogelijk partijen, samengesteld. Na het bepalen van de taxonomie is er eerst, met behulp van een online whiteboard, een diagram opgesteld waarin de informatiestromen en knelpunten rond misconfiguratie-notificaties in kaart zijn gebracht. Daarna heeft een soortgelijke sessie plaats gevonden voor kwetsbaarheids-notificaties en hack-notificaties. Deze twee diagrammen bleken dusdanig veel overlap te hebben dat zij geconsolideerd zijn in één enkele metrokaart. Als laatste zijn de genoteerde knelpunten ontdubbeld en geclusterd.

Alle tussentijdse producten zijn steeds ter review aan het brede AAN netwerk aangeboden.

Dit document is inmiddels de tweede iteratie van dit document. De eerdere versie is te vinden op: https://www.abuse.nl/publicaties/metrokaart-oktober-2020.html.

In deze versie hebben wij de feedback die we op de vorige iteratie hebben ontvangen verwerkt.

## Hoe nu verder…

Zoals we hierboven schreven hebben we bij het samenstellen van De Metrokaart ook diverse knelpunten geïdentificeerd en deze knelpunten geclusterd. Voorlopig gaat het om een kleine veertig knelpunten in achttien clusters.

In de komende weken willen we samen met de betrokken partijen deze knelpunten zo scherp mogelijk in beeld krijgen, om zo tot een startpunt te komen voor mogelijke oplossingen.

## Met medewerking van

Het Anti Abuse Netwerk is een samenwerkingsverband tussen internetproviders, brancheorganisaties, IT-dienstverleners, datacenters, belangenorganisaties en de overheid. De personen en organisaties achter het Anti Abuse Netwerk werken dagelijks aan een veilige en betrouwbare ICT-infrastructuur voor alle Nederlanders. Ze zijn trots op de netwerken die voor iedereen het internet toegankelijk maakt.

De Metrokaart kwam tot stand met medewerking van de volgende partijen.

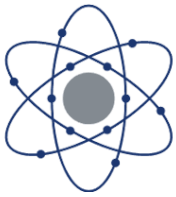
A2B Internet

AbuseIX

AbuseIO

AMS-IX – Amsterdam Internet Exchange

Atom86



Connect2Trust

Cyberveilig Nederland

Deloitte

DHPA – Dutch Hosting Provider Association

Stichting Digitale Infrastructuur Nederland (DINL)

DIVD – Dutch Institute for Vulnerability Disclosure

Digital Trust Center (DTC)

ECP Platform voor de Informatie-samenleving

Expertisecentrum Online Kindermisbruik

Ministerie van Economische Zaken en Klimaat

ISPConnect

NBIP (Nationale Beheersorganisatie Internet Providers)

NLconnect

NLdigital

Privacy Management Partners

Politie

RIPE NCC

Scamadviser.com

Schuberg Philis

SIDN

TU Delft

Vereniging van Registrars