Metrokaart Abuse Informatie – 10-2020

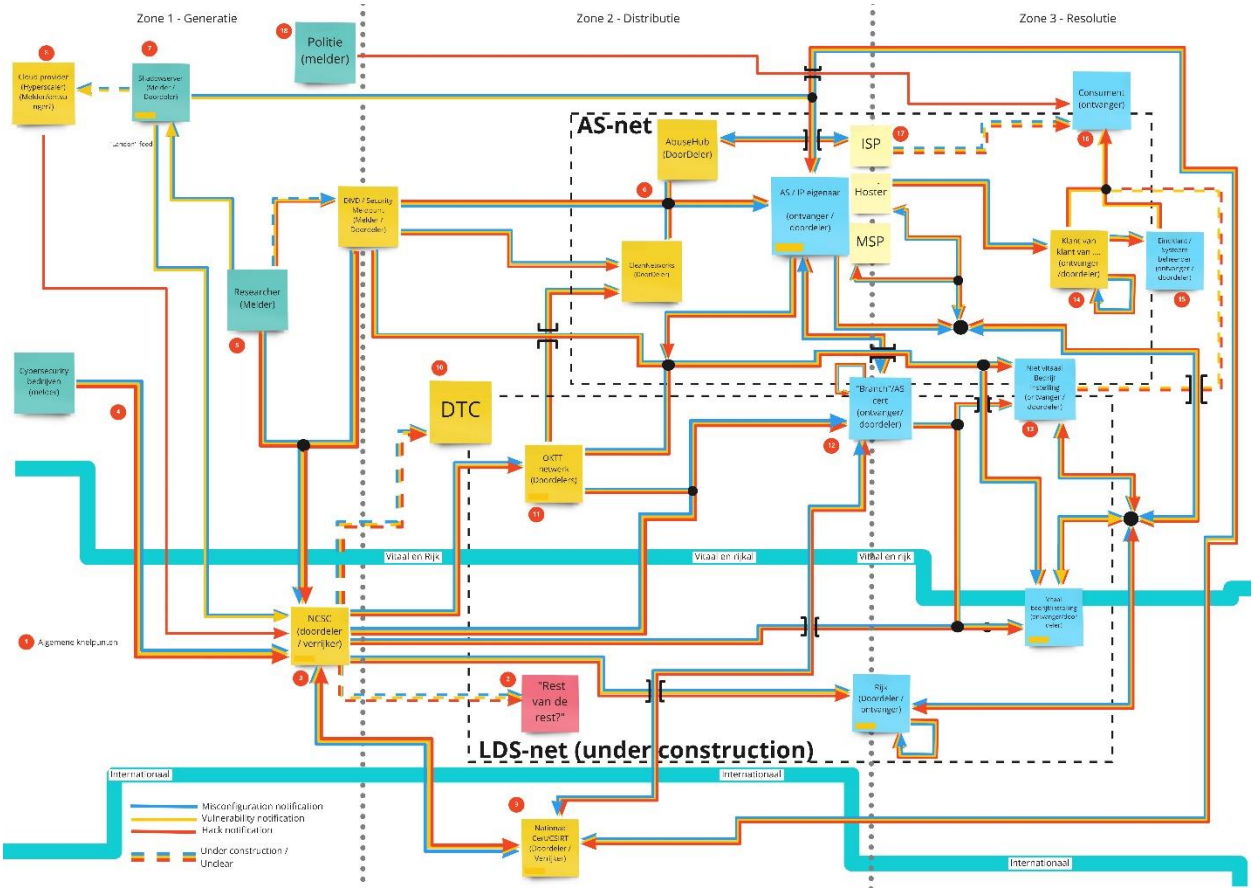
Voor u ligt **De Metrokaart van Abuse gerelateerde informatie**. Deze kaart is samengesteld door de leden van het Anti Abuse Netwerk (AAN) dat zich ten doel stelt het Nederlandse internet veiliger te maken door ervoor te zorgen dat informatie over onveilige configuraties, kwetsbaarheden en misbruik terecht 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 een dynamisch document, wij realiseren ons dat we misschien niet volledig zijn en nodigen eenieder uit om onze kennis aan te vullen. 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_kiUF4aY=/

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, met als achterban het niet-vitale bedrijfsleven, wordt vaak nadrukkelijk naar voren geschoven, als het tussenstation “voor de rest”. Het is, voor abuse informatie, nog niet aangesloten op het LDS informatie en is druk doende met de inrichting van haar organisatie voor deze taak.
6) Aan veel van deze genoemde knelpunten ligt de “status” van een IP -adres als persoonsgegeven ten grondslag.

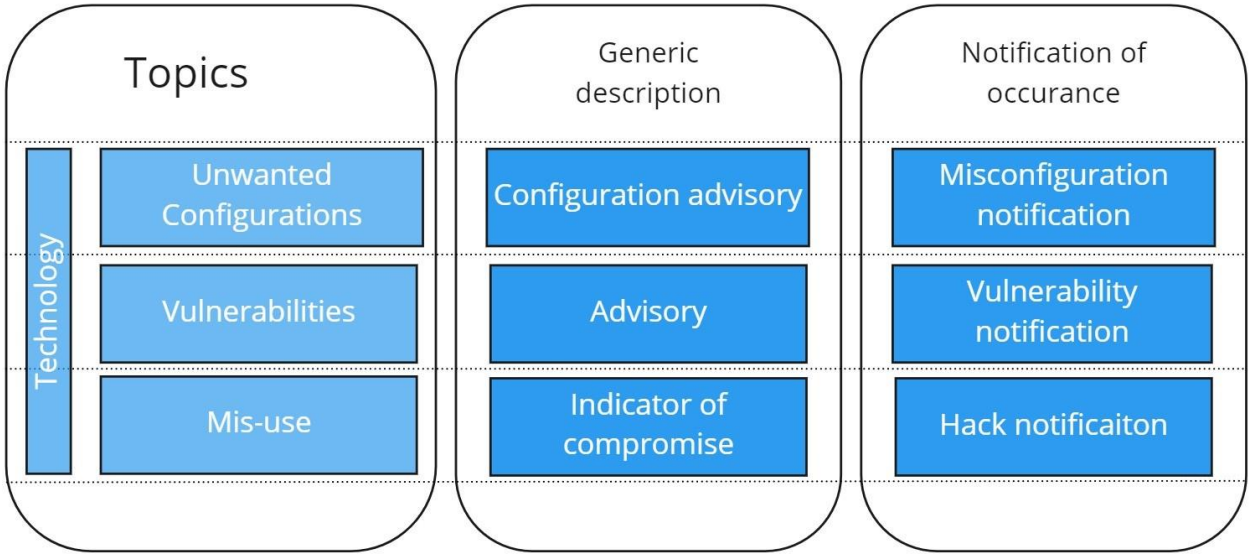
Nadere toelichting op De Metrokaart

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 meldingen 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

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

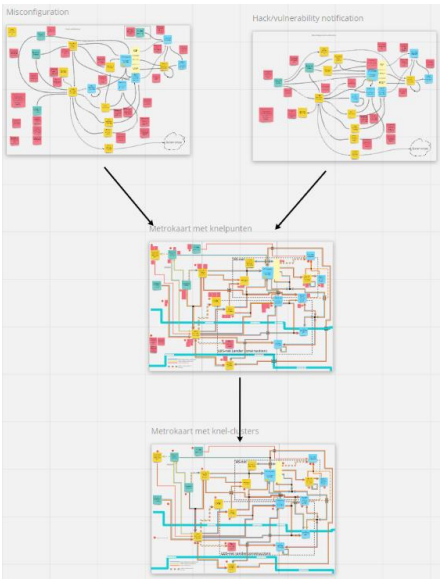
Op De Metrokaart zijn twee aparte "netten" omkaderd, het "AS-net" en "LDS-net". AS-net is een reeds bestaand, oud stelsel van afspraken tussen partijen die een zelfstandige IP-adresreeks op het internet beheren. Zo'n IP-adresreeks wordt in jargon ook wel een AS, of Autonomous System genoemd.

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.

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.

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. We zijn voornemens dit overzicht op 1 december a.s. publiceren en opnieuw een beroep doen op u om mee te denken.

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.

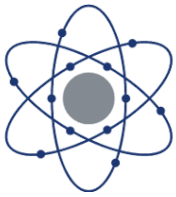
A2B Internet

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