LIA verwerken abuse informatie

Legitimate Interest Assessment

21 april 2021

Versie 1.1

LIA verwerken abuse informatie

Legitimate Interest Assessment

Opdrachtgever
Anti Abuse Netwerk
ECP

Auteurs
drs. Joris Hutter CIPP/E CIPM CIPT
drs. mr. Jeroen Terstegge CIPP/E

21 april 2021

Inhoud

Management samenvatting

Waarom

Het Anti Abuse Netwerk (www.abuse.nl) is een samenwerking van partijen in de aanpak van abuse. Doelstelling van AAN is het verbeteren van de samenwerking tussen bedrijfsleven, overheid, non-profitsector en de wetenschap op het slimmer organiseren van de informatiedeling op abuse. Abuse is het misbruik maken van internetvoorzieningen. Door de eindgebruiker, systeemeigenaar of een handelingsbekwame partij te informeren over een gesignaleerde abuse, kan deze de abuse beëindigen. Hiermee wordt zowel de systeemcomponent van de eindgebruiker veiliger als het internetgebruik als geheel en daarmee de veiligheid van andere internetgebruikers..

Vraagstelling

Abuse informatie kan als persoonsgegeven worden opgevat. Eén van de vraagstukken bij het verwerken en delen van abuse informatie is hoe dit zich verhoudt tot de Algemene Verordening Gegevensverwerking (AVG). De vraag in dit onderzoek is wat de mogelijkheden zijn om in het particuliere domein abuse informatie te ontvangen, te veredelen en te delen op basis van gerechtvaardigd belang. Dit onderzoek wordt uitgevoerd middels een Legitimate Interest Assessment (LIA).

Scope

Wat wordt in dit onderzoek als abuse beschouwd? De AAN-partijen werken op dit moment aan de aanpak van zogenoemde abuse van technologie. Deze bestaat uit:

1. Ongewenste configuraties, waardoor het voor een kwaadwillende mogelijk is een systeem te misbruiken.
2. Kwetsbaarheden van een systeem waardoor een kwaadwillende misbruik kan maken door het iets anders te laten doen dan waarvoor het origineel bedoeld was.
3. Ongewenst gebruik waarbij een systeem wordt gebruikt voor het uitvoeren van activiteiten die ongewenst of zelfs illegaal zijn.

In deze situaties wordt de eindgebruiker, c.q. systeemeigenaar of beheerder van het systeem geïnformeerd op de abuse, waarna deze de abuse kan beëindigen.

Buiten scope

Wat valt buiten scope van dit onderzoek? Onder abuse kan ook ongewenste content (bijvoorbeeld kinderporno) of het lekken van persoonsgegevens worden verstaan. Dit wordt (nog) niet door AAN-partijen aangepakt en vergt in relatie tot de AVG andere afwegingskaders.
Ook zijn er partijen die informatie met elkaar delen aangaande 'bedreigende' IP-adressen. Hierdoor kan een systeemeigenaar of een beheerder het systeem beveiligen tegen dit IP-adres en onderzoeken of vanuit dit IP-adres al kwaad is geschied.
Abuse informatie die zich kwalificeert als strafrechtelijke gegevens ligt niet in de scope van dit onderzoek. Een signaal dat iemand slachtoffer is van een strafbaar feit is overigens geen strafrechtelijk gegeven met betrekking tot het slachtoffer. Er is sprake van een strafrechtelijk gegeven als er een herleidbaarheid is tot de plegers van het strafbare feit. Als dit type informatie, dus met mogelijke herleidbaarheid tot de plegers, in de toekomst wel in scope komt van de abuse meldingen, dan dient er een nieuwe afweging plaats te vinden.

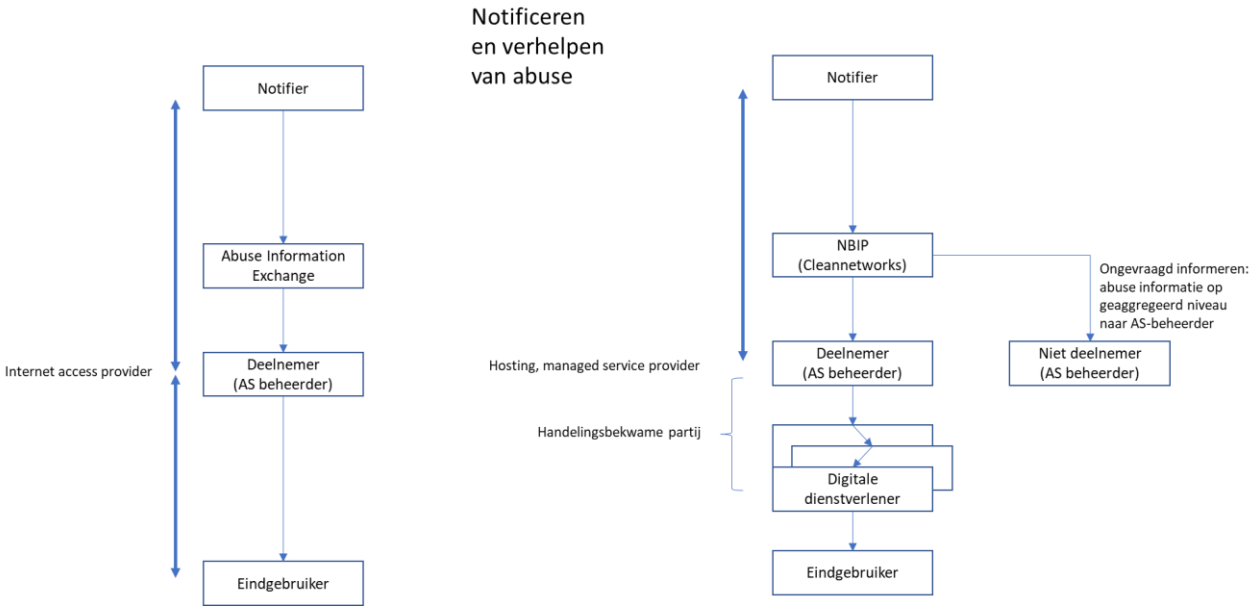
Processen

Er zijn in hoofdlijnen drie processen:

1. Ontvangen van bulk abuse-signalen door een centraal meldpunt vanuit vertrouwde notifiers. Bij dit meldpunt zijn partijen aangesloten met een onafhankelijk netwerk met eigen verbindingen naar het internet. Een aangesloten partij is een 'AS-beheerder' en beheert AS-blokken met IP-nummers. Het centraal meldpunt ontdubbelt de ontvangen meldingen en

splitst deze op en verstrekt deze naar de aangesloten deelnemers. In de context van dit onderzoek zijn er twee centrale meldpunten.
Voor internet access providers is dat meldpunt het Abuse Information Exchange. De deelnemers van het Abuse Information Exchange hebben een directe klantrelatie met de eindgebruiker en informeren de betreffende eindgebruiker dat deze abuse heeft. Dit kan een zakelijke eindgebruiker of een consument zijn.
Hosting, managed service providers en andere digitale dienstverleners met een eigen aansluiting op het internet (AS-beheerder) zijn aangesloten op het meldpunt CleanNetworks van NBIP. Deze bij CleanNetworks deelnemende partijen hebben meestal geen directe klantrelatie met de eindgebruiker, maar leveren diensten aan digitale dienstverleners die blokken van IP-adressen 'huren' van de AS-beheerder. Ook kan deze 'huurder' weer diensten leveren aan andere digitale dienstverleners die IP-adressen huren van deze huurder. De abuse kan de zakelijke of consument eindgebruiker treffen, maar kan ook op een systeemcomponent van een digitale dienstverlener plaatsvinden. De abuse meldingen worden in het domein van de deelnemer van het meldpunt opgesplitst en doorgestuurd naar een 'handelingsbekwame partij' die de technische en organisatorische mogelijkheden heeft om de abuse te beëindigen.

2. Het centrale meldpunt verstrekt op geaggregeerd niveau aan een niet-deelnemer dat deze abuse heeft in diens domein. Dit wordt ongevraagd informeren genoemd. Deze partij wordt daarmee bewust van de abuse en kan daarop actie ondernemen. Ook ontstaat hiermee benchmark informatie waardoor het voor de markt duidelijker wordt hoe AS-beheerders presteren op de aanpak van abuse in het eigen domein.
3. Het actief scannen van Nederlandse IP-adressen op een bepaald type kwetsbaarheid of misconfiguratie en de betreffende eindgebruiker/systeemeigenaar hierop informeren. Deze kan daarop die abuse beëindigen. Dit proces wordt uitgevoerd door DIVD.



Conclusies

1. Voor zover de abuse informatie kwalificeert als persoonsgegevens (wat meestal niet het geval is), kan de informatie worden verwerkt op grond van artikel 6(1)(f) AVG (gerechtvaardigd belang). Een voorwaarde hiervoor is dat deze informatie wordt uitgesplitst naar de partij die de abuse kan verhelpen en dat deze zich netjes aan de basisvoorwaarden van de AVG houdt.

2. Deze conclusie geldt niet als de abuse informatie kwalificeert als strafrechtelijke gegevens over daders (out-of-scope van dit rapport). Indien dit soort informatie in de toekomst in de scope komt, dient een nieuwe afweging gemaakt te worden. Zo is bijvoorbeeld het verwerken van strafrechtelijke gegevens als dienstverlening aan derden niet toegestaan zonder vergunning op grond van de Wet op de particuliere beveiligingsorganisaties en recherchebureaus. Bij gebrek daaraan is een vergunning van de Autoriteit Persoonsgegevens (AP) vereist (art. 33 lid 4 UAVG). Het is wél toegestaan om strafrechtelijke gegevens te verwerken om je eigen belangen of dat van je personeel te beschermen (art. 33 lid 2 UAVG). Als abuse-informatie die kwalificeert als strafrechtelijke persoonsgegevens in de toekomst wél in scope komt van de activiteiten van AAN, dan adviseren wij een wetswijziging in art. 33 UAVG op dit punt.

3. Geaggregeerde informatie is -mits de groepsgrootte groot genoeg is- geen persoonsgegeven. Het verstrekken van geaggregeerde abuse informatie aan niet-aangesloten partijen valt dan ook niet onder de AVG, zodat er vanuit dat punt geen belemmeringen zijn om het te doen.

1 Inleiding

Het Anti Abuse Netwerk (www.abuse.nl) is een samenwerking van partijen in de aanpak van abuse. De doelstelling van AAN is het verbeteren van de samenwerking tussen bedrijfsleven, overheid, non-profitsector en de wetenschap op het slimmer organiseren van de informatiedeling op abuse. Abuse is het misbruik maken van internetvoorzieningen. Door de eindgebruiker, systeemeigenaar of een handelingsbekwame partij te informeren over een gesignaleerde abuse, kan deze de abuse beëindigen. Hiermee wordt zowel de systeemcomponent van de eindgebruiker veiliger alsmede het internet en de veiligheid van anderen.

Vraagstelling

Abuse informatie kan als persoonsgegevens worden opgevat. Eén van de vraagstukken bij het verwerken en delen van abuse informatie is hoe dit zich verhoudt tot de Algemene Verordening Gegevensverwerking (AVG). De vraag in dit onderzoek is wat de mogelijkheden zijn om in het particuliere domein abuse informatie te ontvangen, te veredelen en te delen op basis van gerechtvaardigd belang. Dit onderzoek wordt uitgevoerd middels een Legitimate Interest Assessment (LIA).

Daarbij gaat het in bijzonder om:

- Het verwerken van bulkinformatie
- Niet alleen gevraagd, maar ook ongevraagd informeren
- De (keten)processen van NBIP, Abuse Information Exchange, Cyberveilig Nederland, Connect2Trust en DIVD

Opbouw van rapport

De LIA heeft de volgende opbouw:

A. Beschrijving kenmerken van de gegevensverwerking
B. Juridische beoordeling en conclusie

De beoordeling is uitgevoerd conform de beoordelingsaanpak vanuit advies 217 van de European Data Protection Board.

2 Voorstel

2.1 Anti Abuse Netwerk (AAN)

Het Anti Abuse Netwerk (www.abuse.nl) is een samenwerking van partijen in de aanpak van abuse. De doelstelling van AAN is het verbeteren van de samenwerking tussen bedrijfsleven, overheid, non-profitsector en de wetenschap omwille van het slimmer organiseren van de informatiedeling bij abuse. Dit komt naar voren in het manifest van AAN.

> *"Veel ondernemers, onderzoekers, (non-profit) dienstverleners en overheidsfunctionarissen zijn actief betrokken bij het digitale fundament van de Nederlandse economie. Daarbij wordt gewerkt aan een veilige en betrouwbare online infrastructuur voor alle Nederlanders. Ook in tijden van crisis zoals tijdens de COVID-19-pandemie blijkt hoe stabiel onze digitale infrastructuur is.*
>
> *Toch zijn we er nog niet in Nederland. Risico's voor de digitale weerbaarheid kunnen niet alleen met preventieve maatregelen worden weggenomen. Het gericht informeren van organisaties en consumenten over wat er bij hen mis is, is essentieel om de weerbaarheid verder te verbeteren. Denk aan: informatie over misbruik van online faciliteiten, over online criminaliteit of kwetsbaarheden. Deze informatie komt nu vaak niet terecht bij de partijen die deze onveiligheid het snelst en meest effectief kunnen bestrijden. Als de informatiedeling slimmer georganiseerd wordt kan onze gehele samenleving nog beter weerbaar worden gemaakt maken tegen criminele hackers en statelijke actoren. Om dat te bereiken moet de samenwerking tussen bedrijfsleven, overheid, de non-profitsector en de wetenschap worden verbeterd."*

2.2 Wat te verstaan onder abuse en abuse informatie

Abuse betekent letterlijk vertaald 'misbruik', maar wat wordt bedoeld met de term 'abuse' in de context van AAN, het Anti Abuse Netwerk? [1]
In de context van AAN wordt onder abuse verstaan: alle vormen van misbruik van het internet zoals deze typisch wordt afgehandeld door partijen die internetdiensten leveren. Deze partijen zijn bijvoorbeeld hosters, ISPs en managed service providers. Zij krijgen te maken met veel zaken die typisch in een van de volgende drie gebieden vallen:

1. Abuse van technologie
2. Ongewenste content (bijvoorbeeld kinderporno)
3. Het lekken van persoonsgegevens

Op dit moment richt AAN zich vooral op het verbeteren van de aanpak op de abuse van de technologie.

BUITEN SCOPE: De aanpak op ongewenste content en het lekken van persoonsgegevens.

De abuse van technologie bestaat uit de volgende aspecten:

1. Ongewenste configuraties
   Bij een 'ongewenste configuratie' is het voor een kwaadwillende mogelijk een systeem te misbruiken. Hierbij wordt echter geen misbruik gemaakt van softwarefouten om het systeem

[1] https://www.abuse.nl/publicaties/taxonomie-techniek.html

iets te laten doen waarvoor het niet bedoeld is, maar is het systeem zo ingesteld dat er op een ongewenste manier gebruik van gemaakt kan worden.[2]

2. Kwetsbaarheden
   Als een systeem een kwetsbaarheid bevat, is er meestal sprake van een technische fout, waardoor een kwaadwillende misbruik kan maken van het systeem door het iets anders te laten doen dan waarvoor het origineel bedoeld was. Een kwetsbaarheid in een systeem ontstaat vaak door een fout (bug) in de software of door een verkeerde implementatie van features in de software. Vaak kan de kwetsbaarheid door middel van een patch verholpen worden.[3]
3. Ongewenst gebruik
   Van 'ongewenst gebruik' van een systeem is sprake als een systeem wordt gebruikt voor het uitvoeren van activiteiten die ongewenst of zelfs illegaal zijn. Denk hierbij aan het versturen van spam, uitvoeren van DDoS aanvallen of onderdeel zijn van een botnet. Vaak is 'ongewenst gebruik' het gevolg van misbruik van een systeem via een kwetsbaarheid of een ongewenste configuratie, maar een kwaadwillende kan bijvoorbeeld ook een computer huren bij een hoster en hiermee gaan spammen. In dit geval maakt hij misbruik van een legitieme dienst.

Aspect	*Algemene beschrijving*	*Melding van bestaan*
Ongewenste configuraties	Configuratie advies Algemene beschrijving van een ongewenste configuratie	Misconfiguratie melding Bericht dat een specifiek systeem op een bepaald moment een specifieke ongewenste configuratie bevat
Kwetsbaarheden	Kwetsbaarheid advies Algemene beschrijving van een kwetsbaarheid	Kwetsbaarheid melding Bericht dat een specifiek systeem op een bepaald moment een specifieke kwetsbaarheid bevat
Ongewenst gebruik	Indicator of compromise Algemeen bericht dat beschrijft hoe kan worden vastgesteld dat een systeem op een ongewenste manier gebruikt wordt	Abuse melding Bericht dat op een specifiek systeem op een bepaald moment op een ongewenste manier gebruikt wordt

[2] Een bekend voorbeeld van een ongewenste configuratie is een zogenaamde "Open DNS resolver". Een Open DNS resolver is een DNS server die iedereen op het internet toestaat om een domeinnaam om te zetten in een IP-adres. Op zich is het technisch gezien een valide configuratie waarvoor ook legitieme toepassingen zijn. Zo bieden aanbieders als OpenDNS, CloudFlare, Google, Comodo, Quad9 en Verisign gratis publieke DNS diensten aan die niet mogelijk zouden zijn zonder Open DNS Relay. Het is echter ook mogelijk om deze configuratie te misbruiken voor het uitvoeren van DDoS aanvallen. Door een zogenaamde DNS Amplification Attack uit te voeren kan een kwaadwillende met relatief weinig bandbreedte een systeem overspoelen met verkeer. De Shadow Server Foundation, scant al sinds 2013 op het internet naar ongewenste configuraties. Sinds die tijd is het aantal Open DNS Relays gedaald van ruim bijna 12 miljoen in Juni van 2013 tot bijna 2.5 miljoen in Augustus van 2020.

[3] Een voorbeeld van een kwetsbaarheid was die in het Citrix ADC product van eind 2019 begin 2020. Door een fout in de code van deze software was het voor een aanvaller mogelijk deze systemen over te nemen.

2.3 Scope betreft specifieke meldingen van bestaan van abuse

De scope van de LIA betreft de verwerking van de specifieke melding van het bestaan van abuse op een systeem. Hierbij is die melding gekoppeld aan een IP-adres en daarmee herleidbaar naar de systeemeigenaar.
De scope betreft de verwerking van de volgende type meldingen:

- Misconfiguratie melding
- Kwetsbaarheid melding
- Abuse melding

Een typische melding heeft de volgende opbouw:

- IP-adres
- Datum/tijdstip
- Type melding (type misconfiguratie, type kwetsbaarheid, type abuse)

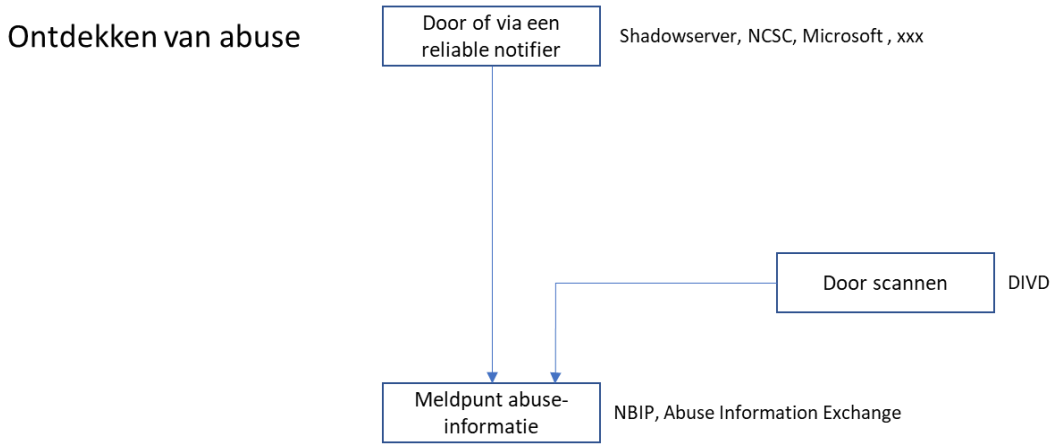
Er zijn ook algemene beschrijvingen van abuse die gedeeld worden in de ketens. Deze zijn niet specifiek herleidbaar naar een systeem of een persoon achter een systeem. De AVG is niet van toepassingen op deze meldingen.

2.4 Meldpunten op abuse informatie en ontdekken van abuse

Er zijn twee meldpunten voor abuse informatie:

- Abuse Information Exchange voor internet toegang dienstverleners.
- NBIP voor hosting bedrijven en andere typen digitale dienstverleners.

De bij deze meldpunten aangesloten partijen hebben een onafhankelijk netwerk dat op het internet is aangesloten. Deze partijen beheren AS-blokken. Een AS-blok bevat IP-reeksen.



Het ontdekken van abuse gebeurt door 'reliable notifiers'. Dat zijn not-profit en commerciële organisaties die het internet scannen. Een belangrijke partij is Shadow Server Foundation, een non-profit organisatie. Dit type partijen verstrekken alleen abuse informatie op IP-reeksen van deelnemers van het meldpunt. Het ontdekken van abuse door notifiers valt buiten scope van het onderzoek.
De meldingen van notifiers kunnen ook via het NCSC verlopen. Het NCSC wordt gezien als een nationaal meldpunt.

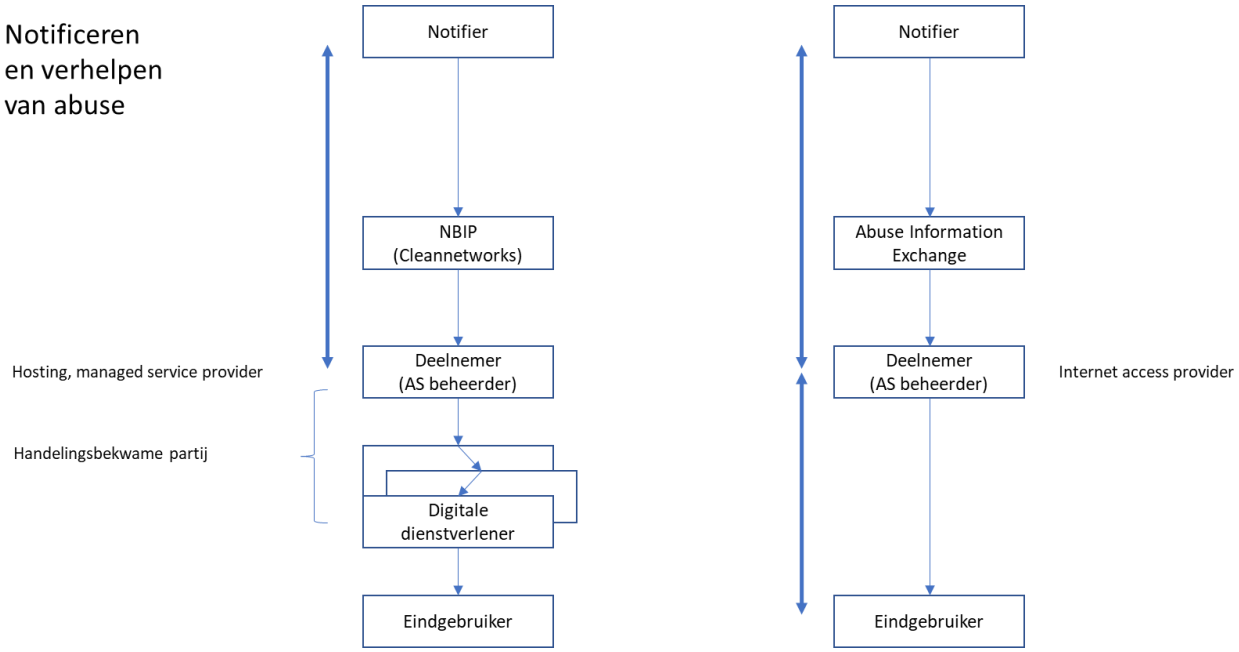
Een andere mogelijkheid is door zelf op kwetsbaarheden of ongewenste configuratie te scannen. Dat gebeurt door DIVD. Dit is in scope van het onderzoek.

2.5 Notificeren, verhelpen van abuse en handelingsbekwame partij

Internet access providers leveren diensten direct aan de eindgebruiker. De Abuse Information Exchange distribueert de meldingen naar de aangesloten leden, waarbij een deelnemer alleen

meldingen ontvangt van de 'eigen IPs'. Iedere deelnemer heeft daarna een eigen proces om meldingen te prioriteren en door te geven aan de eindgebruiker. De eindgebruiker dient de abuse te verhelpen.

Aan het meldpunt van NBIP zijn hosting bedrijven en andere type digitale dienstverleners met een onafhankelijk netwerk aangesloten, echter geen internet toegang providers. NBIP distribueert de meldingen naar deelnemende partijen, waarbij een deelnemer alleen meldingen ontvangt van de 'eigen IPs'. Deze deelnemer levert meestal geen einddienst aan de eindgebruiker, maar diensten aan digitale dienstverleners. Deze kunnen een relatie hebben met de eindgebruiker, maar soms zitten er nog meer schakels van digitale dienstverleners tot de eindgebruiker. Van een deelnemer wordt verwacht dat deze de abuse in de eigen keten aanpakt.
De abuse kan zich op het systeem van de eindgebruiker bevinden, maar ook op één van de systeemcomponenten van de tussenliggende digitale dienstverleners. Daarnaast is de opvatting dat de eindgebruiker (bijvoorbeeld 'de slager om de hoek') niet in staat is om zelf de abuse te verhelpen. Vanuit NBIP wordt het concept uitgewerkt van 'handelingsbekwame partij'. Dit is de beheerder of partij die technisch en organisatorisch in staat is om de melding te begrijpen en de abuse te verhelpen. NBIP onderzoekt de mogelijkheden om deze partij beter te bereiken en te faciliteren in het verhelpen van de abuse.

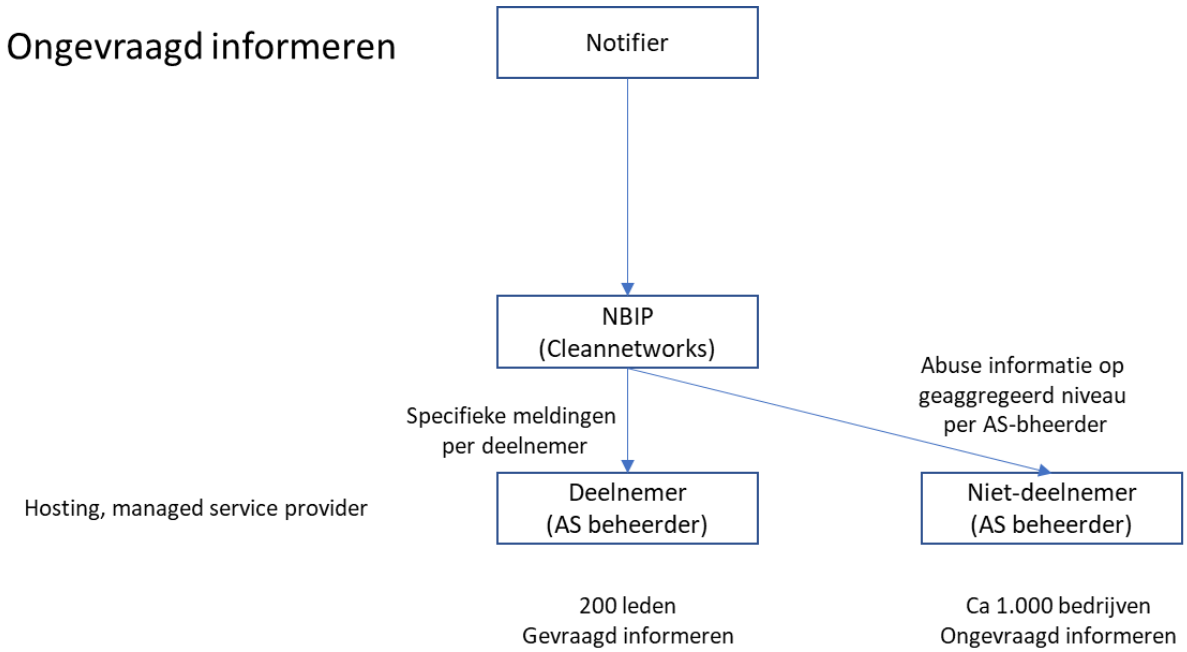


2.6 Gevraagd en ongevraagd informeren

Bij Abuse Information Exchange zijn 13 van de ca. 600 internet access providers aangesloten. Dit zijn organisaties die internet toegang en -communicatie bieden en zijn ingeschreven bij het Agentschap Telecom. Deze 13 deelnemers bedienen echter wel 90% van de markt.

Bij NBIP zijn circa 200 hosting- en andere digitale dienstverleners aangesloten die ieder ook AS-beheerder zijn. Er zijn echter circa 1.000 service providers die AS beheerder zijn en NIET zijn aangesloten. Een groot deel van de markt wordt daarom niet bereikt met gerichte abuse informatie. De deelnemers bij NBIP hebben over het algemeen een betere kwaliteitsorganisatie ten opzichte van de 1.000 andere providers die niet aangesloten zijn. Een groot deel van de abuse in Nederland wordt daarom niet opgemerkt en verholpen. Dit is aangetoond in een benchmark van de TU Delft die voor dat onderzoek meldingen ontving op IP-adressen van alle in Nederland gevestigde AS-beheerders.

Wat zijn mogelijkheden voor het NBIP-meldpunt om structureel meldingen op alle IP-adressen in Nederland te ontvangen en niet-deelnemers te melden hoeveel abuse er bij de beheerder is?
De gedachte is dat bij deze niet-deelnemer nog geen bewustzijn is van de hoeveelheid abuse en hoe daar tegen op te treden is. Door regelmatig de hoeveelheid en soort abuse te melden ontstaat bij die AS-beheerder bewustzijn en wordt deze geactiveerd om hier tegen op te treden en zich aan te sluiten bij het meldpunt. Bij het ongevraagd informeren wordt dan op geaggregeerd niveau abuse informatie naar een niet-deelnemende AS-beheerder gestuurd, dan wel bekend gemaakt.
Ook ontstaat er zicht op AS-beheerders die bewust het niet te nauw nemen en ongewenste activiteiten faciliteren ('bad hosters').



2.7 Meldingen van dreigingen, blacklist

Cyberveilig Nederland en ook Connetc2Trust ontvangen meldingen van dreigingen die vanuit 'kwaadwillende' IP-adressen plaatsvinden.
Een melding op een dergelijk IP-adres is bedoeld voor andere systeemeigenaren en beheerders om waakzaam te zijn voor dat IP-adres. Dit is een één-op-veel ontvangers communicatie van de melding. De ontvanger kan vervolgens dat IP-adres blokkeren (black list) en onderzoeken of vanuit dat verdachte IP-adres al een activiteit heeft plaatsgevonden.
Deze meldingen van IP-adressen waartegen beschermd moet worden vallen buiten scope van dit onderzoek , omdat dit geen abuse meldingen zijn.

Overigens zou het kunnen zijn dat het IP-adres die in een blacklist wordt opgenomen afkomstig is vanuit een systeem van een nietsvermoedende systeemeigenaar en dat het voor die eigenaar abuse is. In die situatie is de systeemeigenaar gebaat bij een abuse melding opdat hij geattendeerd wordt dat hij wordt afgesloten van een dienst (via blacklist).

3 Persoonsgegevens

Een persoonsgegevens betreft alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon.

Veel dreiging- en kwetsbaarheid informatie is gericht op typen organisaties, toepassingen, applicaties of misbruikmethodes, maar is niet herleidbaar naar een specifieke organisatie, locatie of persoon. Een handelingsbekwame partij kan op basis van deze informatie verder onderzoek doen en maatregelen treffen met als doel het vergroten van de weerbaarheid. Aan het delen van dit type informatie worden vanzelfsprekend vertrouwelijkheid-, integriteit-, en bekwaamheidseisen gesteld, maar het zijn geen persoonsgegevens en de AVG is hier niet op van toepassing. Het verwerken van deze informatie is buiten scope van dit onderzoek.

3.1 Opbouw van een abuse melding

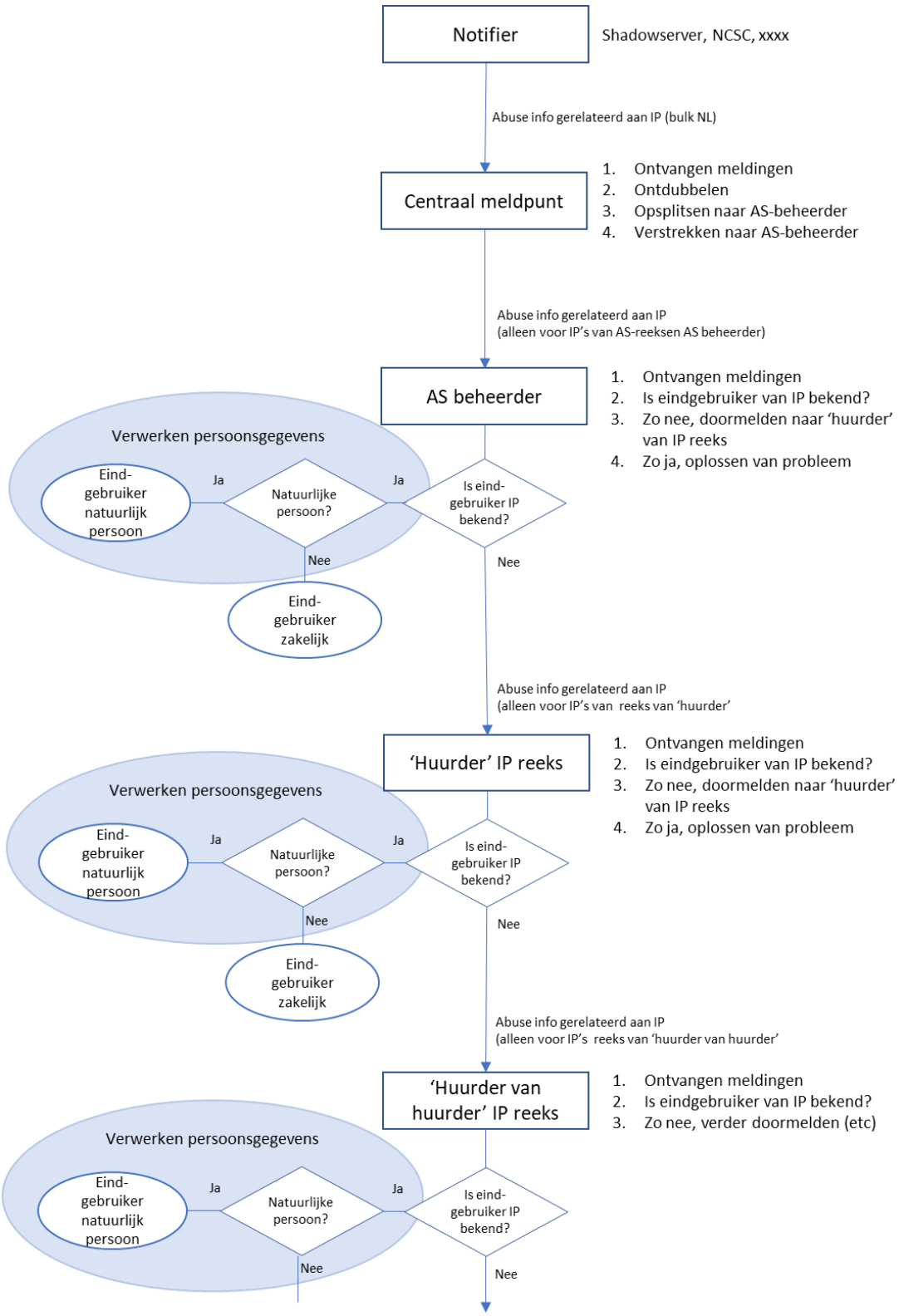
Het onderzoek richt zich op het verwerken van abuse informatie die gekoppeld is aan een IP-adres. Een abuse melding bestaat uit:

- IP-adres
- In enkele situaties een domeinnaam
- Datum/tijdstip
- Type melding (misconfiguratie, kwetsbaarheid, abuse)

3.2 Verwerking van IP adressen

De meldingsketen van abuse-informatie is als volgt:

- Het centraal meldpunt ontvangt de bulkinformatie en splitst dit op in meldingen per deelnemer (AS-beheerder) en stuurt deze door naar de respectievelijke deelnemers.
- Een deelnemer is een AS-beheerder die reeksen van IP-adressen beheert. Een AS-beheerder levert een einddienst naar een eindgebruiker of levert diensten naar andere digitale dienstverleners. In de tweede situatie is het voor de AS-beheerder onbekend wie de eindgebruiker is. De AS-beheerder stuurt dan de melding door naar zijn klant die een reeks IP-adressen heeft gehuurd van de AS-beheerder.
- De klant van de AS-beheerder (‘huurder’ van IP reeks) levert de einddienst naar de eindgebruiker of levert diensten naar andere digitale dienstverleners. Die dienstverlener huurt daarbij een deel van de IP-adressen van de huurder. In de tweede situatie is het onbekend wie de eindgebruiker is. Een abuse-melding wordt dan doorgestuurd naar diens klant. Die klant is dan de ‘huurder van de huurder’ van een IP reeks.
- Enzovoort


Notifier
Shadowserver, NCSC, xxxx
Abuse info gerelateerd aan IP (bulk NL)
Centraal meldpunt
1. Ontvangen meldingen
2. Ontdubbelen
3. Opsplitsen naar AS-beheerder
4. Verstrekken naar AS-beheerder
Abuse info gerelateerd aan IP
(alleen voor IP's van AS-reeksen AS beheerder)
AS beheerder
1. Ontvangen meldingen
2. Is eindgebruiker van IP bekend?
3. Zo nee, doormelden naar 'huurder' van IP reeks
4. Zo ja, oplossen van probleem
Verwerken persoonsgegevens
Eind-gebruiker natuurlijk persoon
Ja
Natuurlijke persoon?
Ja
Is eind-gebruiker IP bekend?
Nee
Eind-gebruiker zakelijk
Nee
Abuse info gerelateerd aan IP
(alleen voor IP's van reeks van 'huurder'
'Huurder' IP reeks
1. Ontvangen meldingen
2. Is eindgebruiker van IP bekend?
3. Zo nee, doormelden naar 'huurder' van IP reeks
4. Zo ja, oplossen van probleem
Verwerken persoonsgegevens
Eind-gebruiker natuurlijk persoon
Ja
Natuurlijke persoon?
Ja
Is eind-gebruiker IP bekend?
Nee
Eind-gebruiker zakelijk
Nee
Abuse info gerelateerd aan IP
(alleen voor IP's reeks van 'huurder van huurder'
'Huurder van huurder' IP reeks
1. Ontvangen meldingen
2. Is eindgebruiker van IP bekend?
3. Zo nee, verder doormelden (etc)
Verwerken persoonsgegevens
Eind-gebruiker natuurlijk persoon
Ja
Natuurlijke persoon?
Ja
Is eind-gebruiker IP bekend?
Nee
Nee

4 Gegevensverwerkingen

4.1 Inleiding

De LIA op abuse informatie wordt beoordeeld op de (keten)processen van de volgende organisaties:

- NBIP
- Abuse Information Exchange
- Cyberveilig Nederland
- Connect2Trust
- DIVD

Dit zijn allen non-profit koepelorganisaties, waaraan private partijen zijn verbonden.

4.2 NBIP

De stichting Nationale Beheersorganisatie Internet Providers, ofwel NBIP, levert ondersteunende diensten aan internetproviders.

Eén van die diensten betreft het ontvangen, veredelen en delen van abuse informatie. Daarvoor wordt het platform CleanNetworks gebruikt. Het doel is bestrijding van abuse door middel van het delen van abuse informatie naar haar deelnemers.

Op dit CleanNetworks platform zijn circa 200 hosting- en cloudpartijen aangesloten. Een aangesloten partij heeft een onafhankelijk netwerk dat aangesloten is op het internet. Iedere deelnemende partij beheert AS-blokken. In een AS-blok zit een reeks IP-adressen.
Sommige deelnemers bieden diensten direct aan de eindgebruiker aan, maar in de meeste situaties is de klant van de deelnemer een digitale dienstverlener die een deel van de IP-adressen van deze AS-beheerder 'huurt' voor diens dienstverlening. De klant van die deelnemer kan ook weer digitale dienstverleners als klant hebben die gebruik maken van diens IP-adressen.

CleanNetworks stelt informatie ter beschikking aan de deelnemers over abuse en kwetsbaarheden in de netwerken van de deelnemers zelf. De informatie is afkomstig van verschillende betrouwbare melders ("notifiers") en internet abuse en security onderzoekers. CleanNetworks ontvangt van notifiers zoals bijvoorbeeld de vereniging Abuse Information Exchange, het NCSC (Nationaal Cyber Security Centrum), Shadowserver en Facebook Threat Exchange meldingen ("feeds") over abuse en kwetsbaarheden in netwerken.

Een deelnemer kan met het IP-adres dan wel de domeinnaam en andere gemelde gegevens nader onderzoek doen en gepaste actie ondernemen, zoals de klant waarschuwen voor kwetsbaarheden op zijn systeem.

Een deelnemer geeft bij de aanmelding op CleanNetworks aan welke AS-blokken zijn uitgegeven. Daarnaast geeft de deelnemer toestemming CleanNetworks om voor de IP-adressen van die deelnemer abuse-informatie te verwerken.

Huidig proces

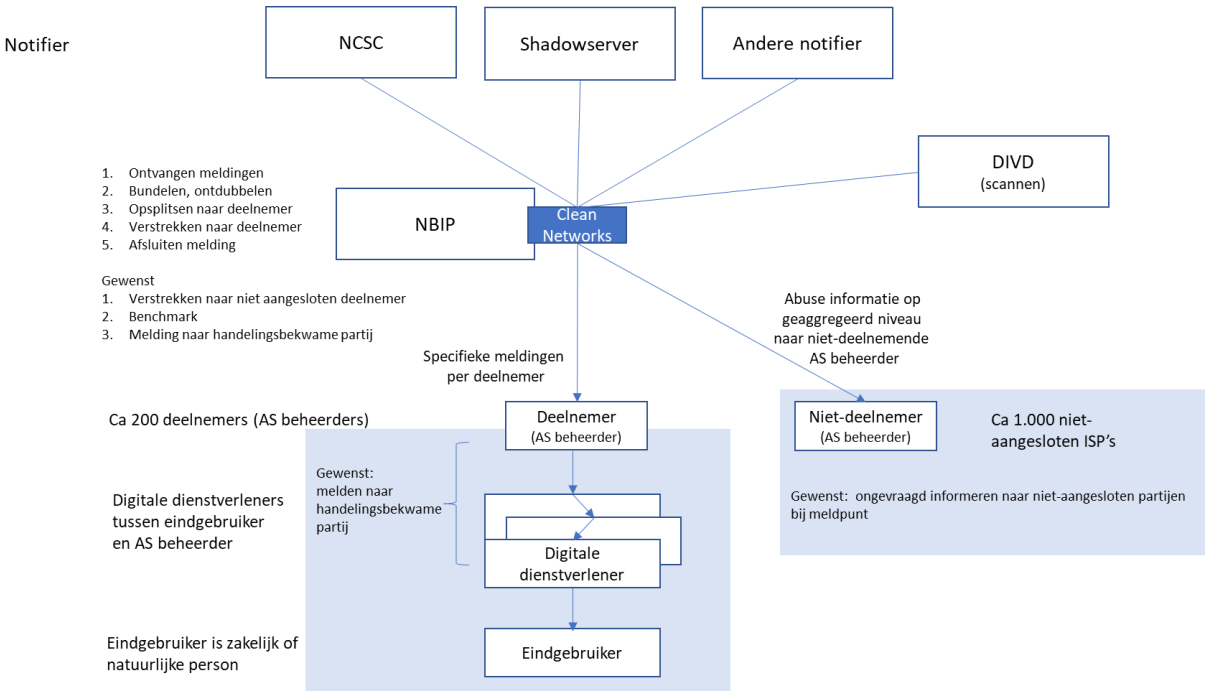
1. CleanNetworks ontvangt van notifiers abuse informatie. Op dit moment vooral van Shadowserver. Shadowserver is voornamelijk gericht op netwerkgerichte abuse. Shadowserver levert alle abuse-informatie van IP-adressen van deelnemers van CleanNetworks (o.b.v. AS).
   NBIP ontvangt ook van DIVD lijsten met gevonden kwetsbaarheden gekoppeld aan IP adressen die vallen onder de AS-en van NBIP leden

2. Op het CleanNetworks platform wordt die ontvangen abuse-informatie gebundeld en ontdubbeld en op basis van de AS-codes gesplitst naar de betreffende deelnemer en verstrekt naar die deelnemer. Een deelnemer ontvangt dus alleen abuse-informatie van de door die deelnemer uitgegeven IP's dan wel AS-reeksen.
3. De deelnemer kan met het IP-adres dan wel de domeinnaam en andere gemelde gegevens nader onderzoek doen en gepaste actie ondernemen, zoals de klant waarschuwen voor kwetsbaarheden op zijn systeem.
4. De deelnemer koppelt terug aan het Cleannetwork platform of het incident is opgelost. Twee maanden na het sluiten van het incident worden de IP-adressen en domeinnamen gewist.

Gewenst proces

NBIP ziet graag de volgende uitbreidingen op het proces.

1. Ontvangen van abuse-informatie van ook andere notifiers.
    - Op dit moment wordt alleen/vooral informatie ontvangen van Shadowserver.
    - Met NCSC zijn gesprekken op het ontvangen van abuse informatie, maar de ontvangst heeft nog niet plaatsgevonden.
2. Ongevraagd melden naar niet bij NBIP aangesloten partijen
   Bij NBIP zijn circa 200 AS beheerders aangesloten. Dit zijn organisaties met een hoge kwaliteitsstandaard. Er zijn echter ca 1.000 hosting- en cloudbedrijven (met een AS beheerstatus) niet aangesloten op CleanNetworks. Dit kunnen zogenaamde bad hosters zijn die ongewenste praktijken van eindgebruikers faciliteren. Maar het zijn vooral kleine ISP's met nog onvoldoende kwaliteit of die nog geen beeld hebben van de vervuilingen binnen het eigen domein.
   Vanuit een pilot project geleid door de TU Delft is in 2017 en 2019 een benchmark uitgevoerd waarbij als pilot vanuit Shadowserver abuse informatie van alle ISP's is ontvangen (deelnemers en niet-deelnemers van NBIP) om helder te maken hoeveel abuse per ISP-domein aanwezig is.
   Door ongevraagd ook een niet-deelnemer van abuse informatie in diens domein te voorzien, wordt gestimuleerd dat die ISP hierop actie onderneemt en handelingsbekwaam wordt om die abuse te verhelpen. Er wordt alleen informatie verstrekt over de hoeveelheid van abuse van een bepaald type in het netwerk van de betreffende ISP. Dit is een verstrekking abuse informatie op geaggregeerd niveau. Dit dient het belang van eindgebruikers die direct of indirect een dienst afnemen bij een niet op CleanNetworks aangesloten partij.



Handelingsbekwame partij

De gedachte is dat een eindgebruiker (bijvoorbeeld 'de slager om de hoek') niet zelf het technisch beheer doet en niet in staat is om met abuse informatie om te gaan. De partij die het technisch beheer doet wordt de 'handelingsbekwame partij' genoemd. Deze handelingsbekwame partij verhelpt de gevonden kwetsbaarheid. Door abuse informatie gericht naar de juiste handelingsbekwame partij te brengen wordt gestimuleerd dat de abuse daadwerkelijk wordt aangepakt.
NBIP werkt het concept van handelingsbekwame partij uit. Hierbij wordt een categorisering van handelingsbekwaamheid opgesteld die gekoppeld is aan type abuse en de feitelijke mogelijkheid om deze te verhelpen. Hierbij wordt ook aan een Keurmerk gedacht, waardoor de eindgebruiker een grotere zekerheid heeft op de handelingsbekwaamheid van diens leverancier bij het omgaan van abuse.

Kwaliteit

- Gedragscode Abusebestrijding. Alle deelnemers onderschrijven deze gedragscode.
- NBIP heeft recent de OKKT status verworven. Dit moet het eenvoudiger maken om abuse informatie met NCSC te delen
- NBIP overweegt om CERT organisatie te worden

4.3 Abuse Information Exchange

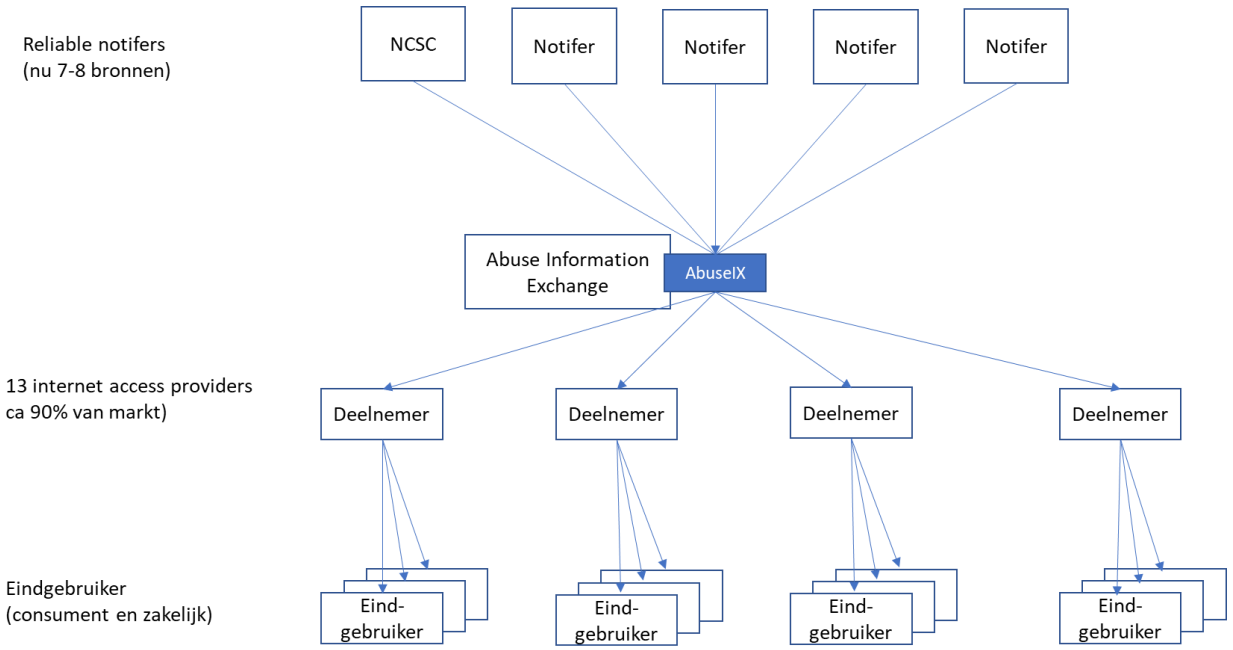
De vereniging vertegenwoordigt meer dan 90% van de markt van Nederlandse internet access providers (internet toegang) en heeft ten doel de informatievoorziening over botnets en andere vormen van internet-abuse in Nederland te verbeteren door data over besmettingen vanuit verschillende bronnen op een centraal punt te verzamelen en te correleren. Daardoor kunnen botnetbesmettingen sneller en beter bestreden worden zodat de veiligheid en stabiliteit van internet verbeterd worden.
De Abuse Information Exchange verzamelt gegevens van zogenaamde reliable notifiers over botnetbesmettingen, analyseert die en verstrekt de gegevens aan de deelnemers zodat die hun klanten kunnen waarschuwen in het geval van een besmetting. Daarnaast is de Abuse Information Exchange een forum waar de leden van de vereniging relevante kennis en informatie kunnen delen.

Bij het Abuse Information Exchange zijn de grote internet toegang providers aangesloten. De 13 aangesloten providers bedienen meer dan 90% van de internet toegang/communicatie markt. Een internet access provider is ook AS beheerder voor de IP-adressen binnen de eigen AS blokken.
Een internet access provider is ingeschreven bij de Autoriteit Consument en Markt. Overigens zijn er ca 600-800 providers bij ACM ingeschreven.

AbuseIX is het systeem van de vereniging Abuse Information Exchange. De leden geven aan Abuse Information Exchange toestemming om abuse informatie op te halen bij reliable notifiers.

1. AbuseIX ontvangt (dagelijks) van 7-8 reliable notifiers abuse informatie met betrekking tot IP-adressen van de deelnemers. Dit betreft informatie over aangetroffen virussen, malware ed. In principe zou ook informatie worden ontvangen van NCSC, maar dat is nog niet gebeurd.
2. AbuseIX ontdubbelt de ontvangen meldingen en splitst dit op richting ieder van de deelnemers. Dit gebeurt o.b.v. de bij AbuseIX bekende IP-reeksen dan wel AS-nummers van de deelnemers.
3. Een deelnemer krijgt de abuse meldingen van het eigen netwerk (op basis van AS reeksen). Hierna voert ieder deelnemer een eigen proces uit. Een lid prioriteert de abuse meldingen, bijvoorbeeld op:
    - Type besmetting (minder ernstig tot ernstig)
    - Hoe vaak een melding bij een bepaalde eindgebruiker (IP adres) voorkomt
4. Een deelnemer informeert de eindgebruiker via e-mail op de besmetting en geeft enkele tips om dit te verhelpen.
5. Van een eindgebruiker wordt verwacht dat deze de abuse verhelpt.
6. Het deelnemer houdt bij welke eindgebruikers geïnformeerd zijn en of dat IP-adres nog steeds voorkomt in de dagelijkse meldingen vanuit AbuseIX.
7. Als een eindgebruiker structureel niets doet met de abuse, dan kan de deelnemer de eindgebruiker in een zogenoemde walled-garden plaatsen. Vanaf dat moment kan de eindgebruiker alleen nog internetbankieren en naar een website gaan met tools om het probleem op te lossen.

Kwaliteit
Abuse Information Exchange heeft een OKKT status. Dit moet het eenvoudiger maken om abuse informatie vanuit NCSC te ontvangen.



4.4 Cyberveilig Nederland

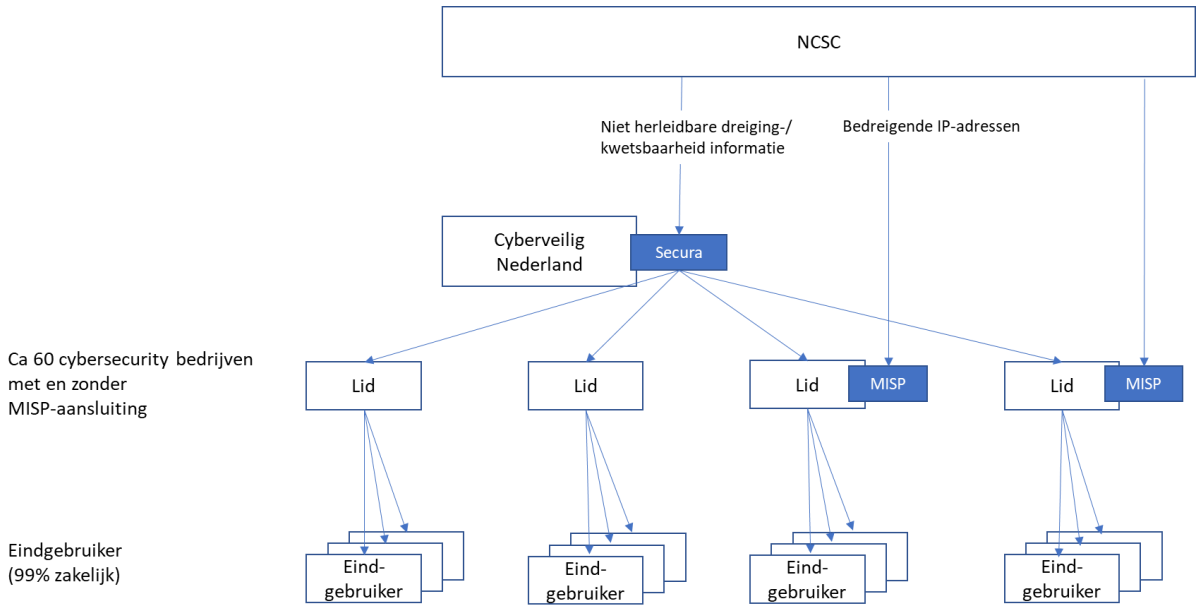
Cyberveilig Nederland is de belangenvereniging van de cybersecurity sector. Doel van Cyberveilig Nederland is de digitale weerbaarheid van Nederland te vergroten en daarnaast de kwaliteit en transparantie binnen de groeiende cybersecurity sector te verhogen. De vereniging is 3 jaar geleden opgericht en heeft nu ca. 60 cybersecurity bedrijven als lid.

Er worden momenteel twee type informatiedeling gerealiseerd:

1. Cyberveilig Nederland gaat hiervoor een platform (Secura) gebruiken welke bij een van de leden staat. Dit platform gaat abuse informatie van NCSC en mogelijk ook van leden ontvangen. Dit betreft dreiging-, kwetsbaarheid- en sectoranalyses en deze abuse informatie is niet gekoppeld aan een IP-adres en niet herleidbaar naar een specifieke eindgebruiker. Dit zijn daarmee geen persoonsgegevens. Deze abuse informatie wordt vanuit het Secura platform gedeeld met aangesloten partijen. Een aangesloten partij gebruikt de abuse informatie om de cyberweerstand van zijn klanten te verbeteren.
2. Meer technische cybersecurity bedrijven hebben een zogenaamde MISP-aansluiting (malware information sharing platform). Met een MISP kan een organisatie malware informatie delen met andere vertrouwde partijen. Er zijn plannen dat deze partijen hun MISP ook op het NCSC gaan aansluiten. In die situatie kan een lid van het NCSC een melding ontvangen die gekoppeld is aan een IP-adres. Dit betreft IP-adressen die bedreigend kunnen zijn. Een lid kan dan bij zijn klant dit IP-adres blokkeren en onderzoeken of er kwaad is geschied.

Beide verwerkingen liggen buiten de scope van het onderzoek.

De eindgebruikers (klanten van de leden) zijn voor 99% zakelijke gebruikers.
Cyberveilig Nederland heeft een OKKT status wat het eenvoudiger maakt om informatie vanuit NCSC te ontvangen. De aangesloten leden delen nu niet rechtstreeks abuse informatie met elkaar. Het is een ster-topologie.
In een werkgroep informatiedeling worden gesprekken gevoerd met betrekking tot de doelgroepen van de specifieke leden en wat voor informatie nodig is voor die leden om een beter handelingsperspectief te krijgen. Ook ligt de vraag op tafel of en hoe informatie van een lid gedeeld kan worden met andere leden, met NCSC en met CERT's.



4.5 Connect2Trust

Connect2Trust is een cross-sectoraal samenwerkingsverband tussen (inter)nationale in Nederland actieve bedrijven. Connect2Trust biedt een veilige en vertrouwde omgeving waarbinnen private partijen die onderdeel zijn van Connect2Trust, samen met de (cyber)security belaste overheidspartijen gevoelige en vertrouwelijke informatie over cyberdreigingen en best practices kunnen analyseren en uitwisselen. Connect2Trust richt zich op de lacune in informatievoorziening van de overheid naar niet-vitale grote bedrijven.

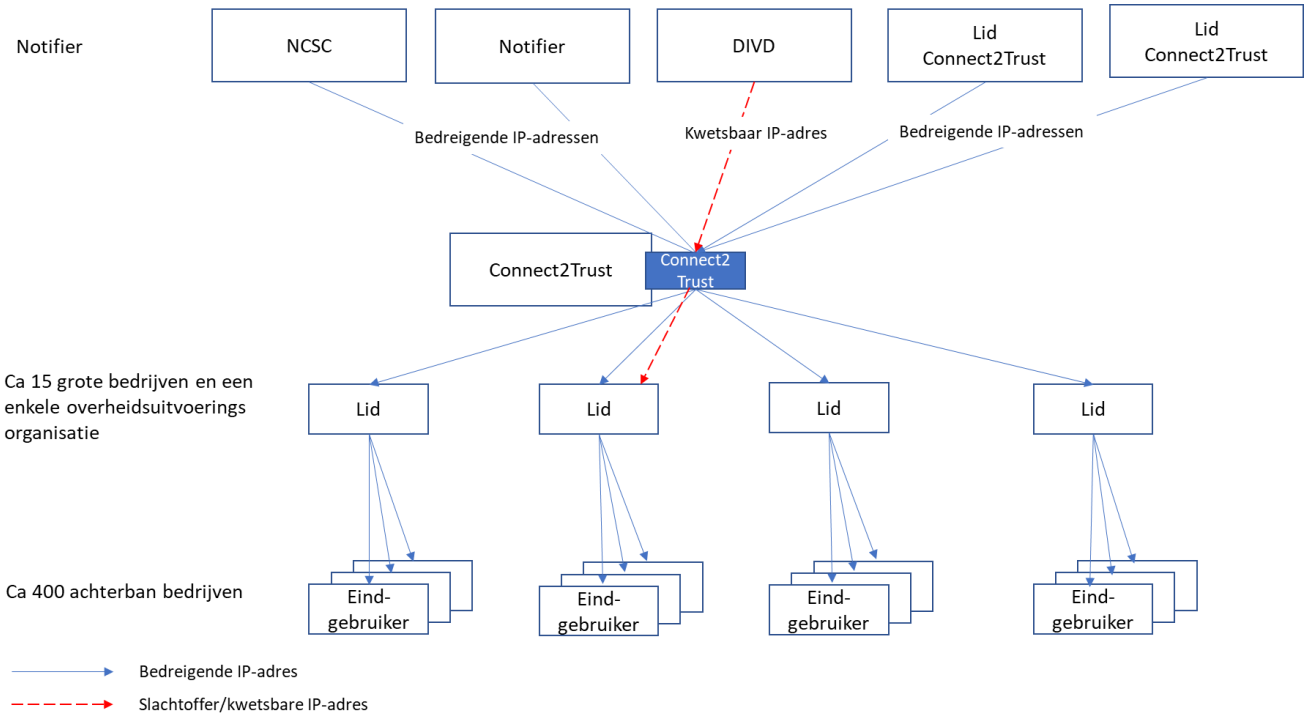
Connecte2Trust heeft een eigen platform om informatie te verwerken. Connect2Trust heeft de OKKT-status.
De leden zijn grote bedrijven en een enkele overheidsuitvoeringsorganisatie (Belastingdienst, politie). Ieder lid heeft een achterban aan bedrijven met wie informatie wordt uitgewisseld. Zo heeft PostNL een achterban richting een aantal logistieke bedrijven en Coolblue via Thuiswinkel.org een achterban richting webwinkels. Die achterban betreft een ecosysteem van het lid (bv PostNL). Het lid bepaalt welke informatie wordt doorgegeven naar de eigen achterban. Via de leden worden ca. 400 achterban bedrijven bereikt.

Connect2Trust ontvangt informatie van NCSC, commerciële notifiers en ook van de leden zelf. Dit betreft twee type meldingen:

1. Dit betreft niet-IP gerelateerde kwetsbaarheid- en dreigingsinformatie. Deze meldingen worden op het Connect2Trust platform geplaatst waarop de leden toegang hebben en informatie halen.
2. Ook worden meldingen ontvangen met betrekking tot verdachte IP-adressen. Een lid of een achterbanbedrijf kan daarop een poort hiervoor afsluiten of onderzoeken of vanuit dat verdachte IP-adres al een activiteit heeft plaatsgevonden.

Deze gegevensverwerkingen zijn geen gerichte abuse informatie en vallen buiten de scope van het onderzoek.
Daarnaast ontvangt Connect2Trust van DIVD meldingen van gevonden kwetsbaarheden gekoppeld aan een adres. Deze worden door Connect2Trust gericht doorgegeven aan het beveiligingsbedrijf welke het beheer doet op het systeem bij dat adres.

Ook DIVD is aangesloten op Connect2Trust. Een melding van DIVD betreft een kwetsbaarheid bij één van de leden. Deze kwetsbaarheid/slachtoffer notificatie gaat direct naar het betreffende lid . Deze gegevensverwerking zit in de scope van het onderzoek.

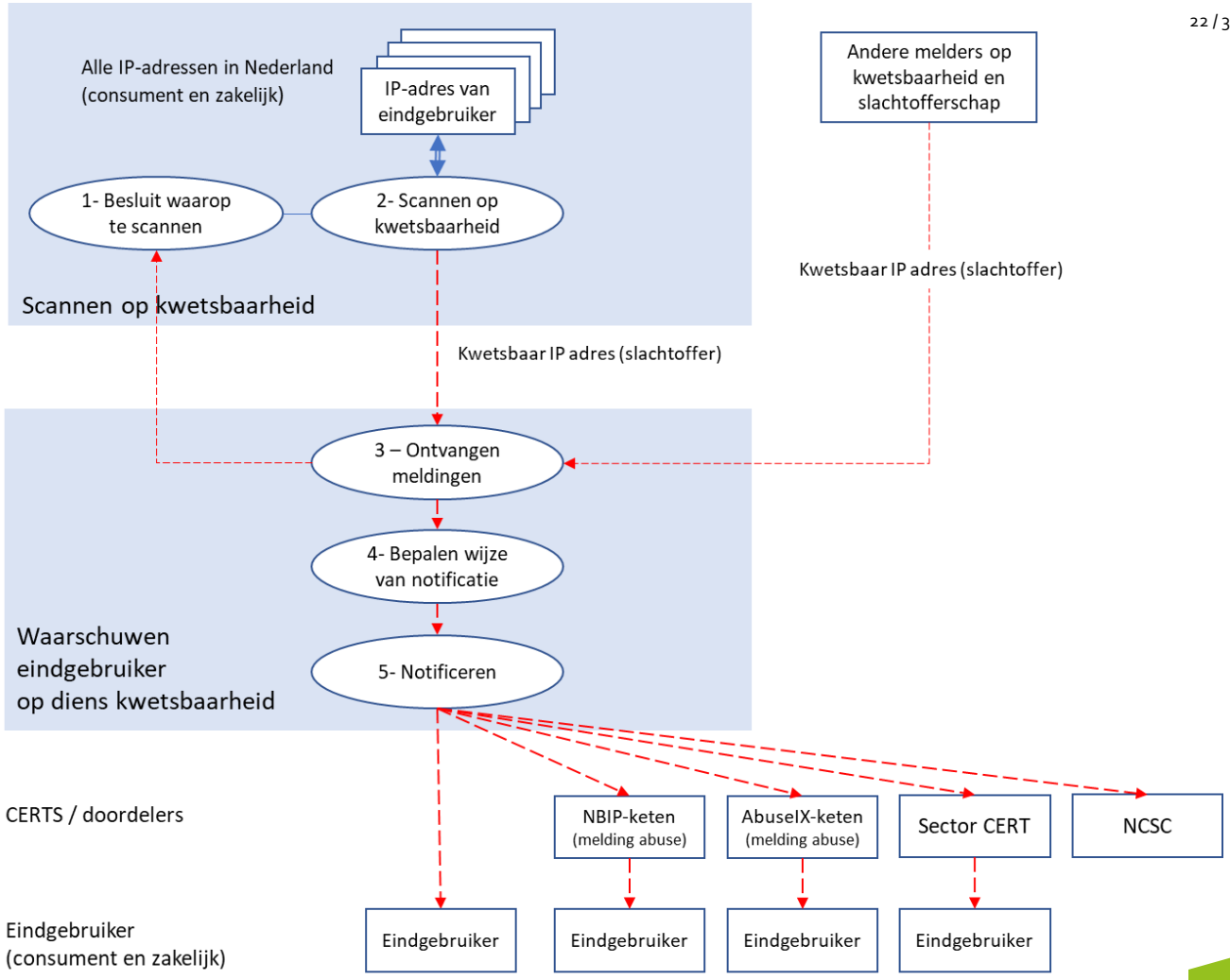


4.6 DIVD

DIVD, het Dutch Institute for Vulnerability Disclosure, richt zich op het veiliger maken van de digitale wereld door kwetsbaarheden in digitale systemen te melden aan die personen die deze kunnen verhelpen.
De DIVD activiteiten worden uitgevoerd door vrijwilligers die research doen en expert zijn op hun vakgebied (dreigingen en kwetsbaarheden). Door de krachten te bundelen in naam van een Instituut wordt een groter maatschappelijk effect bereikt.

Het proces richt zich op het onderzoeken (scannen) van kwetsbaarheid en misconfiguratie en het waarschuwen van een systeemeigenaar op diens kwetsbaarheid. In grote lijnen bestaat dit proces uit twee onderdelen:

- Het scannen van systeemcomponenten bij IP-adressen op bepaalde kwetsbaarheden.
- Het ontvangen van gevalideerde kwetsbare IP-adressen en het waarschuwen van de systeemeigenaar/eindgebruiker van dat IP-adres op die kwetsbaarheid.



Het proces is in grote lijnen als volgt:

1. Beslissen waarop te scannen
   In de voorbereidende fase ontvangt een researcher berichten over een bepaald type dreiging, dan wel kwetsbaarheid. Ook ontvangen researchers soms spontaan lijsten met IP-adressen en signalen van abuse.
   Binnen DIVD wordt besloten of een onderzoek wordt gestart. Een voorbeeld van een onderzoek betreft de opensource Mongo database met verouderde configuratie, waardoor de gegevens in die database niet meer veilig zijn.

2. Scannen op kwetsbaarheid
   Alle Nederlandse IP-adressen worden gescand en onderzocht op de betreffende kwetsbaarheid of misconfiguratie. Dit is technisch hetzelfde als het werk van een onderzoeksjournalist of een hacker. Deze activiteit wordt uitgevoerd door en onder verantwoordelijkheid van een researcher.
   De gevonden kwetsbare IP-adressen worden door de researcher in het DIVD domein geplaatst.

3. Ontvangen van meldingen
   Het meldpunt ontvangt een melding (kwetsbaar IP-adres en type kwetsbaarheid) van een researcher op basis van het scanonderzoek op dat IP-adres.
   Het meldpunt zou ook van andere partijen (bijvoorbeeld politie) een melding kunnen ontvangen van geconstateerde kwetsbaarheid en mogelijk slachtofferschap bij een systeemeigenaar (persoon, zakelijk).

4. Bepalen wijze van notificeren
   Vanuit het IP adres wordt onderzocht wie de systeemeigenaar is. Dat kan een persoon of een bedrijf zijn. Vaak is het mogelijk om vanuit het IP-adres de URL te vinden en daarna een e-mail te sturen naar info@url of abuse@url of security@url.

5. Notificeren
   De betreffende persoon of betreffend bedrijf wordt genotificeerd via een e-mail.
   Ook zijn er mogelijkheden om de melding naar een sector CERT, NBIP, Abuse Information Exchange te sturen opdat die verdere actie richting slachtoffer kan ondernemen.

De uitvoering van het proces wordt uitgevoerd conform de leidraad van Coordinated Vulnerability Disclosure. Hierbij is de insteek om het slachtoffer te informeren en de kwetsbaarheid uit de media te houden.
DIVD heeft de status van een CSIRT (computer security incident response team)

Kwaliteit
DIVD beschikt over de volgende kwaliteitsfactoren, die overigens nog steeds in verdere ontwikkeling zijn.

- Code of Conduct. Dit zijn de spelregels waarmee DIVD werkt. Met het Openbaar Ministerie zijn overigens gesprekken om deze Code of Conduct nog verder invulling te geven aan de Coordinated Vulnerabilty Disclusure
- Selectie van vrijwilligers en vrijwilligersovereenkomst
- Opleiden van onderzoekers
- CISO en FG
- Formaliseren van processen
- Via slack veel onderlinge communicatie en zelfreinigend vermogen

5 Juridisch en beleidsmatig kader

5.1 Aanpak abuse

5.1.1 Gedragscode abusebestrijding

De sector hanteert de Gedragscode Abusebestrijding.
https://www.CleanNetworks.net/gedragscode/gedragscode-abusebestrijding/

- De samenleving moet erop kunnen vertrouwen dat operators en aanbieders van digitale infrastructuur zich inspannen om gebruik van hun faciliteiten voor onrechtmatige activiteiten te voorkomen en te bestrijden. Daartoe hanteren zulke operators en/of aanbieders deze gedragscode.
- Doen al wat redelijkerwijs binnen hun mogelijkheden ligt om informatie te verkrijgen over kwetsbaarheden en abuse in hun netwerken en op hun voorzieningen. Dat doen zij door zich in ieder geval te abonneren op abuse feeds of een abuse meldpunt, het aansluiten op een nationale CERT en het raadplegen van- of aansluiten bij andere informatiebronnen die daarover inzicht geven.
- Met verwijzingen naar gedragscodes:
    - Notice and takedown 2018
    - M3AAWG Anti-Abuse Best Common Practices for Hosting and Cloud Service Providers)
- Initiatiefnemers: DHPA, DINL, ECP, ISPConnect, Ministerie van Economische Zaken en Klimaat, NBIP, TUDelft, Vereniging van Registrars. April 2018

5.1.2 Gedragscode NTD (Notice and Takedown 2018)

https://noticeandtakedowncode.nl/

- De NTD code richt zich op de afhandeling van meldingen ten aanzien van (vermeende) onrechtmatige en/of strafbare inhoud op internet.
- De code richt zich op tussenpersonen die in Nederland een openbare (telecommunicatie) dienst op Internet leveren.
- De NTD code wordt door vrijwel de gehele Nederlandse internet industrie gebruikt en wordt gesteund door de overheid (min BZK, min EZK, min JenV, NCTV, Openbaar Ministerie).

5.1.3 M3AAWG Anti-Abuse Best Common Practices for Hosting and Cloud Service Providers)

https://www.CleanNetworks.net/wp-content/uploads/2019/12/M3AAWG_Hosting_Abuse_BCPs-2015-03.pdf

- Definities en best practices voor hosting en cloud services providers op de aanpak van abuse

5.2 Aanpak malware

Op de aanpak van malware is onder meer een Werkgroep ransomware bestaande uit o.m. Cyberveilig Nederland, politie, NCSC. Dit richt zich onder meer op het vraagstuk om IP-adressen behorend bij ransomaanvallen breed te delen.

5.3 Coordinated Vulnerability Disclosure

Coordinated Vulnerability Disclosure (CVD) is het op een verantwoorde wijze en in gezamenlijkheid tussen melder en organisatie openbaar maken van ICT-kwetsbaarheden. Iedereen kan een responsible disclosure-melding doen bij een bedrijf, overheidsinstantie of andere organisatie.

NCSC heeft hierop een leidraad opgesteld.
DIVD hanteert deze leidraad en wil het slachtoffer informeren zonder daarbij de publiciteit te zoeken.

5.4 NIB Richtlijn / Wbni / OKKT

De NIB Richtlijn uit 2016, zoals neergelegd in de Wet beveiliging netwerk- en informatiesystemen (Wbni) richt zich op vergroten van cyberweerbaarheid van essentiële diensten. In december 2020 is een aangepast voorstel gepubliceerd om ook belangrijke diensten onder richtlijn te brengen. De essentiële en belangrijke diensten zijn benoemd. De NIB richt zich dus niet op overige diensten (niet-essentieel en niet-belangrijk).

De NIB geeft onder meer verplichtingen op het faciliteren van CSIRT's (of wel CERT's) voor het delen van dreiging- en kwetsbaarheid informatie
In Nederland wordt dit geconcretiseerd met een Landelijks Dekkend Stelsel waarin publieke en private partijen, zoals CERTs, sectorale en regionale samenwerkingsverbanden, het NCSC en het Digital Trust Center (DTC), informatie en kennis uitwisselen. Het NCSC fungeert hierbij als een centraal informatieknooppunt. Het concept van sectorale samenwerkingsverbanden is uitgewerkt via OKTT. Een OKTT is een samenwerkingsverband dat objectief kenbaar tot taak heeft anderen organisaties of het publiek te informeren

5.5 NCSC wel/geen nationaal meldpunt

Veel internationale melders melden alleen naar een nationaal meldpunt. Het NCSC is voor Nederland het nationaal meldpunt en ontvangt vanuit het buitenland meldingen op dreigingen en kwetsbaarheden. NCSC voert haar activiteiten uit op grond van een wettelijke taak en dat betreft het informeren van de nationale overheid en van vitale sectoren. Als ook de nieuwe NIB-richtlijn wordt aangenomen zou het NCSC ook informatie kunnen delen met benoemde belangrijke sectoren. Vanuit het NCSC wordt geen grondslag gevonden om die informatie te delen naar overige organisaties. Deze organisaties blijven daarmee ongeïnformeerd over die meldingen.

B. Juridische beoordeling

Vooropgesteld moet worden dat de gegevensverwerking tussen de partijen in deze keten in beginsel **niet** leidt tot een verwerking van persoonsgegevens. In uitzonderlijke gevallen *kunnen* er wel persoonsgegevens tussen zitten. Dit zou bijvoorbeeld het geval kunnen zijn als de informatie betrekking heeft op een specifieke eindgebruiker. Wij gaan hieronder daar nader op in.

6 Persoonsgegevens

Het begrip 'persoonsgegevens'
Het delen van abuse informatie *kan* een verwerking van persoonsgegevens opleveren, afhankelijk van de inhoud van de informatie en de context waarin deze wordt gedeeld. Wij wijzen hierbij op overweging 26 AVG en het *Breyer*-arrest van het Europese Hof van Justitie, waarin de norm voor identificeerbaarheid nader wordt uitgelegd.[4]

> Overweging 26 AVG
> De beginselen van gegevensbescherming moeten voor elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon gelden. Gepseudonimiseerde persoonsgegevens die door het gebruik van aanvullende gegevens aan een natuurlijke persoon kunnen worden gekoppeld, moeten als gegevens over een identificeerbare natuurlijke persoon worden beschouwd. Om te bepalen of een natuurlijke persoon identificeerbaar is, moet rekening worden gehouden met alle middelen waarvan redelijkerwijs valt te verwachten dat zij worden gebruikt door de verwerkingsverantwoordelijke of door een andere persoon om de natuurlijke persoon direct of indirect te identificeren, bijvoorbeeld selectietechnieken. Om uit te maken of van middelen redelijkerwijs valt te verwachten dat zij zullen worden gebruikt om de natuurlijke persoon te identificeren, moet rekening worden gehouden met alle objectieve factoren, zoals de kosten van en de tijd benodigd voor identificatie, met inachtneming van de beschikbare technologie op het tijdstip van verwerking en de technologische ontwikkelingen. De gegevensbeschermingsbeginselen dienen derhalve niet van toepassing te zijn op anonieme gegevens, namelijk gegevens die geen betrekking hebben op een geïdentificeerde of identificeerbare natuurlijke persoon of op persoonsgegevens die zodanig anoniem zijn gemaakt dat de betrokkene niet of niet meer identificeerbaar is. Deze verordening heeft derhalve geen betrekking op de verwerking van dergelijke anonieme gegevens, onder meer voor statistische of onderzoeksdoeleinden.

Het Hof zegt hierover in *Breyer*:

> 43. Aangezien deze overweging verwijst naar de middelen die redelijkerwijs kunnen worden ingezet door zowel de persoon die voor de verwerking verantwoordelijk is als een „ander[e] persoon", kan uit de bewoordingen ervan worden opgemaakt dat het voor de kwalificatie van een gegeven als "persoonsgegeven" in de zin van [nu art. 4 lid 1 AVG, *JT*] niet vereist is dat alle informatie aan de hand waarvan de betrokkene kan worden geïdentificeerd, bij een en dezelfde persoon berust.
> 44. Dat de extra informatie die nodig is om de gebruiker van een website te identificeren, niet berust bij de aanbieder van onlinemediadiensten, maar bij de internetprovider van deze gebruiker, lijkt dan ook niet uit te sluiten dat dynamische IP-adressen die worden geregistreerd door deze aanbieder, voor hem persoonsgegevens vormen in de zin van [nu artikel 4 lid 1 AVG. *JT*].
> 45. Vastgesteld dient evenwel te worden of de mogelijkheid om een dynamisch IP-adres te combineren met

[4] De abuse informatie moet uiteraard ook voldoen aan de drie andere eisen van het begrip 'persoonsgegevens': het moet 'informatie' zijn (1), 'over' (2) een natuurlijke persoon (3). 'Informatie' en 'over' zijn in deze casus een gegeven. De informatie kan echter ook over een rechtspersoon gaan (bijv. een BV). Voor deze casus gaan wij er van uit dat abuse informatie gerelateerd aan de apparatuur of het IP-adres van een consument een persoonsgegeven is in de zin van de AVG.

de extra informatie waarvan die internetprovider in het bezit is, een middel vormt waarvan mag worden aangenomen dat het redelijkerwijs kan worden ingezet om de betrokken persoon te identificeren.

Vervolgens concludeert het Hof:

> [Nu art. 4 lid 1 AVG, *JT*] moet aldus worden uitgelegd dat een dynamisch internetprotocoladres dat door een aanbieder van onlinemediadiensten wordt geregistreerd telkens als een persoon een website bezoekt die door deze aanbieder toegankelijk wordt gemaakt voor het publiek, ten aanzien van die aanbieder een persoonsgegeven in de zin van voormelde bepaling vormt, wanneer hij beschikt over wettige middelen waarmee hij de betrokken persoon kan identificeren aan de hand van extra informatie die bij de internetprovider van deze persoon berust.

Deze uitspraak betekent voor de onderhavige casus drie dingen:

1. Identificatie van de eindgebruiker is **contextueel**, niet theoretisch. Er moet in de context van de gegevensverwerking dus sprake zijn van identificeerbaarheid. Enerzijds kan dat besloten liggen in het doel van de gegevensverwerking, anderzijds kan dat volgen uit de middelen die de ketenpartner(s) ter beschikking staan. Het enkele feit dat het niet uitgesloten is, dat er ergens iemand is die de persoon achter een IP adres kan identificeren, is dus niet genoeg om de AVG te triggeren.

2. Als één of meer ketenpartners de redelijke mogelijkheden heeft om de gegevens die in de keten worden doorgegeven aan de betrokkene kunnen koppelen, verwerken in beginsel **alle partijen** in de keten persoonsgegevens; dus óók als zij zelf niet de mogelijkheid hebben om iemand te identificeren. Dat is alleen anders als er duidelijke afspraken zijn gemaakt om niet te proberen iemand te identificeren (dan wel als dat wettelijk is verboden) of als de identificatie in de rest van de keten, gelet op de omstandigheden, onwaarschijnlijk is.

3. Geaggregeerde informatie zijn geen persoonsgegevens, mits de groepsgrootte groot genoeg is, en valt dus niet onder de AVG.

In het vervolg van dit rapport gaan wij er van uit dat er In de keten wél persoonsgegevens worden verwerkt.

Wel of geen persoonsgegeven?

Wél een persoonsgegeven is (doorgaans):
- Een IP adres dat is te herleiden tot de internetaansluiting van een consument of een werknemer van een organisatie.
- Een kwetsbaarheid op het systeem van een consument of werknemer van een organisatie.
- E-mail adres van een medewerker van een bedrijf (jan.jansen@bedrijf.nl)
- E-mail adres van een éénpersoonsbedrijf (info@JanJansenKeukens.nl)

Geen persoonsgegeven is (doorgaans):
- Een IP adres of kwetsbaarheid dat hoort bij een op internet aangesloten machine die eigendom is van een bedrijf en niet aan een persoon gekoppeld is (bijv. een server of een netwerkprinter).
- Geaggregeerde informatie, mits de groepsgrootte groot genoeg is.
- Algemeen e-mail adres van een bedrijf (abuse@bedrijf.nl)

7 Criteria gerechtvaardigd belang

Een verwerking van persoonsgegevens behoeft een grondslag. Deze staan genoemd in artikel 6 lid 1 AVG. De enige in aanmerking komende verwerkingsgrondslag in artikel 6(1) AVG voor het delen van abuse informatie tussen de ketenpartners, die kwalificeert als persoonsgegevens, is het gerechtvaardigd belang (art. 6(1), onderdeel f AVG).

Om een beroep te kunnen doen op artikel 6(1)(f) AVG moeten aan drie criteria worden voldaan:

1. Het belang moet gerechtvaardigd zijn;
2. De verwerking moet noodzakelijk zijn voor dat belang;
3. Het belang van de verwerkingsverantwoordelijke of een derde waaraan de gegevens worden verstrekt moet zwaarder wegen dan het belang van de betrokkene (belangenafweging).

Ad 1) Beoordeling gerechtvaardigdheid van het belang
Als gerechtvaardigde belangen kunnen worden beschouwd: alle belangen van de verwerkingsverantwoordelijke of een derde die niet door de wet verboden zijn of als maatschappelijk onaanvaardbaar worden beschouwd.[5] Ofwel zoals de voorganger van de EDPB, de Artikel 29 Werkgroep, het verwoordde:

> *Om relevant te zijn in het kader van [artikel 6 lid 1 sub f AVG, JT], moet een "gerechtvaardigd belang" daarom:*
> *- rechtmatig zijn (d.w.z. in overeenstemming met toepasselijk EU- en nationaal recht);*
> *- voldoende duidelijk zijn verwoord om de afweging uit te kunnen voeren met de belangen en fundamentele rechten van de betrokkene (d.w.z. voldoende specifiek);*
> *- een werkelijk en aanwezig belang vertegenwoordigen (d.w.z. niet speculatief zijn).*

Het belang van het delen van abuse informatie in de keten is het veiliger maken van het internet. Dit belang is noch verboden noch een doel dat in strijd is met de ongeschreven rechtsregel van de maatschappelijke betamelijkheid. Het belang van de betrokken partijen in de keten is ook voldoende specifiek en niet speculatief.

Derhalve voldoet het delen van de abuse informatie volgens ons aan het eerste criterium van artikel 6(1)(f) AVG (gerechtvaardigdheid).

Ad 2) Beoordeling van de noodzakelijkheid
Noodzakelijkheid van de gegevensverwerking is onderdeel van het bredere beginsel van *dataminimalisatie.*[6] Het valt uiteen in twee aspecten:

1. Is de gegevensverwerking geschikt om het doel te bereiken (*effectiviteit)*?
2. Is het doel ook met minder vergaande middelen te bereiken (*subsidiariteit)*?

Zonder nader onderzoek te hebben gedaan naar vraag of elke specifieke gegevensverwerking in de keten van abuse informatie ook daadwerkelijk bijdraagt aan het stoppen van abuse, mogen we wel aannemen dat het aannemelijk is dat het delen van abuse informatie een belangrijke bijdrage levert aan het stoppen van abuse. Dat is immers het hele bestaansrecht van de keten.

---

[5] NB. De Normuitleg van de AP gaat uit van een belang dat door de wet is erkend (positieve beoordeling), maar die normuitleg is door de rechtbank Midden-Nederland -terecht- afgewezen in de *VoetbalTV*-zaak. De rechtbank stelt dat alle belangen in beginsel gerechtvaardigd kunnen zijn, tenzij door de wet verboden (negatieve beoordeling).

[6] Zie ook artikel 5(1)(c) AVG.

Abuse informatie kan op grond van de principes van de AVG alleen gedeeld kunnen worden met partijen die het in hun macht hebben om de abuse te stoppen (de zg. 'handelingsbekwame partijen'). Het delen van alle data met alle partijen in de keten is niet nodig en in AVG-termen dus niet proportioneel. Voor zover de abuse informatie kwalificeert als persoonsgegevens zal dus een uitsplitsing naar ontvangers moeten plaatsvinden.

De bestaande kanalen op grond van de Wet beveiliging netwerk- en informatiesystemen (Wbni) bieden volgens de deelnemers onvoldoende mogelijkheden om de abuse te delen met partijen die niet zijn c.q. kunnen worden aangesloten op de NCSC informatiestromen. Het NCSC kan momenteel vanuit zijn wettelijke grondslag alleen informatie over dreigingen en incidenten delen met:

- een samenwerkingsverband dat objectief kenbaar tot taak (OKTT) heeft andere organisaties of het publiek te informeren,
- Europese nationale CSIRT's,
- computercrisisteams (CERT's of CSIRT's) die bij ministeriële regeling zijn aangewezen,
- aanbieders van internettoegang om de gebruikers ervan te informeren.

Dit alles overziend, achten wij de gegevensdeling in de keten noodzakelijk.

Ad 3) Belangenafweging
Bij de belangenafweging moet rekening gehouden worden met de **gevolgen** die de gegevensverwerking heeft voor de betrokkene. Daarbij zijn de volgende factoren van belang:

- de aard van de gegevens
- de manier waarop de gegevens worden verwerkt
- de redelijke verwachtingen van de betrokkene, en
- de verhouding tussen de verwerkingsverantwoordelijke en de betrokkene.

Deze factoren leiden tot een **voorlopige balans** tussen de belangen van partijen. Indien deze balans niet in evenwicht is, moet worden gekeken naar de door de verwerkings-verantwoordelijke toegepaste **aanvullende waarborgen**. Hoe aanzienlijker de gevolgen voor de betrokkene, hoe meer aandacht moet worden geschonken aan de toepasselijke waarborgen.

<u>Aard van de gegevens</u>
Een abuse melding bestaat uit: een IP-adres, de datum/tijdstip van het abuse, en het type melding (misconfiguratie, kwetsbaarheid, abuse). Deze gegevens kunnen, afhankelijk van de inhoud ervan, gevoelig zijn.[7] Echter, gelet op de scope van dit rapport achten wij de gevoeligheid van de gegevens laag.

[7] NB. Abuse informatie die bestaat uit het plegen van strafbare feiten is in dit rapport out-of-scope. Als dit type informatie in de toekomst wel in scope komt van de abuse meldingen, dan dient een hernieuwde afweging plaats te vinden. Wij merken daarbij op dat er *geen* sprake is van strafrechtelijke gegevens in de zin van artikel 10 AVG als de informatie geen betrekking heeft op, d.w.z., niet direct of indirect herleidbaar is tot, plegers van het strafbare feit. Een signaal dat iemand slachtoffer is van een strafbare abuse is dus geen strafrechtelijk gegevens met betrekking tot het slachtoffer, alleen met betrekking tot de dader (mits herleidbaar). Voor zover de abuse informatie strafrechtelijke gegevens opleveren over de eigenaar van het systeem van waaruit de abuse plaatsvindt, kan de bevoegdheid om de gegevens te verwerken in sommige gevallen gevonden worden in artikel 33 lid 2 sub c UAVG. Het gaat echter mis als de strafrechtelijke gegevens worden verwerkt "ten behoeve van een derde" in de keten. Artikel 33 lid 4 UAVG kent slechts een beperkt aantal gronden waarop private partijen strafrechtelijke gegevens mogen verwerken voor anderen en die gegevens met hen mogen uitwisselen, zoals een vergunning in het kader van de Wet op de particuliere recherchebureaus en beveiligingsorganisaties dan wel een vergunning van de AP. Als dit in de toekomst wel in scope komt, dan is waarschijnlijk een wetswijziging nodig om een structurele basis te bieden aan het verwerken van strafrechtelijke abuse informatie in de keten.

Manier waarop de gegevens worden verwerkt.
De beoordeling van de gevolgen in bredere zin kan inhouden dat ernaar wordt gekeken of de gegevens openbaar zijn gemaakt of anderszins toegankelijk zijn gemaakt voor een groot aantal personen of dat grote hoeveelheden persoonsgegevens worden verwerkt in combinatie met andere gegevens. Ook moet de beschikbaarheid van alternatieve methoden voor het bereiken van de door de voor de verwerking verantwoordelijke nagestreefde doeleinden met minder negatieve gevolgen voor de betrokkene worden meegewogen.

Voorop gesteld moet worden dat in deze casus de verwerkte gegevens meestal geen persoonsgegevens zullen zijn. Er is dan ook geen sprake van een gegevensverwerking op grote schaal. Ook is de dataset per geval beperkt. Hoewel er wel meerdere partijen in de keten zijn betrokken waartussen de abuse informatie wordt doorgegeven, is er in casu geen sprake van openbaarmaking. Uiteraard is het nodig dat partijen alleen de informatie ontvangen die voor hen relevant zijn. Op dit punt na, zien wij ook hier geen belemmeringen.

Redelijke verwachtingen van de betrokkene
Bij dit aspect van de belangenafweging dient te worden gekeken of er risico's of belemmeringen voortvloeien uit hetgeen de betrokkene redelijkerwijs van de verwerkingsverantwoordelijke mag verwachten, zoals de status van de verwerkingsverantwoordelijke, de aard van de relatie tussen de partijen, de aard van de dienst waarin de gegevens zijn verzameld, en de toepasselijke wettelijke of contractuele verplichtingen en beloften die aan de betrokkene zijn gedaan. In het algemeen geldt dat hoe specifieker en beperkter de context van de verzameling is, des te meer beperkingen er waarschijnlijk aan het gebruik zullen worden gesteld.

Ons zijn geen wettelijke of contractuele beperkingen bekend. Voor zover de abuse informatie is verkregen als gevolg van een inbreuk op het communicatiegeheim, kan mogelijk aansluiting worden gezocht bij artikel 11.2 lid 2 sub b Telecommunicatiewet: "waarborgen van de integriteit en de veiligheid van de netwerken en diensten". Dit is wel afhankelijk van de vraag of de betrokken partij kan worden gekwalificeerd als een "aanbieder van een openbaar elektronisch communicatienetwerk en de aanbieder van een openbare elektronische communicatiedienst".[8]

Wij wijzen in deze ook op de recent in de Europese Raad van Ministers aangenomen concepttekst van de ePrivacy Verordening. Artikel 6 lid 1 sub b en c zegt dat een eventuele inbreuk op het communicatiegeheim is toegestaan indien:

> *(b) it is necessary to maintain or restore the security of electronic communications networks and services, or detect technical faults, errors, security risks or attacks on electronic communications networks and services;*
> *(c) it is necessary to detect or prevent security risks or attacks on end-users' terminal equipment;*

Vooral de (c)-grond geeft hier ruimte om abuse-informatie te verwerken.

De verhouding tussen de verwerkingsverantwoordelijke en de betrokkene

[8] Wij wijzen in deze ook op de recent in de Europese Raad van Ministers aangenomen concepttekst van de toekomstige ePrivacy Verordening. Artikel 6 lid 1 sub b en c zegt dat een eventuele inbreuk op het communicatiegeheim is toegestaan indien:

> (b) it is necessary to maintain or restore the security of electronic communications networks and services, or detect technical faults, errors, security risks or attacks on electronic communications networks and services;
> (c) it is necessary to detect or prevent security risks or attacks on end-users' terminal equipment;

Vooral de (c)-grond geeft hier ruimte om abuse-informatie te verwerken.

Afhankelijk van de vraag of de voor de verwerking verantwoordelijke een individueel persoon of een kleine organisatie, een multinational of een overheidsinstantie is, en afhankelijk van de specifieke omstandigheden, kan zijn positie in meer of mindere mate dominant zijn ten opzichte van de betrokkene. Aan de andere kant is ook de status van de betrokkene relevant. Hoewel bij de belangenafweging in beginsel moet worden uitgegaan van een gemiddeld persoon, moet er in specifieke omstandigheden een meer ad-hoc-benadering plaatsvinden, zoals in geval de betrokkene een kind is of tot een andere kwetsbare groep behoort. Ook de vraag of een ongelijkheid bestaat in de relatie tussen de betrokkene en de voor de verwerking verantwoordelijke is relevant.

Dit criterium achten wij in deze kwestie niet relevant. Er is geen sprake van machtsongelijkheid, noch van kwetsbare groepen.

Voorlopige balans

Het doel van de belangenafweging overeenkomstig art. 6(1)(f) AVG, is niet het voorkomen van alle negatieve gevolgen voor de betrokkene. Het doel is eerder het voorkomen van onevenredige gevolgen. Als we de balans opmaken, dan komen we tot de conclusie dat er geen sprake is van onevenredige gevolgen. Sterker, de gevolgen zijn over het algemeen positief: de betrokkene wordt geïnformeerd over kwetsbaarheden of abuse in zijn systeem en kan daar indien nodig actie op ondernemen.

Waarborgen

Anders dan de reeds genoemde uitsplitsing van de gegevensstromen en de basismaatregelen in de AVG, zoals beperkte bewaartermijnen en informatiebeveiliging, zijn er geen bijzondere waarborgen nodig om het evenwicht te herstellen.

8 Conclusie

1. **Voor zover de abuse informatie kwalificeert als persoonsgegevens (wat meestal niet het geval is), kan de informatie worden verwerkt op grond van artikel 6(1)(f) AVG (gerechtvaardigd belang).**
   Een voorwaarde hiervoor is dat deze informatie wordt uitgesplitst naar de partij die de abuse kan verhelpen en dat deze zich netjes aan de basisvoorwaarden van de AVG houdt.

2. Deze conclusie geldt niet als de abuse informatie kwalificeert als strafrechtelijke gegevens over daders (out-of-scope van dit rapport). Indien dit soort informatie in de toekomst in de scope komt, dient een nieuwe afweging gemaakt te worden. Zo is bijvoorbeeld het verwerken van strafrechtelijke gegevens als dienstverlening aan derden niet toegestaan zonder vergunning op grond van de Wet op de particuliere beveiligingsorganisaties en rechercheburaus. Bij gebrek daaraan is een vergunning van de Autoriteit Persoonsgegevens (AP) vereist (art. 33 lid 4 UAVG). Het is wél toegestaan om strafrechtelijke gegevens te verwerken om je eigen belangen of dat van je personeel te beschermen (art. 33 lid 2 UAVG). Als abuse-informatie die kwalificeert als strafrechtelijke persoonsgegevens in de toekomst wél in scope komt van de activiteiten van AAN, dan adviseren wij een wetswijziging in art. 33 UAVG op dit punt.

3. Geaggregeerde informatie is -mits de groepsgrootte groot genoeg is- geen persoonsgegeven. Het verstrekken van geaggregeerde abuse informatie aan niet-aangesloten partijen valt dan ook niet onder de AVG, zodat er vanuit dat punt geen belemmeringen zijn om het te doen.

Bijlage 1 Gesprekspartners

De volgende personen zijn gesproken bij deze LIA:

- Marjolijn Durinck, projectmanager ECP
- Octavia de Weerdt, NBIP
- Rene Blankestein, Abuse Internet Exchange
- Danielle Hermsen, Abuse Internet Exchange
- Chris van 't Hof, DIVD
- Fleur van Leusden, DIVD
- Astrid Oosenbrug, DIVD
- Liesbeth Holterman, Cyberveilig Nederland
- Petra Oldengarm, Cyberveilig Nederland
- Raymond Bierens, Connect2Trust
- Gunther Cleijn, Connetc2Trust

Documenthistorie

Versie	*Wijziging*	*Verspreiding*
0.9		Astrid Oosenbrug, Chris van 't Hof, Danielle Hermsen, Liesbeth Holterman, Marjolijn Durinck, Octavia de Weerdt, Raymond Bkierens
0.91	Managementsamenvatting	Leden van AAN tbv review en behoefte aan verduidelijkingen
1.0	Opnemen van een enkele verduidelijking	
1.1	Toevoeging enkele verduidelij-kingen in beschrijving DIVD	

Einde rapportage

Privacy
Management
Partners
Coöperatie UA

adres
Vondellaan 58
3521 GH Utrecht

telefoon
+31 85 401 38 66

e-mail
info@pmpartners.nl

website
www.pmpartners.nl