Van: 5.1.2.e
Verzonden: donderdag 4 februari 2021 12:56
Aan: 5.1.2.e
CC: 5.1.2.e
Onderwerp: Leesvoer over encryptiedilemmas

We zijn in goed gezelschap met onze beweringen, los van wat AIVD wil gaan vertellen. Ligt daarom nogal een bewijslast als je beweert dat boel niet verzwakt.
Hierbij zo wat linkjes naar documenten. Heb er nog meer (ook een van een Amerikaanse commissie die dit heeft bekeken), maar zou even moeten zoeken.

http://www.nytimes.com/2015/07/08/technology/code-specialists-oppose-us-and-british-government-access-to-encrypted-communication.html?hp&action=click&pgtype=Homepage&module=first-column-region&region=top-news&WT.nav=top-news&_r=1

https://www.security.nl/posting/434820/Experts+waarschuwen+voor+overheidstoegang+tot+versleutelde+data?channel=rss

http://dspace.mit.edu/bitstream/handle/1721.1/97690/MIT-CSAIL-TR-2015-026.pdf

Van: 5.1.2.e @minjenv.nl>
Verzonden: donderdag 4 februari 2021 13:09
Aan: 5.1.2.e
CC: 5.1.2.e
Onderwerp: Nota en aanmeldingsformulier ACEV
Bijlagen: AanbiedingsFormulier ACEV 5G en de opsporing feb2021.pdf; 210204 Nota ACEV februari 2021 EZKJenV.docx

Urgentie: Hoog

Categorieën: Categorie Rood

Let op, in de bijlage van deze e-mail, verzonden door 5.1.2.e @minjenv.nl, is een macro aangetroffen. Macro's kunnen misbruikt worden om malware op uw systeem te installeren. Open de bijlage alleen als de e-mail afkomstig is van een door u vertrouwde afzender.

Indien dit niet het geval is dient u deze e-mail direct te verwijderen zonder de bijlage te openen.

DICTU Servicedesk

Dag allen,

Bijgesloten vinden jullie de wat ons betreft defintieve nota een aangepaste versie van het aanbiedingsformulier. Zonder tegenreactie stuur ik deze set om 13:15 straks naar AZ. Ik heb 5.1.2.e als tweede contactpersoon daarin opgenomen.

5.1.2.e heeft 5.1.2.e net geappt, argument dat controversieel verklaring van encryptie-brief van invloed kan zijn op keuze ACEV of MCEV is toch echt voor EZK. Daar staat het nu ook. Is voor JenV geen argument om in ACEV of MCEV een bepaalde keuze wel of niet te laten nemen. Als MCEV dat wil kunnen ze dat meenemen vanuit het EZK standpunt en daar alsnog toe besluiten.

Groet,

5.1.2.e

Van: 5.1.2.e @minjenv.nl>
Verzonden: donderdag 4 februari 2021 13:20
Aan: 5.1.2.e
CC: 5.1.2.e
Onderwerp: OTT Nota en aanmeldingsformulier ACEV
Bijlagen: AanbiedingsFormulier ACEV 5G en de opsporing feb2021.pdf; 210204 Nota ACEV februari 2021 EZKJenV.docx; Bijlage bij nota.docx; Bijlage 2 bij nota.pdf

Urgentie: Hoog

Categorieën: Categorie Rood

Let op, in de bijlage van deze e-mail, verzonden door 5.1.2.e @minjenv.nl, is een macro aangetroffen. Macro's kunnen misbruikt worden om malware op uw systeem te installeren. Open de bijlage alleen als de e-mail afkomstig is van een door u vertrouwde afzender.

Indien dit niet het geval is dient u deze e-mail direct te verwijderen zonder de bijlage te openen.

DICTU Servicedesk

Dag 5.1.2.e

Hierbij op de valreep de stukken voor agendapunt aftapbaarheid OTT diensten voor ACEV van volgende week. Dank alvast voor het verspreiden.

Groet,

5.1.2.e

69b

Ministerie van Justitie en Veiligheid

ACEV

Minister van Justitie en Veiligheid

Turfmarkt 147
2511 DP Den Haag
Postbus 20301
2500 EH Den Haag
www.rijksoverheid.nl/jenv

Datum
31 januari 2021

Ons kenmerk
3158369

nota

Interceptie 5G en OTT-communicatiediensten

Doel

- U te informeren over de dilemma's die ten grondslag liggen aan de vraag hoe zorgvuldig invulling gegeven kan worden aan het MCEV-besluit van mei 2020 om Over-The-Top-communicatiediensten (OTT) net als telecommunicatiediensten wettelijk te verplichten om hun communicatiedienst, in het bijzonder met betrekking tot encryptie, zodanig in te richten dat communicatie daarover afgetapt kan worden ten behoeve van de opsporing of nationale veiligheid.
- Vervolgens is het doel dat u, na kennisname over de gevolgen en risico's, een keuze maakt uit de hieronder geschetste opties en deze ter besluitvorming doorgeleidt aan de MCEV, conform het verzoek daartoe van de Minister van Justitie en Veiligheid.

Beslispunt

In de MCEV van mei 2020 is, op basis van eerdere besluitvorming en een beleidstraject van JenV en EZK in de ACEV en MCEV in 2019 en 2020, ingestemd met bijgesloten beleidsnota '5G en de opsporing'. Op basis daarvan is gestart met de uitwerking van de daarbij beoogde wet- en regelgeving. Onderdeel van dat besluit is dat de verplichtingen uit hoofdstuk 13 van de Telecommunicatiewet – waaronder interceptie/kunnen tappen – die nu enkel gelden voor openbare telecommunicatiediensten ook van toepassing worden voor alle aanbieders van elektronische communicatiediensten, waaronder OTT-communicatiediensten, zoals WhatsApp, Signal, Telegram, etc. Dat is nodig om interceptie van gesprekken tussen personen als effectief middel voor de opsporings- en veiligheidsdiensten te behouden, omdat de laatste tien jaar het merendeel van de interpersoonlijke communicatie via versleutelde OTT-communicatiediensten is gaan verlopen. De communicatie via OTT-diensten is beveiligd met end-to-end encryptie en daardoor, in tegenstelling telecommunicatiediensten, niet inhoudelijk af te luisteren. Dit heeft in toenemende mate grote gevolgen voor de effectiviteit van de opsporing en risico's voor de nationale veiligheid.

Bij het MCEV-besluit is tevens bepaald dat verkend zal worden of de realisatie van dit besluit kan worden meegenomen in het reeds lopende wetsvoorstel voor het behoud van interceptiemogelijkheden bij de komst van 5G. Dat kan, maar EZK voorziet ondanks eerdere besluitvorming en debat hierover toch risico's ten aanzien van veilige encryptie als OTT-diensten aftapbaar worden. Bovendien heeft

de Kamer de brief van de Minister van JenV over de EU-Raadsconclusies over rechtmatige toegang tot versleuteld bewijs van 14 december jl. controversieel verklaard (zie bijlage).

Om een vervolg te geven aan het MCEV-besluit ligt een viertal opties voor:

1. De MCEV handhaaft haar besluit van mei 2020 dat OTT-communicatiediensten in de Telecommunicatiewet (Tw) tot dezelfde inrichtings- en medewerkingseisen worden verplicht als telecommunicatiediensten.
2. Hetzelfde als 1, maar de gewijzigde wet treedt nog niet in werking voor OTT-communicatiediensten. Een besluit over eventuele inwerkingtreding wordt pas later genomen, mede op basis van de verkenning naar toegang tot versleuteld digitaal (bewijs)materiaal door de Europese Commissie. De Commissie gaat dit verkennen naar aanleiding van de EU raadsverklaring van december jl. Dit kan worden uitgelegd in de Memorie van Toelichting van het wetsvoorstel.
3. De MCEV besluit om nog geen wijzigingen in de Tw op te nemen en eerst de effecten van een verplichting tot ontsleuteling t.b.v. aftappen in kaart te brengen. Hiertoe kan de Europese technische inventarisatie benut worden, waarbij ook de OTT-spelers worden betrokken. Vervolgens kan er een belangenafweging plaatsvinden op grond waarvan de MCEV kan besluiten tot het al dan niet alsnog opnemen van een dergelijke bepaling in de Tw.
4. De MCEV neemt het besluit om voorlopig af te zien van het opnemen van een verplichting tot het aftappen OTT-dienstverleners.

<u>Standpunt JenV</u>
JenV onderschrijft vanuit haar verantwoordelijkheid voor cyberveiligheid het belang van goed beveiligde communicatie door encryptie, maar acht het ook van groot belang dat rechtmatige toegang tot communicatie en bewijs voor opsporings- en veiligheidsdiensten mogelijk blijft, in lijn met het MCEV besluit van mei 2020. De operationele noodzaak hiertoe is groot en neemt in een hoog tempo toe. Sinds 2016 (het encryptiestandpunt) is de wereld steeds verder gedigitaliseerd en is de versleuteling en omvang van de communicatie via OTT-communicatiediensten sterk toegenomen. Met als gevolg dat onze opsporings- en veiligheidsdiensten steeds minder toegang daartoe hebben. Ook bedienen steeds meer criminaliteitsvormen zich in toenemende mate van de online communicatiemogelijkheden en zien we een grote verschuiving van off- naar online criminaliteit.
De noodzaak voor het realiseren van toegang tot versleutelde informatie voor de opsporingen is ook in het encryptiestandpunt van het Kabinet uit 2016 opgenomen. Het netto resultaat tot nu toe is echter - ondanks vele inspanningen en wetgevingstrajecten vanuit JenV - dat er steeds minder toegang tot versleutelde communicatie en informatie is.
Een derde belangrijk argument om OTT-communicatiediensten te verplichten om aan de inrichtings- en medewerkingseisen van hoofdstuk 13 te laten voldoen is het ongelijke speelveld dat er is tussen deze diensten en de traditionele telecommunicatiediensten. Ze leveren dezelfde dienst – communicatie tussen personen – maar alleen de telecommunicatiediensten moeten aan die eisen van hoofdstuk 13 van de Tw voldoen. Daar beklagen de telecommunicatiediensten zoals KPN zich ook actief over. Daarnaast vinden we tot op heden de encryptie en andere maatregelen die de telecommunicatiediensten toepassen om

communicatie via hun diensten te beschermen ook niet onveilig. Zij kunnen door de verplichtingen van hoofdstuk 13 Tw – o.a. om aftapbaar te zijn - geen end-to-end encryptie toepassen zoals de OTT-diensten dat doen. Toch hebben zij alsnog voldoende mogelijkheden om onze communicatie adequaat te beschermen tegen het afluisteren door kwaadwillende derden.
JenV erkent dus het dilemma op basis waarvan EZK zich genoodzaakt ziet om het MCEV besluit te heroverwegen, maar ziet daarin geen nieuw argument voor en reden toe. De argumenten – gevolgen voor de versleuteling, alternatieven, Europees traject etc. - zijn ook in het gezamenlijk beleidstraject dat aan het MCEV besluit vooraf is gegaan meegenomen en –gewogen. De keuzes is toen gezamenlijk gemaakt om, ondanks het dilemma, OTT-communicatiediensten in de Tw te verplichten om hun dienst zodanig in te richten dat communicatie daarover door de opsporings- een veiligheidsdiensten afgetapt kan worden.

JenV stelt daarom voor om het MCEV besluit van mei 2020 te herbevestigen en om te zetten in een wetsvoorstel, maar om ter compromis deze wettelijke verplichting voor OTT-communicatiediensten nog niet in werking te laten treden; optie 2 uit de mogelijkheden hierboven. Dan houden we vast aan de normatief duidelijke keuze dat ook OTT-communicatiediensten evenals telecommunicatiediensten, die een zelfde product leveren, aftapbaar moeten zijn. En dus ook evengoed beveiligd kunnen worden. Omdat de bepaling niet in werking treedt heeft deze echter nog geen gevolgen voor de encryptiewijze van OTT-communicatiediensten. Een besluit over het al dan niet in werking laten treden zal dan later, mede gebaseerd op de uitkomsten van de verkenning door de Europese Commissie, door het Kabinet en de Kamers worden genomen. Hiermee nemen we een stapje om uit de impasse te komen die sinds het encryptiestandpunt bestaat en steeds meer gevolgen heeft voor de opsporing en nationale veiligheid. Tevens geeft de overheid daarmee een duidelijk signaal dat zij bepaalt wat veilig is, moet en mag en niet de (grote) technologiebedrijven. Zonder dat meteen een onverantwoorde stap wordt genomen. Mogelijk dat het de technologiebedrijven – waarvan de grootste spelers de rijkste en technologisch meest geavanceerde bedrijven ter wereld zijn – ook welwillender maakt om zelf met proportionele oplossingsvoorstellen te komen, hetgeen ze tot nu toe niet doen.
JenV wijst de deelnemers er wel op dat met optie 2, 3 en 4 uit deze nota de reeds bestaande en steeds verder toenemende ineffectiviteit van interceptie voor opsporings- en veiligheidsdiensten en gevolgen daarvan voor onze veiligheid blijft en daarmee gezamenlijk door de leden van de ACEV en MCEV wordt aanvaard.

<u>Standpunt EZK</u>
Communicatie van OTT-diensten wordt beveiligd door middel van end-to-end encryptie. Hierbij heeft de dienstverlener zelf geen sleutel (lees: toegang) tot de communicatie. De communicatieboodschap wordt op het apparaat van de eindgebruiker pas ontsleuteld. Encryptie is van belang voor de beveiliging van gecommuniceerde en opgeslagen informatie en voor de integriteit van ICT-systemen, die in toenemende mate van belang zijn voor het functioneren van de samenleving (burgers èn bedrijfsleven). Daarmee vormt end-to-end encryptie in het digitale communicatieverkeer een belangrijke waarborg voor de bescherming van privacy en het communicatiegeheim (incl vertrouwelijke bedrijfsinformatie).
EZK erkent volmondig het belang van de digitale opsporing, maar wijst op het kabinetsstandpunt van 2016 dat stelt dat er *"op dit moment geen zicht [is] op mogelijkheden om […] encryptie producten te verzwakken zonder daarmee de veiligheid van digitale systemen die van encryptie gebruik maken te*

compromitteren." Hetzelfde kabinetsstandpunt benadrukt ook dat "*door een technische ingang in een encryptie product te introduceren die het voor opsporingsinstanties mogelijk zou maken versleutelde bestanden in te zien, kunnen digitale systemen kwetsbaar worden voor bijvoorbeeld criminelen, terroristen en buitenlandse inlichtingendiensten."* Dit standpunt is wat EZK betreft nog steeds actueel: technisch gezien is het tot op heden niet mogelijk communicatie via OTT-diensten af te tappen zonder deze systemen kwetsbaar te maken voor misbruik door kwaadwillenden. Bovendien is nog steeds niet helder in kaart gebracht wat de precieze negatieve effecten van ontsleuteling zijn, en is nog niet (afdoende) verkend of er technische mogelijkheden zijn die voldoende rekening houden met de negatieve effecten. De Tweede Kamer heeft meermaals aangegeven dat het sterke encryptie als een belangrijk speerpunt ziet binnen onze samenleving.[1] Inmiddels is de meest recente kabinetsbrief omtrent versleuteld bewijs (14 december jl.) controversieel verklaard.

Om die reden wil EZK inzetten op optie 3: eerst de effecten van een verplichting tot ontsleuteling t.b.v. aftappen in kaart te brengen alvorens wijzigingen in de Tw op te nemen. Dit kan door opvolging te geven aan de EU-raadsverklaring van 14 december jl. waarin de Europese Commissie wordt gevraagd samen met internetdienstverleners en de wetenschap een inventarisatie uit te voeren naar technische mogelijkheden voor rechtmatige toegang tot versleuteld bewijs. Naar aanleiding van de inventarisatie volgen er mogelijk technische oplossingen. Deze dienen beoordeeld te worden aan de hand van noodzakelijkheid, evenredigheid en proportialiteit.

In aanvulling hierop stelt EZK dat een Europese aanpak ook de voorkeur verdient ten behoeve van het belang van een gelijk speelveld op de Europese interne markt, mede gelet op het grensoverschrijdende karakter van OTT-dienstverlening. In de genoemde brief van 14 december jl. aan de Tweede Kamer onderschrijft het kabinet ook dat er een focus moet liggen op onderzoek naar technische oplossingen en dat tevens een Europese aanpak genomen zou moeten worden.[2]

Wat betreft het door JenV aangestipte gelijk speelveld tussen de internationale OTT-dienstverleners en nationale aanbieders van openbare telecommunicatiediensten merkt EZK op dat de dienstverlening (klassieke spraakverkeer en SMS-verkeer) van deze telecommunicatiedienstaanbieders nimmer op sterke encryptie is gestoeld. Destijds was end-to-end encryptie nog niet gebruikelijk, het kan nu niet worden ingevoerd vanwege de bestaande aftapverplichting en het betreft alleen communicatie binnen het eigen netwerk van de nationale aanbieder van openbare telecommunicatiediensten. Bij OTT-dienstverlening gaat het berichtenverkeer over meerdere onbekende (ook buitenlandse) netwerken. Sterke encryptie is nodig om de communicatie van OTT-dienstverleners over deze onbekende netwerken adequaat te kunnen beschermen, anders wordt de communicatie voor derden, waaronder kwaadwillenden, eenvoudig toegankelijk. OTT-spelers, die internationaal actief, zijn zullen technologie niet aanpassen wegens de wensen van enkel Nederland. Indien een dergelijke nationale bepaling van kracht wordt zullen de OTT-dienstverleners naar verwachting hun diensten niet meer aanbieden. Goedwillende gebruikers, consumenten en bedrijfsleven, zullen hierdoor

[1] Kamerstukken II 21 501-02, 2232 (motie Baudet).

[2] Kamerstukken II 21 501-02, 2232(motie Baudet).

benadeeld worden. De Nederlandse gebruikers zullen zich vervolgens wenden tot buitenlandse OTT-aanbieders (die niet behoeven te voldoen aan de Tw). Dit is geen goede ontwikkeling van de Nederlandse digitale economie, noch voor de wens om grip te krijgen op versleutelde communicatie. Een dergelijke mogelijke ontwikkeling onderstreept dat een Europese aanpak sterk prevaleert ten opzichte van een nationale aanpak.

Bijlage
- MCEV beleidsnota '5G en de opsporing'
- Kamerbrief d.d. 14 december 2020 'raadsconclusies over rechtmatige toegang tot versleuteld bewijs'

Ministerie van Justitie en Veiligheid

Dep. VERTROUWELIJK
MCEV

Directoraat-Generaal Rechtspleging en Rechtshandhaving
Directie Rechtshandhaving en Criminaliteitsbestrijding
Criminaliteit en Veiligheid

Turfmarkt 147
2511 DP Den Haag
Postbus 20301
2500 EH Den Haag
www.rijksoverheid.nl/jenv

Contactpersoon
5.1.2.e

T 070 5.1.2.e
F 070 5.1.2.e

Datum
12 december 2019

Ons kenmerk
2883475

Beleidsnota 5G en de opsporing

Doel nota

U wordt verzocht de voorstellen tot benodigde wettelijke aanpassingen te accorderen om te bevorderen dat bestaande noodzakelijke opsporingsmethodieken ook met de uitrol van 5G behouden blijven. Na uw akkoord kan onder coördinatie van de Directie Wetgeving en Juridische Zaken van het ministerie van Justitie en Veiligheid de benodigde aanpassing van wet- en regelgeving worden voorbereid.

Inleiding

Op 11 juni 2019 is de MCEV geïnformeerd over de negatieve gevolgen van de uitrol van 5G voor de opsporing en zijn mitigerende functionele eisen vastgesteld die een juridische basis in wet- en regelgeving moeten hebben. Er heeft vervolgens overleg plaatsgevonden met de Nederlandse telecomaanbieders, waarna de functionele eisen op 27 augustus 2019 akkoord zijn bevonden door de ACEV. Hierop is opdracht gegeven tot het opstellen van een beleidsnota waarin wordt aangegeven of, en zo ja hoe, het wet- en regelgevendkader moet worden geactualiseerd om bestaande noodzakelijke opsporingsmethodieken in de nieuwe 5G netwerken te behouden. Wat voor de opsporingsdiensten geldt, is ook van toepassing op de inlichtingendiensten. In het belang van de nationale veiligheid moet gewaarborgd worden dat ook de inlichtingendiensten toegang blijven behouden tot telecommunicatie via de netwerk- en dienstenaanbieders. Deze nota is opgesteld in de werkgroep 5G en de opsporing onder coördinatie van JenV (DGRR), in nauwe samenwerking met BZK, EZK, Defensie, politie, OM en het Agentschap Telecom.

De opsporingsmethodieken die zijn geanalyseerd zijn interceptie (zowel het tappen als vorderen van gegevens), de inzet van de IMSI-catcher en de stealth SMS. Gegeven de negatieve consequenties voor de effectiviteit van deze bestaande methodieken is het gevoel van urgentie binnen de werkgroep groot. Dit komt ook omdat in de werkgroep is vastgesteld dat een wijziging van de Telecommunicatiewet nodig is en dit geruime tijd in beslag kan nemen. De termijnen waarin aanbieders de uitrol van een (volwaardig) 5G netwerk starten is onzeker. De band die het meest belangrijk is voor 5G en problematisch voor de opsporing, de 3,5GHz band, komt per 1 september 2022 vrij voor mobiele communicatie. Het is noodzakelijk dat de modernisering van de wet- en regelgeving afgerond is voordat 5G volwaardig wordt uitgerold. De benodigde wijzigingen komen voort uit twee kernbeginselen die reeds volgen uit hoofdstuk 13 Telecommunicatiewet:

13.1) 1)Aanbieders van openbare telecommunicatienetwerken en –diensten zijn uitsluitend beschikbaar aan gebruikers indien deze aftapbaar zijn

Directoraat-Generaal Rechtspleging en Rechtshandhaving
Directie Rechtshandhaving en Criminaliteitsbestrijding
Criminaliteit en Veiligheid

Datum
12 december 2019

Ons kenmerk
2883475

13.2 1.) Aanbieders van openbare telecommunicatienetwerken zijn verplicht medewerking te verlenen aan de uitvoering van een bevel tot het aftappen of opnemen van telecommunicatie die over hun telecommunicatienetwerken wordt afgewikkeld.

2.) Aanbieders van openbare telecommunicatiediensten zijn verplicht medewerking te verlenen aan de uitvoering van een bevel tot het aftappen of opnemen van door hen verzorgde telecommunicatie

Functionele eisen
De functionele eisen die worden uitgewerkt zijn:

1. Aanbieders dienen bij een tap (near)realtime een exacte en complete kopie van de data stroom van de communicatie aan te leveren.
2. Aanbieders dienen bij een tap de kopie van de datastroom van de communicatie ontsleuteld aan te leveren.
3. Aanbieders dienen hun dienst of netwerk zodanig in te richten dat unieke identificatie van een device/gebruiker altijd mogelijk is.
4. Aanbieders dienen hun dienst of netwerk zodanig inrichten dat van alle communicatiepaden locatie-informatie geleverd kan worden.
5. De huidige security-eisen gesteld aan tappen blijven ook in de toekomst onverkort van toepassing

Vanaf september 2019 is in de werkgroep geïnventariseerd welke oplossingsrichtingen het meeste draagvlak hebben binnen de werkgroep. In deze inventarisatie stond centraal dat bestaande opsporingsmethodieken effectief inzetbaar moeten blijven voor opsporings- en inlichtingendiensten in 5G netwerken. Hierbij is tevens aandacht besteed aan het niveau van wet- of regelgeving dat zou moeten worden aangepast, aan uitvoeringsconsequenties van betrokken organisaties en er heeft overleg plaatsgevonden met de betrokken aanbieders. De invulling van de functionele eisen is ook besproken met de huidige drie (grote) aanbieders. Specifiek commentaar komt terug in de invulling van de onderstaande eisen. In het algemeen werd in januari door aanbieders betreurd dat OTT-diensten geen medewerkingsverplichting krijgen. Tevens werd door hen benadrukt dat de overheid niet buiten de bestaande wettelijke kaders zou moeten treden. Daarnaast werd door hen toegelicht dat de nationale mogelijkheden om de internationale technologische ontwikkeling te reguleren beperkt zijn. Als laatste werd geopperd dat indien samenwerking tussen netwerk- en dienstenaanbieders nodig is geen bedrijfsgevoelige informatie kan worden gedeeld en het kabinetsstandpunt rond encryptie moet worden gerespecteerd.

Invulling functionele eisen

1.Aanbieders dienen bij een tap (near)realtime een exacte en complete kopie van de data stroom van de communicatie aan te leveren.
Taps moeten kunnen worden gezet op alle toegangs- en communicatiediensten zodat al het verkeer van en naar een device en/of een uniek kenmerk wordt getapt, ongeacht het gebruikte netwerk en ongeacht de netwerkconfiguratie. Bijvoorbeeld ook lokaal in een basisstation of tussen devices afgehandeld verkeer

Deze eis komt onder andere voort uit de eis dat de aanbieder zijn netwerk of dienst inricht zodat afgetapte communicatie onverwijld ter beschikking wordt gesteld aan de bevoegde autoriteit en de kwaliteit van de communicatie,

Directoraat-Generaal Rechtspleging en Rechtshandhaving
Directie Rechtshandhaving en Criminaliteitsbestrijding
Criminaliteit en Veiligheid

Datum
12 december 2019

Ons kenmerk
2883475

verkregen door aftappen, vergelijkbaar is met het origineel.[1] Bij deze eis staan twee problemen centraal. Ten eerste wordt in het huidige wet- en regelgevend kader gesproken over 'openbare telecommunicatienetwerken en openbare telecommunicatiediensten'. Onder 5G wordt het onderscheid tussen openbare en niet-openbare aanbieders diffuser. Ten tweede loopt het communicatieverkeer niet meer per se via het centrale netwerk of basisstation, maar kan dit ook aan de randen van het netwerk worden afgehandeld.

Daarnaast speelt het punt dat het onderbrengen van OTT-diensten onder de medewerkingsverplichting door de geconsulteerde aanbieders wordt aangemoedigd. Zij wijzen erop dat met betrekking tot eisen 2 en 4 samenwerking met deze partijen steeds noodzakelijker is en dat een medewerkingsverplichting nu ontbreekt. Gegeven de gelijksoortige diensten die worden geleverd kan het voorschot dat wordt genomen op het regelen van de aftapverplichting van OTT worden gezien als normalisering van het interceptielandschap die tevens noodzakelijk is voor de toekomstbestendigheid van de aftapbevoegdheid. Ter illustratie, het aantal Nederlandse gebruikers van WhatsApp is gegroeid tot 10 miljoen in december 2014.[2] WhatsApp kent op dit moment geen medewerkingsverplichting.

Advies:
Ad 1) In lijn met de implementatiewetgeving van het Europees wetboek voor elektronische communicatie, de Telecomcode, wordt ook in hoofdstuk 13 van de Telecommunicatiewet het begrip 'elektronische communicatiedienst' gehanteerd. Dit begrip omhelst diverse soorten diensten, waaronder 'nummeronafhankelijke interpersoonlijke communicatiediensten (zogenaamde Over The Top diensten (OTT) zoals WhatsApp en Signal), die nu geen medewerkings- en aftapbaarheidsverplichting kennen in hoofdstuk 13. De werkgroep 5G ziet op het effectief houden van bestaande opsporingsbevoegdheden onder 5G. Echter, gegeven de signalen uit het gesprek met de netwerkaanbieders en de opsporingspraktijk worden de mogelijkheden verkend om nummeronafhankelijke interpersoonlijke communicatiediensten mee te nemen in het wijzigingstraject van 5G. Tenzij dit leidt tot vertraging van de invoering van de benodigde wet- en regelgeving van de functionele eisen.[3]
Bekeken wordt nog in hoeverre de huidige, niet-openbare netwerken, die ook onder de nieuwe definitie van Hoofdstuk 13 komen te vallen, aftapbaar moeten worden gemaakt. Gegeven de compensatieregeling voor aanbieders die meewerken aan de aftapverplichting kan het financiële gevolgen hebben voor de Staat als de betrokken aanbieders hiervoor compensatie eisen.
Ad 2) Het is een implementatiekwestie voor de aanbieder om taps centraal af te kunnen leveren. In regelgeving zoals het Besluit Aftappen kunnen nadere eisen

[1] Art. 2 (d)(f)(i) Besluit aftappen openbare telecommunicatienetwerken en -diensten
[2] TNO e.a. (2016), Study on future trends and business models in communication services, EU DG Home, Brussels
[3] Besloten netwerken hoeven in beginsel niet bij voorbaat te investeren in een aftapfaciliteit of een ontheffing daarvoor aan te vragen. Op dit moment ziet deze eis op aanbieders die nu als 'openbaar telecommunicatienetwerk of openbare telecommunicatiedienst' kunnen worden aangewezen, maar onder 5G niet meer of aanbieders die soortgelijke diensten gaan aanbieden onder 5G. Pas bij een regulier verzoek zullen voorzieningen moeten worden getroffen of worden verzocht om een ontheffing.

Directoraat-Generaal Rechtspleging en Rechtshandhaving
Directie Rechtshandhaving en Criminaliteitsbestrijding
Criminaliteit en Veiligheid

Datum
12 december 2019

Ons kenmerk
2883475

worde gesteld om af te dwingen dat lokaal afgehandeld verkeer nog wel via het netwerk centraal geleverd kan worden bij een tap.

2. Aanbieders dienen bij een tap de kopie van de datastroom van de communicatie ontsleuteld aan te leveren.

Een aanbieder dient er daarom voor te zorgen de beschikking te hebben over (sleutel) materiaal om te ontsleutelen. De ontsleuteling geldt zowel voor de inhoud van de tap (content) als voor alle tap gerelateerde gegevens (zoals verkeers-gegevens en IRI). Roaming scenario's dienen gelijk te worden behandeld als non- roaming scenario's.

Voor nationale aanbieders van netwerken en diensten geldt dat telecommunicatie die wordt verkregen door middel van aftappen door de aanbieder wordt ontdaan van eventueel door hem aangewende cryptografie en andere door hem aangewende bewerkingen en als zodanig aan de in de bijzondere last vermelde personen of instanties doorgegeven.[4] Voor 'andere door hem aangewende bewerkingen' kan worden gedacht aan het aanstellen van derde partijen om telecommunicatie te versleutelen.

Het ontsleuteld aanleveren van communicatie wordt problematisch wanneer een netwerkaanbieder communicatie afhandelt van een andere (buitenlandse) dienstenaanbieder. Dit wordt ook wel 'roaming' genoemd. Indien deze andere aanbieder zijn communicatie aanvullend versleutelt verliest de netwerkaanbieder toegang tot deze data. Het is de verwachting dat ook onder 5G deze aanvullende versleuteling zal worden aangebracht. Het realtime bewijs vorderen (of tappen) van de buitenlandse dienstenaanbieder is geen realistische optie aangezien Nederland geen rechtsmacht heeft grensoverschrijdend te handhaven en een rechtshulpverzoek geen geschikt kanaal is. De onvermijdelijke vertraging tussen het indienen van een rechtshulpverzoek, het in behandeling nemen daarvan door een andere (buitenlandse) justitiële autoriteit en het uiteindelijk zetten en doorsturen van een tap naar de Nederlandse autoriteiten, zou onacceptabele risico's opleveren. Dit geldt temeer daar de betreffende communicatie in Nederland zelf plaatsvindt en (kwaadwillende) subjecten de noodzakelijke activiteiten van opsporings- en veiligheidsdiensten zouden kunnen frustreren door simpelweg een buitenlandse simkaart te gebruiken.

In de ACEV nota van 29 juli 2019 staat dat aanvullende regelgeving nodig is om te voorkomen dat inhoudelijke communicatie van subjecten met een buitenlandse simkaart straks niet langer toegankelijk is voor de opsporing. Conform verzoek zijn verschillende oplossingsrichtingen uitgewerkt en voorzien van een advies.

2.1 Oplossingsrichtingen

In overleg met de aanbieders is naar voren gekomen dat er steeds meer digitale diensten over een netwerk worden geleverd waar geen contractuele relatie mee bestaat voor de kwaliteit van de dienstverlening. Een voorbeeld hiervan zijn de eerdergenoemde OTT-diensten (de problematiek die hieruit voortkomt is eerder in deze nota beschreven). Van netwerkaanbieders wordt bijvoorbeeld niet verwacht dat zij communicatie leveren van diensten die buiten de reikwijdte van wet- en regelgeving vallen van hoofdstuk 13.

[4] Art. 2(e) van het Besluit Aftappen openbare netwerken en –diensten dat telecommunicatie,

Directoraat-Generaal Rechtspleging en Rechtshandhaving
Directie Rechtshandhaving en Criminaliteitsbestrijding
Criminaliteit en Veiligheid

Datum
12 december 2019

Ons kenmerk
2883475

Voor mobiele communicatienetwerken dient de netwerkaanbieder – anders dan bij OTT-diensten waarbij het transport van signalen over het internet verloopt – via een overeenkomst voor het gebruik van zijn netwerk door derden de aftapbaarheid te borgen. Hierdoor wordt voor de telecommunicatiediensten van derden dezelfde functionaliteit geleverd als voor eigen gebruikers. Dit worden 'roamingovereenkomsten' genoemd. In deze overeenkomsten kunnen aanvullende afspraken worden gemaakt over de wijze waarop telecommunicatiediensten worden afgehandeld.

Bij het besluit welke optie wordt uitgewerkt zodat opsporingsmethodieken effectief blijven, is belangrijk dat een bevel tot het aftappen van ontsleutelde communicatie handhaafbaar is. Tevens worden belangen van aanbieders afgewogen en wordt bezien hoe de optie zich verhoudt tot binnenlands beleid, bijvoorbeeld het kabinetsstandpunt over encryptie. In zijn algemeenheid kan worden gesteld dat er twee manieren zijn om binnenkomend verkeer uit het buitenland af te handelen en ontsleuteld te kunnen tappen: Local Breakout Scenario en Home-routing.

2.1.1 Local breakout scenario

Bij Local Breakout wordt afgesproken dat het binnenkomende verkeer verder wordt afgehandeld door een binnenlandse netwerkaanbieder. Bij deze variant blijft het communicatieverkeer van de buitenlandse gebruiker inzichtelijk voor de binnenlandse aanbieder. Voor de opsporing bestaat het voordeel dat de communicatie lokaal wordt versleuteld en afgehandeld en dus voor de Nederlandse aanbieder beschikbaar is. In beginsel bestaat bij aanbieders terughoudendheid bij deze optie, omdat dit wordt gezien als verdere nationale regulering van de internationale telecommarkt. Immers, in dit scenario kunnen gebruikers alleen de diensten geleverd krijgen die in de desbetreffende lidstaat worden aangeboden. Dat aanbod kan minder zijn dan in het thuisland van de gebruiker. Dat heeft mogelijk ook consequenties voor de afscherming van de tap.

2.1.2 *Home Routing*

Bij Home-routing wordt de communicatie weliswaar over het binnenlandse netwerk geleid, maar wordt de dienst vanuit het land van herkomst verzorgd. Indien de communicatiedienst door de aanbieder uit het land van herkomst extra wordt versleuteld is dit voor de binnenlandse netwerkaanbieder niet inzichtelijk. Er zouden afspraken in de (roaming)overeenkomsten moeten worden gemaakt om aanvullende versleuteling niet te activeren en het verkeer door de binnenlandse netwerkaanbieder te laten beveiligen.

2.2 *Weging van oplossingsrichtingen*

Ten eerste blijft een afspraak in (roaming) overeenkomsten tussen netwerk- en dienstaanbieders kwetsbaar voor de opsporing en lastig voor het toezicht. Deze overeenkomsten worden gesloten tussen twee private partijen binnen het civielrechtelijke domein. Een partij zou daarom moeten aangeven op welke wijze door hem uitvoering is gegeven aan zijn verplichting om te borgen dat de aftapbaarheid van de telecommunicatiediensten voor derden dezelfde functionaliteit geeft als voor zijn eigen gebruikers.
Om ook toezicht hierop te kunnen houden is een wettelijke grondslag nodig die het aangeven van deze wijze van uitvoering voorschrijft, althans de verplichting bij de aanbieder neerlegt om aan te tonen dat hier uitvoering aan is gegeven, waardoor het Agentschap Telecom toezicht kan houden. Het betreft hier een

Directoraat-Generaal Rechtspleging en Rechtshandhaving
Directie Rechtshandhaving en Criminaliteitsbestrijding
Criminaliteit en Veiligheid

Datum
12 december 2019

Ons kenmerk
2883475

zorgplicht. Indien een partij hier niet aan voldoet, is vervolgens het handelingsperspectief complex. Het weigeren van dienstverlening door de betreffende partij af te sluiten heeft verregaande consequenties voor alle klanten van deze aanbieder in het bezoekende land en in algemene zin voor het vrije verkeer van diensten in Europa.

Ten tweede bestaat in de werkgroep een verschil van mening over hoe het uitschakelen van aanvullende versleuteling zich verhoudt tot het kabinetsstandpunt inzake encryptie van 2016. EZK is van mening dat deze voorwaarde op gespannen voet staat met het standpunt dat er in Nederland geen wettelijke beperkingen zouden moeten komen voor de ontwikkeling, beschikbaarheid en toegang tot encryptie en staat ook op gespannen voet met Europese privacybepalingen. Echter, vanuit de technische standaardisatiegremia komt naar voren dat de veiligheid van het 5G netwerk zodanig is dat aanvullende versleuteling niet hoeft te worden aangezet. OM, politie, BZK, Def en DGRR zijn van mening dat de encryptie niet structureel wordt verzwakt, aangezien de encryptie van binnenlandse aanbieders wordt toegepast. Daarnaast doet deze regeling recht aan het uitgangspunt van rechtmatige toegang tot bewijs dat ook onderdeel is van het encryptiestandpunt.
Ten derde wordt door de aanbieders gesuggereerd dat deze regulering vanuit de EU moet komen. EZK staat hierbij op het standpunt dat gezien het grensoverschrijdende karakter van deze oplossing, eerst binnen Europa consensus dient te worden gevonden over de aanpak. Regelgeving voor de aftapbevoegdheid betreft echter een nationale bevoegdheid. Gegeven het nationale opsporing- en veiligheidsbelang zien DGRR, OM, politie, IenV diensten, BOD'en geen oplossing in het afwachten van de Europese route. Zij moedigen Europese regelgeving aan, echter bedacht moet worden dat er vele niet-Europese aanbieders actief zijn op de Nederlandse markt en het tijdsgewricht waarin oplossingen in Nederland nodig zijn is relatief kort.

Advies:
Voor de oplossing met betrekking tot buitenlandse dienstverleners of andere netwerkaanbieders wordt geadviseerd een nadere verkenning uit te voeren naar de praktische uitvoering van de oplossingsrichtingen. Deze verkenning ziet ten eerste op de toepassing van versleuteling van communicatie bij de verschillende technische oplossingsrichtingen. Hierbij wordt bijvoorbeeld inzicht verkregen in hoeverre eventuele (aanvullende) encryptie, en de extra bescherming die dit biedt, zich verhoudt tot rechtmatige toegang tot informatie. Ten tweede worden de internationaal privaatrechtelijke gevolgen van deze oplossingsrichtingen verkend. Dit is bijvoorbeeld van belang voor de handhaafbaarheid een oplossing. Het belang van de consequenties voor de handhaafbaarheid ligt met name in het gegeven dat (roaming)afspraken tussen partijen plaatsvinden binnen het internationaal privaatrechtelijke domein en dat ten aanzien van de totstandkoming van overeenkomsten, alsmede de nakoming en afdwingbaarheid daarvan, binnen dit domein eigenstandige wettelijke regels en beginselen gelden. De verkenning stelt de beleidsdirecties van EZK en JenV beter in staat een oordeel te vormen over de verhouding van de oplossingsrichting tot het kabinetsstandpunt op encryptie en maakt inzichtelijk wat men van Nederlandse aanbieders kan verwachten.

De verkenning dient snel te worden afgerond om geen vertragend effect op de uitwerking van de wet- en regelgeving te hebben. Het opsporingsbelang dat is

Directoraat-Generaal Rechtspleging en Rechtshandhaving
Directie Rechtshandhaving en Criminaliteitsbestrijding
Criminaliteit en Veiligheid

Datum
12 december 2019

Ons kenmerk
2883475

geformuleerd in functionele eis twee is het uitgangspunt bij deze verkenning en staat niet ter discussie.

3. Aanbieders dienen hun dienst of netwerk zodanig in te richten dat unieke identificatie van een device/gebruiker altijd mogelijk is.

Aanbieders dienen derhalve medewerking te verlenen om de volgende functionaliteiten te faciliteren:
a. Het real time op een gegeven locatie bepalen van het unieke kenmerk (van een device), aan de hand waarvan een gebruiker van een communicatiedienst kan worden geïdentificeerd in het netwerk.
b. Het real time bepalen van de aanwezigheid van bepaalde unieke kenmerken in een bepaald gebied.
c. Het real time nauwkeurig kunnen bepalen van de feitelijke locatie van een device.

Kern van het probleem is dat de identiteit van een gebruiker van een telefoon, de IMSI, niet meer wordt verzonden over de radioweg. De permanente identiteit blijft op het apparaat, een versleutelde identiteit wordt verzonden over de radioweg tezamen met een tijdelijke identiteit. Deze identiteiten moeten door de opsporing zelfstandig te koppelen zijn om identificatie en lokalisatie plaats te laten vinden. Voor behoud van de functionaliteit genoemd in functionele eis 3 is nodig dat de *credentials* van het netwerk beschikbaar worden gesteld zodat de catcher zich als basisstation kan laten identificeren. Welke *credentials* en/of aanvullende gegevens nodig zijn wordt nog onderzocht in de diverse standaardisatiegremia. Naar verwachting heeft men hier nog een half jaar voor nodig. De verstrekking van de benodigde informatie moet op zodanige wijze gebeuren dat de opsporing een eigenstandige mogelijkheid heeft om apparaten te lokaliseren en identificeren. Dit is nodig omdat rekening gehouden moet worden met gevallen waarin het doelwit geen bereik heeft, bijvoorbeeld midden in een natuurgebied, een afgelegen loods, etc. Omdat onduidelijk is welke gegevens de opsporing nodig heeft en of deze vallen onder de definitie van art. 13.4 Tw is onduidelijk of de Tw reeds een grondslag biedt om een medewerkingsverplichting voor de aanbieder uit te werken in een apart besluit.

Advies: Op dit moment is het nog onduidelijk welke gegevens nodig zijn zodat de opsporing zelfstandig een verdachte kan identificeren en lokaliseren. Daarom is onduidelijk of de Telecommunicatiewet moet worden aangepast om een medewerkingsverplichting te creëren voor aanbieders, of dat deze in een apart besluit vorm kan krijgen. Er wordt geadviseerd de beleidsnota niet te vertragen tot hierover duidelijkheid bestaat, maar deze afweging mee te nemen in het wetgevingsproces. Met het accorderen van deze nota blijft het uitgangspunt dat de opsporing een eigenstandige mogelijkheid houdt om apparaten te lokaliseren en identificeren en voorts dat netwerkaanbieders in voorkomende gevallen medewerking verlenen.

4. Aanbieders dienen hun dienst of netwerk zodanig inrichten dat van alle communicatiepaden locatie-informatie geleverd kan worden.

De locatie van gebruikers moet real-time (en historisch indien beschikbaar voor de eigen bedrijfsvoering) kunnen worden bepaald, tenminste op antenne niveau. Onder het begrip antenne valt ook bijvoorbeeld een radiocel en een zendmast.

Een aanbieder genoemd in de Regeling aftappen openbare telecommuncienetwerken en –diensten moet onverwijld uitvoering geven aan een

Directoraat-Generaal Rechtspleging en Rechtshandhaving
Directie Rechtshandhaving en Criminaliteitsbestrijding
Criminaliteit en Veiligheid

Datum
12 december 2019

Ons kenmerk
2883475

bijzondere last.[5] Verder is voorgeschreven dat locatiebepalingen moeten worden overgeleverd en dat telecommunicatie en identificerende gegevens uitsluitend gekoppeld ter beschikking worden gesteld.[6]
In 5G-netwerken is het niet langer vanzelfsprekend dat de dienstaanbieder dezelfde partij is als de netwerkaanbieder. Tot nog toe is dit veelal wel het geval, waardoor een tap op een communicatiedienst (bellen) kan worden verrijkt met netwerkinformatie, waaronder locatiegegevens. Om de huidige functionaliteit te behouden zal een dienstaanbieder die gebruik maakt van het netwerk van een andere partij moeten worden verplicht in zijn contracten met netwerkaanbieders te bepalen dat deze laatsten, in geval van een tap op een gebruiker van de dienstaanbieder, locatie-informatie uit het netwerk aanleveren opdat de dienstaanbieder die informatie gecorreleerd met zijn eigen tapgegevens kan aanleveren. Aanbieders geven aan dat deze verplichting tot medewerking niet kan gelden voor OTT-diensten en dat men geen bedrijfsgevoelige informatie wil overdragen aan concurrenten. In reactie hierop kan worden aangegeven dat, voor zover dit al wordt gevraagd, bedrijven hier onderling nadere afspraken over kunnen maken.

Advies: De koppeling die nu reeds plaatsvindt moet ook onder 5G kunnen worden gemaakt. In de Regeling aftappen openbare telecommunicatienetwerken en –diensten wordt een verplichting geïntroduceerd dat de ontvanger van een bevel, hetzij een dienstaanbieder of netwerkaanbieder, de inhoud van de elektronische communicatiesessie deelt gepaard met de locatiegegevens met medewerking van de benodigde partij. Om dit te bewerkstelligen wordt ook een medewerkingsverplichting geïntroduceerd om deze informatie te leveren aan de ontvanger van een bevel, zowel voor de dienstenaanbieder richting de netwerkaanbieder en vice versa. Dit betreft een actualisering van de eis in artt. 10 en 11 (c) van de Regeling aftappen openbare telecommunicatienetwerken en –diensten dat telecommunicatie en identificerende gegevens gekoppeld worden voor de situatie onder 5G. Bij een eventuele actualisering zal aandacht zijn voor het kostenaspect.

5. De huidige security-eisen gesteld aan tappen blijven ook in de toekomst onverkort van toepassing

Dit is onafhankelijk van het gebruikte netwerk en ongeacht de netwerkconfiguratie.

De beveiligingsvereisten zijn voldoende en techniekneutraal vastgelegd in het Besluit beveiliging gegevens telecommunicatie. Dit onderwerp wordt ook meegenomen in de standaardisatiegremia, zodat er apparatuur wordt gebouwd die voldoet aan de vereisten. Er is geen discussie over deze eis, wel bestaan er onderlinge verschillen van inzicht tussen de aanbieders over de invulling hiervan. Dit onderwerp zal verder bilateraal worden besproken met aanbieders.

Advies: Gesprekken met aanbieders hebben niet geleid tot benodigde aanpassingen in regelgeving. Men kan in het wetgevingstraject ruimte bieden om eventuele zorgen te adresseren.

[5] Art. 3 ev. Regeling aftappen openbare telecommunicatienetwerken en -diensten

[6] Art. 10 en 11 Regeling aftappen openbare telecommunicatienetwerken en -diensten

Directoraat-Generaal Rechtspleging en Rechtshandhaving
Directie Rechtshandhaving en Criminaliteitsbestrijding
Criminaliteit en Veiligheid

Datum
12 december 2019

Ons kenmerk
2883475

Bijlage:

Leden van de werkgroep: DGRR, DJOA, DWJZ JenV, ministeries van AZ, EZK, Def, en BZK, plus het Agentschap Telecom, de Politie, OM, bijzondere opsporingsdiensten (FIOD, KMAR), PIDS

Hieronder vindt u het juridisch kader dat daarvoor is geanalyseerd.

Bevoegdheid opsporing/ I&V	Verplichting telecomaanbieder	Uitwerking AMVB	Regeling
Wetboek van Strafvordering	Telecommunicatie wet hoofdstuk 13	Besluit aftappen openbare telecommunicatien etwerken en -diensten	Regeling aftappen openbare telecommunicatienet werken en -diensten
WIV 2017		Besluit bijzondere vergaring nummergegevens telecommunicatie	Vrijstellingsregeling afwijkend gebruik frequentieruimte Justitie; Vrijstellingsregeling afwijkend gebruik frequentieruimte IVD
		Besluit verstrekking gegevens telecommunicatie	
		Frequentiebesluit 2013	
		Besluit beveiliging gegevens telecommunicatie	

Van: 5.1.2.e
Verzonden: maandag 8 februari 2021 11:38
Aan: 5.1.2.e
CC: 5.1.2.e
Onderwerp: RE: 210402 GA ACEV aftappen 5.1.2.e 33064 5.1.2

Categorieën: Categorie Rood

Mooi zo!

5.1.2.e
Directie Digitale Economie
Ministerie van Economische Zaken en Klimaat

Tel: +31 6 5.1.2.e
Mail: 5.1.2.e @minezk.nl
Web: Telecommunicatie | Rijksoverheid.nl

Van: 5.1.2.e
Verzonden: maandag 8 februari 2021 10:59
Aan: 5.1.2.e
CC: 5.1.2.e
Onderwerp: 210402 GA ACEV aftappen 5.1.2.e 33064 5.1.2.

Zie nu bullet 4 en 6

Van: 5.1.2.e @minaz.nl>
Verzonden: dinsdag 9 februari 2021 11:53
Aan: 5.1.2.e
Onderwerp: RE: ACEV nota OTT/aftappen

Helder verhaal :)

Van: 5.1.2.e @minezk.nl>
Datum: dinsdag 09 feb. 2021 11:21 AM
Aan: 5.1.2.e @minaz.nl>, 5.1.2.e @minaz.nl>
Onderwerp: ACEV nota OTT/aftappen

Ha 5.1.2.e en goedemorgen 5.1.2.e

Fijn vanochtend weer even bij te kletsen 5.1.2.e Goed te horen dat het jou, 5.1.2.e en 5.1.2.e zo goed gaat, en goed dat je weer terug op het AZ-honk bent.

Ik borduur even voort op waar 5.1.2.e en ik vanochtend eindigden, te weten het dossier OTT/aftappen die donderdag weer op de ACEV staat. Wilde jullie hier een paar punten over meegeven:

- Vooropgesteld: alle begrip voor de wens van J&V om ook versleutelde digitale communicatie te kunnen aftappen. Duidelijk dat daar stappen in moeten worden gezet.

- Zorg EZK zit hem in dus niet in de vraag óf we hier iets mee moeten/willen, maar in de wijze waarop J&V daar invulling aan wenst te geven. En daar zit 'm nu juist de kneep: de wetswijziging die JenV bepleit maakt aftappen mogelijk maar doet afbreuk aan de integriteit van het encryptiestelsel, wat leidt tot een aantal grote bezwaren (zie de nota voor nadere toelichting, maar trefwoorden zijn privacy, communicatiegeheim, en kwaadwillenden zoals spionagediensten en criminelen die meeliften op de verzwakking).

- Die zorg leeft niet alleen bij EZK: het is een gevoelige kwestie, ook in de Kamer. De Kamerbrief van JenV d.d. 14 december omtrent versleuteld bewijs is dan ook controversieel verklaard. Daarmee ligt een wetswijziging, ook al voer je die vervolgens niet meteen uit (JenV's optie 2), niet voor de hand. Kamer gaat hier geheid voor liggen (met D66 als coalitiepartij die een motie over het belang van sterke encryptie heeft gesteund).

- Voorkeursoptie is om die reden optie 3: laten we eerst nader onderzoek verrichten inzake de technische mogelijkheden en de effecten van een verplichting tot ontsleuteling t.b.v. aftappen alvorens we wetgeving invoeren. Niet om niets te doen (sterker nog: NL kan CIE aansporen hier met prioriteit werk van te maken, kunnen we zichtbaar op zijn) maar om te zorgen dat, zodra er weer een missionair kabinet zit, een geïnformeerd besluit kan worden genomen. Bovendien trekken we dan samen op met de andere EU-lidstaten, wat ook bevorderlijk voor een Europees gelijk speelveld (OTT-aanbieders als Whatsapp zijn natuurlijk overal aanwezig en gaan niet obv alleen NL wetgeving hun systemen aanpassen).

Bovenstaande is de kern van de inzet van EZK as do in de ACEV. Wilde jullie deze punten niet onthouden, hopelijk vallen ze in vruchtbare aarde. Hoe dan ook hoop ik, zoals besproken met 5.1.2.e vanmorgen, constructief met jullie samen te kunnen werken op de diverse telecom, digitale en cyberdossiers; weet dat jullie mij bij EZK altijd kunnen aanpingen!

Hartelijke groet,
5.1.2.e

5.1.2.e
Directie Digitale Economie
Ministerie van Economische Zaken en Klimaat

Tel: +31 6 5.1.2.e
Mail: 5.1.2.e @minezk.nl
Web: Telecommunicatie | Rijksoverheid.nl

Dit bericht kan informatie bevatten die niet voor u is bestemd. Indien u niet de geadresseerde bent of dit bericht abusievelijk aan u is toegezonden, wordt u verzocht dat aan de afzender te melden en het bericht te verwijderen. De Staat aanvaardt geen aansprakelijkheid voor schade, van welke aard ook, die verband houdt met risico's verbonden aan het elektronisch verzenden van berichten.
This message may contain information that is not intended for you. If you are not the addressee or if this message was sent to you by mistake, you are requested to inform the sender and delete the message. The State accepts no liability for damage of any kind resulting from the risks inherent in the electronic transmission of messages.

Van: 5.1.2.e
Verzonden: dinsdag 9 februari 2021 13:21
Aan: 5.1.2.e
CC: 5.1.2.e
Onderwerp: ACEV aftappen OTT GA
Bijlagen: 210402 GA ACEV na versie aftappen v2.docx

Hoi 5.1.2.e

Bijgaand inbreng van DE m.b.t. geannoteerde agenda voor 5.1.2.e Het is het stukje over aftappen en OTT's.

In geval van vragen/opmerkingen hoor ik het graag.

Gr.

5.1.2.e

Directoraat-Generaal Bedrijfsleven en Innovatie
.....
Ministerie van Economische Zaken
Bezuidenhoutseweg 73 | 2594 AC | Den Haag
Postbus 20401 | 2500 EK | Den Haag
.....
T: +31 65.1.2.e
E: 5.1.2.e @minez.nl
.....

Van: 5.1.2.e
Verzonden: woensdag 10 februari 2021 21:11
Aan: 5.1.2.e
CC: 5.1.2.e
Onderwerp: Re: ACEV nota OTT/aftappen

Categorieën: Categorie Rood

Eens, dat zou idd het beste zijn maar helaas gaan wij daar niet over.

Hoe dan ook, denk dat wij echt ons beste beentje hebben voorgezet in aanloop naar de acev morgen. Heb 5.1.2.e net gemaild met korte wrap-up van onze outreach de afgelopen dagen zodat hij weet wat we hebben gedaan; was hij zeer erkentelijk voor.

Nu is het even out of our hands; het speelveld ligt echt verdeeld dus het is nog geen gelopen race maar we zijn zeker niet kansloos. We gaan het zien!

5.1.2.e

Verstuurd vanaf mijn iPhone

Op 10 feb. 2021 om 17:40 heeft 5.1.2.e @minezk.nl> het volgende geschreven:

5.2.1

Van: 5.1.2.e @minezk.nl>
Verzonden: woensdag 10 februari 2021 17:34
Aan: 5.1.2.e @minezk.nl>; 5.1.2.e @minezk.nl>; 5.1.2.e @minezk.nl>
Onderwerp: RE: ACEV nota OTT/aftappen

BZK krijgt voorbereiding van AIVD en ook van Constitutionele Zaken, zij nemen beide (tegenstrijdige) punten maar gingen mij nog niet vertellen wat de inbreng gaat worden. Snap ik wel. Ik heb onze inzet gedeeld en daar was begrip voor btw. Heb jij nog meer gehoord van je contact 5.1.2.e

---

Van: 5.1.2.e @minezk.nl>
Verzonden: woensdag 10 februari 2021 17:22
Aan: 5.1.2.e @minezk.nl>; 5.1.2.e @minezk.nl>; 5.1.2.e @minezk.nl>
Onderwerp: RE: ACEV nota OTT/aftappen

Van bzk iets terug gehoord ?

Met vriendelijke groet,

5.1.2 e
Digitale Veiligheid / ePrivacy

T : +31-70 - 5.1.2.e
M : +31 6 - 5.1 2.e

Van: 5.1.2.e @minezk.nl>
Verzonden: woensdag 10 februari 2021 16:58
Aan: 5.1.2.e @minezk.nl>; 5.1.2.e @minezk.nl>
Onderwerp: RE: ACEV nota OTT/aftappen

Collega's,

Ter info nog, ik heb gisteren BZ-counterpart 5.1.2.e een soortgelijke mail gestuurd (dus heb 'm even van je gejat 5.1.2.e Hij was hier blij mee en voor BZ is het punt m.b.t. het 'controversiële' een big deal btw.

Benieuwd naar morgen

Gr

5.1 2.e

Van: 5.1.2.e @minezk.nl>
Verzonden: dinsdag 9 februari 2021 11:30
Aan: 5.1.2.e @minezk.nl>; 5.1.2.e @minezk.nl>; 5.1.2.e @minezk.nl>
Onderwerp: FW: ACEV nota OTT/aftappen

Zie hier de mail die ik net aan AZ stuurde.

Van: 5.1.2.e
Verzonden: dinsdag 9 februari 2021 11:21
Aan: 5.1.2.e .
Onderwerp: ACEV nota OTT/aftappen

Reeds beoordeeld in dit verzoek

Reeds beoordeeld in dit verzoek

74

Ministerie van Economische Zaken
en Klimaat

ADVIES

Aan de Staatssecretaris

Directoraat-generaal
Bedrijfsleven & Innovatie
Directie Digitale Economie

Auteur
5.1.2.e
T 070 [redacted]
5.1.2.e @minezk.nl

Datum
17 februari 2021

Kenmerk
DGBI-DE / 21042217

Bhm: 21047718

5.1.2.e

Bijlage(n)
3

nota

MCEV: aftappen Over-The-Top dienstverleners

Parafenroute
5.1.2.e

14/2/21 5.2.1
5.2.1
5.1.2.e

Aanleiding

JenV zet erop in dat er in de MCEV van 26 februari 2021 besloten wordt om de verplichting omtrent het aftappen van OTT-dienstverleners op te nemen in een bredere aanpassing van de Telecommunicatiewet inzake de aftapbevoegdheden van de opsporing. EZK is het hier niet mee eens. In voorliggende nota zijn de standpunten van beide departementen opgenomen (zie bijgaand), met daarbij een viertal opties voor follow-up. De MCEV wordt gevraagd met één van deze opties in te stemmen.

Advies

U wordt geadviseerd om aan te geven dat EZK een sterke voorkeur heeft voor optie 3. U kunt daarbij ter onderbouwing de volgende argumenten inbrengen:

- U kunt aangeven dat EZK in algemene zin begrip heeft voor de wens van JenV om ook versleutelde digitale communicatie te kunnen aftappen, maar dat de wijze waarop J&V daar invulling aan wenst te geven (opties 1 en 2 doen afbreuk aan de integriteit van encryptie) niet de steun van EZK kan dragen.
- U kunt wijzen op nieuwe en relevante ontwikkelingen sinds mei 2020: (1) er is een Europese aanpak aangekondigd dat de moeite van het verkennen waard is, en (2) het controversieel verklaren van het dossier maakt het politiek uitermate risicovol om deze wetswijziging zo door te zetten.
- Optie 3 betekent nadrukkelijk geen afstel maar is gericht op het nemen van een geïnformeerd besluit, met meer draagvlak en in samenspraak met de andere EU-lidstaten en bedrijfsleven/wetenschap: eerst worden de uitkomsten van de (aangekondigde) inventarisatie op EU-niveau inzake technische mogelijkheden en de effecten van een verplichting tot ontsleuteling t.b.v. aftappen in kaart gebracht. Vervolgens kan er een gegrond politiek besluit genomen worden om OTT-dienstverleners al dan niet af te tappen.

Spreekpunten

- Vooropgesteld: alle begrip voor de wens van J&V om ook versleutelde digitale communicatie te kunnen aftappen. Duidelijk dat daar stappen in moeten worden gezet. Ik zie dat zelf ook zo.

Ontvangen BBR

5.2.1

5.2.1

Directoraat-generaal
Bedrijfsleven & Innovatie
Directie Digitale Economie

Kenmerk
DGBI-DE / 21042217

- Mijn zorg zit hem in dus niet in de vraag óf we hier iets mee moeten/willen, maar in de wijze waarop J&V daar invulling aan wenst te geven. Want daar zit 'm nu juist de kneep: de wetswijziging die JenV bepleit maakt aftappen mogelijk maar doet afbreuk aan de integriteit van het encryptiestelsel, wat leidt tot een aantal grote zorgen en bezwaren.
- Deze staan verwoord in de nota, maar in het kort gaan die over privacy en het communicatiegeheim, terwijl er ook zorgen bestaan juist ook over de verzwakking van de veiligheid van het versleutelde digitale verkeer, aangezien kwaadwillenden zoals spionagediensten en criminelen kunnen meeliften op de verzwakking in het encryptiestelsel die als uitvloeisel van dit wetsvoorstel moet worden aangebracht om te kunnen tappen.
- Het gaat in deze discussie dus niet alleen om een afweging tussen veiligheid (opsporing) en privacy. In dit geval gaat het om sterke encryptie OF encryptie die voor een ieder makkelijk toegankelijk is omdat sterke encryptie zoals end-2-end encryptie, dan de facto verboden wordt.
- Ik wil benadrukken dat die zorgen niet alleen bij EZK leven: het is een gevoelige kwestie, in het publieke debat maar ook in de Kamer. De Kamerbrief van JenV d.d. 14 december omtrent versleuteld bewijs is dan ook controversieel verklaard.
- Daarmee ligt een wetswijziging, ook al voer je die vervolgens niet meteen uit (JenV's optie 2), niet voor de hand. 5.2.1
- Daarom pleit ik voor optie 3: laten we eerst nader onderzoek verrichten inzake de alternatieve technische mogelijkheden en de effecten van een verplichting tot ontsleuteling t.b.v. aftappen, vóórdat we wetgeving invoeren.
- Niet om niets te doen, sterker nog: NL kan de Europese Commissie aansporen hier met prioriteit werk van te maken; daar kunnen we actief en zichtbaar op zijn. Maar wèl om te zorgen dat er, zodra er weer een missionair kabinet zit, een geïnformeerd besluit kan worden genomen waar de Kamer zich achter kan scharen.
- Tot slot: bovendien trekken we dan samen op met de andere EU-lidstaten, wat ook bevorderlijk voor een Europees gelijk speelveld.

5.2.1

Kernpunten
J&V ontwerpt een wetsvoorstel welke de huidige aftapmogelijkheden dient te borgen bij de invoering van 5G. In dit wetsvoorstel wil J&V ook een verruiming van de bevoegdheden, namelijk het kunnen aftappen van Over-The-Top-(OTT) dienstverleners. OTT-dienstverleners dienen daarbij de opgevraagde communicatie te ontsleutelen.

De MCEV heeft 19 mei 2020 ingestemd met de 'beleidsnota 5G en de opsporing' waarin onder andere deze verruiming is opgenomen. EZK erkent dan ook een rol van OTT-dienstverleners inzake aftappen. Echter indien dit ook voor OTT-dienstverleners een verplichting tot ontsleuteling omhelst heeft dit negatieve effecten. Daarmee wordt afgeweken van het kabinetsstandpunt van 2016 waarin is geconcludeerd dat een wettelijke inperking van het gebruik van encryptie niet mogelijk is zonder de veiligheid van digitale systemen die van encryptie gebruik maken te compromitteren.

Wat EZK (en een Kamermeerderheid) betreft is het kabinetsstandpunt uit 2016 nog steeds actueel. Daar komt bij dat er recentelijk twee nieuwe ontwikkelingen zijn die pleiten voor een heroverweging van het besluit van de MCEV van mei 2020:

- eind 2020 zijn er EU-Raadsconclusies over dit specifieke thema aangenomen, waarin de lidstaten de Europese Commissie hebben gevraagd om samen met internet dienstverleners en de wetenschap een inventarisatie uit te voeren naar technische mogelijkheden voor rechtmatige toegang tot versleuteld bewijs, zonder de veiligheid van encryptie te compromitteren;
- de Kamer heeft het onderwerp kort na de val van het kabinet controversieel verklaard.

Vanwege dit verschil van inzicht is bijgaande nota opgesteld vanuit de wens van JenV deze patstelling te doorbreken. JenV stuurt aan op optie 2, terwijl EZK de voorkeur uitspreekt voor optie 3 5.2.1 .

5.2.1

Toelichting
Politiek-procedureel:

- U kunt centraal stellen dat encryptie (in bijzonder maatregelen die encryptie aantasten) uitermate gevoelig ligt in de Kamer. Een meerderheid in de Kamer, inclusief coalitiepartij D66, hecht veel waarde aan encryptie, privacy en borging van betrouwbaarheid van communicatiesystemen en heeft november jl. nog een motie aangenomen welke het belang van sterke encryptie voor communicatie tussen burgers onderschrijft.[1]

[1] Kamerstukken II, 21501-02, nr. 2232 (motie Baudet)

- De Minister van JenV onderstreept bovendien zelf in de bijgaande, recente TK-brief d.d. 14 december jl. dat een Europese aanpak prevaleert voor dit vraagstuk en dat het van groot belang is om technische mogelijkheden en effecten te onderzoeken, onder meer wegens het belang van sterke encryptie voor onze digitale economie en maatschappij. Dit heeft de minister van JenV recentelijk nogmaals bevestigd in het AO Cybersecurity.[2] In dat AO heeft JenV nog medegedeeld dat goedwillende eindgebruikers van volledige encryptie moeten zijn voorzien. Deze publieke signalen stroken dan ook niet met het voornemen om toch een nationale aftapverplichting voor encryptiediensten op te nemen.
- Daarbij is de genoemde Kamerbrief van JenV d.d. 14 december jl. omtrent versleuteld bewijs controversieel verklaard. Gelet hierop, is het dan ook politiek uitermate risicovol dat een demissionair kabinet toch het politieke besluit neemt om een aftapverplichting op te nemen: de kans dat de Kamer het kabinet terugfluit is zeer reëel.
- NB: JenV zal sturen op optie 2. Hierbij wordt er een bepaling opgenomen in de Telecomwet om OTT-dienstverleners af te tappen, echter deze bepaling treedt nog niet direct in werking. Een besluit over inwerkingtreding wordt op een niet nader moment genomen. EZK acht het onwenselijk om slechts normatieve bepalingen op te nemen. Een dergelijke insteek creëert veel onzekerheid en zal naar verwachting veel maatschappelijke weerstand teweegbrengen vanwege nadelige effecten inzake encryptie. Bovendien schuilt er een risico inzake precedentwerking. De Kamer zal naar verwachting ontstemd zijn over optie 2. De Kamer zal geen wetgeving aannemen die niet inwerking treedt.

Beleidsinhoudelijk:
- EZK onderschrijft de doelstelling om digitale opsporing waar nodig te versterken, gezien veranderingen in hoe mensen communiceren. Zoals het feit dat steeds meer communicatie via OTT-dienstverleners laten verlopen.
- Voor EZK is het daarbij echter van belang dat het beschermingsniveau niet wordt aangetast. Het kabinetsstandpunt van 2016 inzake encryptie onderstreept niet voor niets het belang van sterke encryptie.
- Door het inbouwen van een ontsleutelplicht bij OTT dienstverleners wordt de communicatie niet alleen makkelijker toegankelijk gemaakt voor opsporingsdiensten, maar ook voor kwaadwillenden zoals cybercriminelen en spionagediensten uit derde landen.
- Afzwakking of inperking van sterke encryptie impliceert zodoende de acceptatie van disproportionele veiligheidsrisico's. Het vormt bovendien een aantasting van de privacy en het communicatiegeheim voor consumenten en bedrijven. Goedwillende afnemers zullen hier ernstig hinder van ondervinden en het ondermijnt het vertrouwen in het digitale communicatieverkeer. Deze zorgen leven ook nadrukkelijk in de Tweede Kamer.

[2] Kamerstukken II 28 684, nr. 645 (verslag AO cybersecurity, 9 december 2020).

- De aftapverplichting houdt namelijk in dat OTT-dienstverleners de opgevraagde communicatie moeten ontsleutelen, terwijl zij niet zelf over de sleutel beschikken (het betreft nl. zogenaamde end-to-end encryptie). Een dergelijke ontsleutelplicht betekent dat OTT dienstverleners een andere encryptievorm moeten aanbieden die makkelijk toegankelijk is en dus resulteert in een afzwakking van adequate encryptie.
- EZK, verantwoordelijk voor wettelijke bepalingen in de Tw, acht zorgvuldigheid van cruciaal belang. Een gegrond besluit kan pas genomen worden nadat er eerst gedegen onderzoek is gedaan naar de effecten van een dergelijke aftapverplichting, als ook naar alternatieve technologische mogelijkheden.
- Een bepaling die leidt tot zwakke encryptie zal bovendien tot veel onrust en weerstand leiden onder het maatschappelijk middenveld en bedrijfsleven. De gevolgen hiervan komen voor rekening van EZK, aangezien de Telecommunicatiewet onder de verantwoordelijkheid van EZK valt.
- Gegeven het bovenstaande is, mede op verzoek van de lidstaten, een Europese inventarisatie aangekondigd naar de technische mogelijkheden voor de rechtmatige toegang tot versleuteld bewijs. Gelet op het grensoverschrijdende karakter van OTT-dienstverlening en de wenselijkheid van een Europees gelijk speelveld, heeft een Europese aanpak dan ook sterk de voorkeur. Er is dan ook geen reden om de onlangs aangekondigde Europese technische inventarisatie te negeren en alvast op nationaal niveau wettelijke maatregelen te treffen.
- 5.2.1 [redacted]

Kabinetstandpunt encryptie

- Het kabinetsstandpunt van 2016 inzake encryptie (zie bijgaand) onderstreept het belang van sterke encryptie. Zo staat er: "*Op dit moment is er geen zicht op mogelijkheden om in algemene zin, bijvoorbeeld via standaarden, encryptie producten te verzwakken zonder daarmee de veiligheid van digitale systemen die van encryptie gebruik maken te compromitteren.*" Het kabinetsstandpunt biedt geen ruimte om afwijkende maatregelen te nemen zonder de encryptie ernstig af te zwakken.
- Het kabinetstandpunt is helder: de '*door een technische ingang in een encryptie product te introduceren die het voor opsporingsinstanties mogelijk zou maken versleutelde bestanden in te zien, kunnen digitale systemen kwetsbaar worden voor bijvoorbeeld criminelen, terroristen en buitenlandse inlichtingendiensten. Dit kan onwenselijke gevolgen hebben voor de beveiliging van gecommuniceerde en opgeslagen informatie, en de integriteit van ICT-systemen, die in toenemende mate van belang zijn voor het functioneren van de samenleving.*"

Van: 5.1.2.e
Verzonden: dinsdag 16 februari 2021 16:23
Aan: 5.1.2.e
Onderwerp: RE: nota OTT v2
Bijlagen: nota aftappen_Over-The-Top_dienstverleners5.1.2.docx

Categorieën: Categorie Rood

Excuus, hierbij ook juiste bijlage

Met vriendelijke groet,

5.1.2 e
Digitale Veiligheid / ePrivacy

T : +31-70 -5.1.2.e
M : +31 6 -5.1 2.e

Van: 5.1.2.e @minezk.nl>
Verzonden: dinsdag 16 februari 2021 15:36
Aan: 5.1.2.e @minezk.nl>; 5.1.2.e @minezk.nl>; 5.1.2.e @minezk.nl>
Onderwerp: RE: nota OTT v2

Zie mijn suggesties

Met vriendelijke groet,

5.1.2 e
Digitale Veiligheid / ePrivacy

T : +31-70 -5.1.2.e
M : +31 6 -5.1 2.e

Van: 5.1.2.e @minezk.nl>
Verzonden: dinsdag 16 februari 2021 14:11
Aan: 5.1.2.e @minezk.nl>; 5.1.2.e @minezk.nl>;5.1.2.e @minezk.nl>
Onderwerp: RE: nota OTT v2

Ha,

Hierbij een schone variant. Prettiger leesbaar.

Gr

5.1 2.e

Van: 5.1.2.e
Verzonden: dinsdag 16 februari 2021 14:02
Aan: 5.1.2.e @minezk.nl>; 5.1.2.e @minezk.nl>; 5.1.2.e @minezk.nl>
Onderwerp: nota OTT v2

Ha allen,

Hierbij aangepaste nota OTT's. Spreekpunten veel meer inkorten lukt mij nog niet helemaal zonder alle belangrijke punten te benoemen. Wellicht hebben jullie nog een mooie slag?

Gr

5.1 2.e

Van: 5.1.2.e
Verzonden: woensdag 17 februari 2021 09:50
Aan: 5.1.2.e
Onderwerp: RE: Aanbiedingsform MCEV

Categorieën: Categorie Rood

Thx, je vervelend.
5.2.1, 5.1.2.i

Met vriendelijke groet,

5.1.2.e
Digitale Veiligheid / ePrivacy

T : +31-70 - 5.1.2.e
M.: +31 6 - 5.1.2.e

Van: 5.1.2.e @minezk.nl>
Verzonden: woensdag 17 februari 2021 09:20
Aan: 5.1.2.e @minezk.nl>; 5.1.2.e @minezk.nl>; 5.1.2.e @minezk.nl>
Onderwerp: FW: Aanbiedingsform MCEV

Opgelost. Maar het blijft bewerkelijk…

Van: 5.1.2.e
Verzonden: woensdag 17 februari 2021 09:17
Aan: 5.1.2.e
Onderwerp: FW: Aanbiedingsform MCEV

Verzonden vanuit Mail voor Windows 10

Van: 5.1.2.e
Verzonden: dinsdag 16 februari 2021 17:36
Aan: 5.1.2.e
Onderwerp: RE: Aanbiedingsform MCEV

Ik verwerk m in die tekst idd. Groet, 5.1.2.e

Van: 5.1.2.e @minezk.nl>
Verzonden: dinsdag 16 februari 2021 16:50
Aan: 5.1.2.e @minjenv.nl>
Onderwerp: RE: Aanbiedingsform MCEV

5.1.2.e
Ik neem aan dat je deze zin toevoegt aan de tekst die ik eerder heb gestuurd?
5.1.2.e

Verzonden vanuit Mail voor Windows 10

Van: 5.1.2.e
Verzonden: dinsdag 16 februari 2021 16:41
Aan: 5.1.2.e
Onderwerp: RE: Aanbiedingsform MCEV

Dag 5.1.2.e

Eens met je dat we discussies niet opnieuw gaan doen. Ik wil wel scherp hebben waarom we dit gesprek nu op de MCEV voeren en bijgaande zin haal ik uit de nota: EZK voorziet ondanks eerdere besluitvorming en debat hierover toch risico's ten aanzien van veilige encryptie als OTT-diensten aftapbaar worden.

Wat mij betreft zetten we die overeengekomen zin dan ook terugkomen in het aanbiedingsformulier, want volgens mij geeft deze het correct weer (anders waren we m ook niet overeen gekomen ;-).

Groet, 5.1.2.e

Van: 5.1.2.e @minezk.nl>
Verzonden: dinsdag 16 februari 2021 15:21
Aan: 5.1.2.e @minjenv.nl>
Onderwerp: RE: Aanbiedingsform MCEV

5.1.2.e
De reden voor mijn tekstvoorstel was dat ik uit de semantiek zou willen blijven en een eerdere discussie niet over wil doen.
Wij hebben eerder, om goede redenen, bezwaar gemaakt tegen de zin die nu weer wordt voorgesteld. Daar zijn we toen in de herkansing goed uitgekomen, met de overeengekomen passage in de nota, die een goede discussie in de ACEV heeft gefaciliteerd. Laten we het daarom houden bij de agreed language en die ook weer op te nemen in dit aanbiedingsformulier.

Groet,
5.1.2.e

Verzonden vanuit Mail voor Windows 10

Van: 5.1.2.e
Verzonden: dinsdag 16 februari 2021 14:12
Aan: 5.1.2.e
Onderwerp: RE: Aanbiedingsform MCEV

Ha 5.1.2.e

Naar mijn idee moet wel helder zijn dat de nota er nu ligt omdat er een wijziging is van de eerder ingezette koers, dus een heroverweging van jullie kant op het eerder genomen besluit. 5.2.1

Groet, 5.1.2.e

Van: 5.1.2.e @minezk.nl>
Verzonden: dinsdag 16 februari 2021 13:31
Aan: 5.1.2.e @minjenv.nl>
Onderwerp: RE: Aanbiedingsform MCEV

Ha 5.1.2.e

Ik heb bezwaren tegen de volgende zin: "Dit laatste onderdeel van het MCEV besluit wordt door EZK niet meer gesteund. De Minister van Justitie en Veiligheid wil deze impasse en hoe hiermee om te gaan bespreken in de MCEV."

Daarom het volgende tekstvoorstel: ..

"Bijgesloten nota is door JenV en EZK opgesteld en besproken in de ACEV van 11 februari 2021. Het verslag van die bespreking is tevens toegevoegd.

Doel van de nota is u te informeren over de dilemma's die ten grondslag liggen aan de vraag hoe zorgvuldig invulling gegeven kan worden aan het MCEV-besluit van mei 2020 om Over-The-Top-communicatiediensten (OTT) net als telecommunicatiediensten wettelijk te verplichten om hun communicatiedienst, in het bijzonder met betrekking tot encryptie, zodanig in te richten dat communicatie daarover afgetapt kan worden ten behoeve van de opsporing of nationale veiligheid. Vervolgens is het doel dat u, na kennisname over de gevolgen en risico's, een keuze maakt uit de in de nota geschetste opties."

Groet,
5.1.2.e

Groet,
5.1.2.e

Verzonden vanuit Mail voor Windows 10

Van: 5.1.2.e
Verzonden: dinsdag 16 februari 2021 12:17

Aan: 5.1.2.e
Onderwerp: Aanbiedingsform MCEV

Let op, in de bijlage van deze e-mail, verzonden door 5.1.2.e @minjenv.nl, is een macro aangetroffen. Macro's kunnen misbruikt worden om malware op uw systeem te installeren. Open de bijlage alleen als de e-mail afkomstig is van een door u vertrouwde afzender.

Indien dit niet het geval is dient u deze e-mail direct te verwijderen zonder de bijlage te openen.

DICTU Servicedesk

Dag 5.1.2.e

Voor de MCEV van volgende week moet nog een aanbiedingsformulier opgesteld worden, zie bijgaand. Tevens wordt de nota en het verslag van ACEV er bij aangeboden. Ben jij akkoord met bijgaande formulering. Deze moet uiterlijk vandaag bij AZ. Dank al vast voor je reactie.

Groet, 5.1.2.e

Van: 5.1.2.e
Verzonden: woensdag 17 februari 2021 13:04
Aan: 5.1.2.e
Onderwerp: RE: verslag mcev mei 2020

Categorieën: Categorie Rood

Even mijn beeld heirbij.

Klopt in belgie en australie meen ik.
In beide gevallen is slechts sprake van symbolisch overheidsingrijpen.
5.2.1
oet
worden naar innovatieve opsporingsmogelijkheden / -methoden.

5.2.1

Met vriendelijke groet,

5.1.2 e
Digitale Veiligheid / ePrivacy

T : +31-70 - 5.1.2.e
M : +31 6 - 5.1 2.e

Van: 5.1.2.e @minezk.nl>
Verzonden: woensdag 17 februari 2021 12:41
Aan: 5.1.2.e @minezk.nl>; 5.1.2.e @minezk.nl>; 5.1.2.e @minezk.nl>
Onderwerp: RE: verslag mcev mei 2020

5.2.1

Van: 5.1.2.e @minezk.nl>
Verzonden: woensdag 17 februari 2021 12:07
Aan: 5.1.2.e @minezk.nl>; 5.1.2.e @minezk.nl>; 5.1.2.e @minezk.nl>
Onderwerp: RE: verslag mcev mei 2020

Kan je dat uitzoeken? Wil graag de stukken die er zijn, hebben.

5.1.2.e
Directie Digitale Economie
Ministerie van Economische Zaken en Klimaat

Tel: +31 6 5.1.2.e
Mail: 5.1.2.e @minezk.nl
Web: Telecommunicatie | Rijksoverheid.nl

Van: 5.1.2.e
Verzonden: woensdag 17 februari 2021 11:52
Aan: 5.1.2.e
Onderwerp: RE: verslag mcev mei 2020

De brief van 14 april betreft meen ik het aanbiedingsformulier voor de MCEV, waarin naar de beleidsnota gerefereerd wordt.

Van: 5.1.2.e @minezk.nl>
Verzonden: woensdag 17 februari 2021 11:01
Aan: 5.1.2.e @minezk.nl>; 5.1.2.e @minezk.nl>; 5.1.2.e @minezk.nl>
Onderwerp: RE: verslag mcev mei 2020

Heb nagelezen. Was ultrakort want een pro forma vergadering waar alleen FIN een opmerking heeft gemaakt nav de brief / beleidsnota over 5G en opsporing, over evt te dragen kosten die ten late moeten vallen voor het verantwoordelijke departement. Verder niks. Zo te zien gebruikt JenV het niet indienen van commentaar aan als argument dat we akkoord zijn. 5.2.1

Er wordt daarbij dus verwezen naar een brief van MJenV dd 14/4 2020 en de 'beleidsnota 5G en opsporing'. Kan niet zien of brief en nota hetzelfde zijn of twee separate stukken. Herkennen jullie ze? Misschien helpt dat nog.

5.1.2.e

5.1.2.e
Directie Digitale Economie
Ministerie van Economische Zaken en Klimaat

Tel: +31 6 5.1.2.e
Mail: 5.1.2.e @minezk.nl
Web: Telecommunicatie | Rijksoverheid.nl

Van: 5.1.2.e
Verzonden: woensdag 17 februari 2021 10:48
Aan: 5.1.2.e
Onderwerp: FW: verslag mcev mei 2020

Ha 5.1.2.e

Nog een reminder, mogelijk ten overvloede, dat de stukken te zien bij BBR.

Gr

5.1 2.e

Van: BBRMREZK 5.1.2.e @minezk.nl>
Verzonden: vrijdag 12 februari 2021 12:34
Aan: 5.1.2.e @minezk.nl>
CC: 5.1.2.e @minezk.nl>
Onderwerp: RE: verslag mcev mei 2020

Het kan in de ochtend tot 12.00 uur.

5.1.2.e

Van: 5.1.2.e @minezk.nl>
Verzonden: vrijdag 12 februari 2021 11:52
Aan: 5.1.2.e @minezk.nl>
CC: BBRMREZK 5.1.2.e @minezk.nl>; 5.1.2.e @minezk.nl>; 5.1.2.e @minezk.nl>
Onderwerp: Re: verslag mcev mei 2020

Dank. Ja gaat om passage over wetsvoorstel aftappen 5G. 5.1.2.e mijn mt lid is woensdag op kantoor. Kan hij dan kijken? groet

Verstuurd vanaf mijn iPhone

> Op 11 feb. 2021 om 19:26 heeft 5.1.2.e @minezk.nl> het volgende geschreven:
>
> Hi 5.1.2.e
>
> Het verslag kan worden ingezien bij 5.1.2.e en 5.1.2.e Ben je op zoek naar een specifieke passage?
> 5.1.2.e is morgen op kantoor, wellicht kan hij wat voorlezen.
>
> Groet,
> 5.1.2.e
>
> ---
>
> **Van:** 5.1.2.e @minezk.nl>
> **Verzonden:** donderdag 11 februari 2021 18:14
> **Aan:** 5.1.2.e @minezk.nl>
> **Onderwerp:** Fwd: verslag mcev mei 2020

Hoi 5.1.2.e

Kan jij mij helpen met verslag van MCEV van mei 2020?

Dank.

Gr

5.1.2.e

Verstuurd vanaf mijn iPhone

Begin doorgestuurd bericht:

> **Van:** 5.1.2.e @minezk.nl>
> **Datum:** 11 februari 2021 om 17:57:32 CET
> **Aan:** 5.1.2.e
> 5.1.2.e @minezk.nl>
> **Kopie:** 5.1.2.e @minezk.nl>
> **Onderwerp: RE: verslag mcev mei 2020**
>
> Hi 5.1.2.e
>
> Wij krijgen geen verslag of terugkoppeling van de MCEV. BBR (Voor SEZK-zaken 5.1.2.e kan je daar mogelijk verder mee helpen.
>
> Groet,
> 5.1 2.e
>
> ---
>
> **Van:** 5.1.2.e
> @minezk.nl>
> **Verzonden:** donderdag 11 februari 2021 17:54
> **Aan:** 5.1.2.e @minezk.nl>; 5.1.2.e
> @minezk.nl>
> **Onderwerp:** verslag mcev mei 2020
>
> Hoi 5.1.2.e
>
> Hebben jullie toevallig nog voor ons het verslag van de MCEV van mei 2020. Toen stond ook het aftappen en 5G geagendeerd.
>
> Dank vast.
>
> Gr
>
> 5.1.2.e
>
> [redacted]

Directoraat-Generaal Bedrijfsleven en Innovatie
.....
Ministerie van Economische Zaken
Bezuidenhoutseweg 73 | 2594 AC | Den Haag
Postbus 20401 | 2500 EK | Den Haag
.....
T: +31 5.1.2.e
E: 5.1.2.e @minez.nl
.....

Van: 5.1.2.e
Verzonden: donderdag 18 februari 2021 08:46
Aan: 5.1.2.e
Onderwerp: RE: nota OTT v2
Bijlagen: 210217 nota aftappen_Over-The-Top_dienstverleners 5.1.2.docx

Heren,

Een mooi stuk !!! Zie nog enkele suggesties van mijn kant.
In de spreektekst maak ik hem nog scherper want dat is de feitelijke situatie.

Gr.
5.1.2.e

Met vriendelijke groet,

5.1.2 e
Digitale Veiligheid / ePrivacy

T : +31-70 - 5.1.2.e
M : +31 6 - 5.1 2.e

Van: 5.1.2.e @minezk.nl>
Verzonden: woensdag 17 februari 2021 20:23
Aan: 5.1.2.e @minezk.nl>; 5.1.2.e @minezk.nl>
Onderwerp: RE: nota OTT v2

Hoi allen,

Mooi stuk. Bijgaand paar puntjes nog toegevoegd, ik laat aan jou 5.1.2.e de keuze om dit wel of niet op te nemen:
- actief meegeven aan Stas dat Grapperhaus toegevoegd aan TK om binnen kabinetsstandpunt te blijven bij het maken van maatregelen (quod non).
- meegeven dat we niet tegen aftappen zijn, maar wel nog bezwaar hebben indien dit ook een ontsleutelplicht betreft vanwege de impact op encryptie. Het gaat ons dus met name om de ontsleuteling niet het aftappen sec.

Gr

5.1.2.e

Van: 5.1.2.e @minezk.nl>
Verzonden: woensdag 17 februari 2021 17:45
Aan: 5.1.2.e @minezk.nl>; 5.1.2.e @minezk.nl>; 5.1.2.e @minezk.nl>
Onderwerp: RE: nota OTT v2

Zie hier wat ik er van heb gemaakt. Excuses dat ik m heb omgegooid, ik wilde het vooral korter, toegankelijker en politieker hebben. Heb dus ook wat nuanceringen en argumenten weggelaten; mijn

ervaring in dit soort ministeriële commissies is dat daarvoor de tijd/ruimte niet bestaat. Bovendien staat het allemaal goed in de nota die in de MCEV voorligt. Benieuwd of jullie dit zo OK vinden.

5.1.2.e

PS zodra we dit af hebben en ik lijntje met de PA van de Stas heb (staat nog steeds uit via 5.1 2 e kunnen we dit gebruiken voor onze outreach.

Van: 5.1.2.e @minezk.nl>
Verzonden: dinsdag 16 februari 2021 16:23
Aan: 5.1.2.e @minezk.nl>; 5.1.2.e @minezk.nl>; 5.1.2.e @minezk.nl>
Onderwerp: RE: nota OTT v2

Excuus, hierbij ook juiste bijlage

Met vriendelijke groet,

5.1.2 e
Digitale Veiligheid / ePrivacy

T : +31-70 - 5.1.2.e
M : +31 6 - 5.1 2.e

Van: 5.1.2.e @minezk.nl>
Verzonden: dinsdag 16 februari 2021 15:36
Aan: 5.1.2.e @minezk.nl>; 5.1.2.e @minezk.nl>; 5.1.2.e @minezk.nl>
Onderwerp: RE: nota OTT v2

Zie mijn suggesties

Met vriendelijke groet,

5.1.2 e
Digitale Veiligheid / ePrivacy

T : +31-70 5.1.2.e
M : +31 6 - 5.1 2.e

Van: 5.1.2.e @minezk.nl>
Verzonden: dinsdag 16 februari 2021 14:11
Aan: 5.1.2.e @minezk.nl>; 5.1.2.e @minezk.nl>; 5.1.2.e @minezk.nl>
Onderwerp: RE: nota OTT v2

Ha,

Hierbij een schone variant. Prettiger leesbaar.

Gr

5.1 2.e

Van: 5.1.2.e
Verzonden: dinsdag 16 februari 2021 14:02
Aan: 5.1.2.e @minezk.nl>; 5.1.2.e @minezk.nl>; 5.1.2.e @minezk.nl>
Onderwerp: nota OTT v2

Ha allen,

Hierbij aangepaste nota OTT's. Spreekpunten veel meer inkorten lukt mij nog niet helemaal zonder alle belangrijke punten te benoemen. Wellicht hebben jullie nog een mooie slag?

Gr

5.1 2.e

Van: 5.1.2.e
Verzonden: donderdag 18 februari 2021 12:26
Aan: 5.1.2.e
CC: 5.1.2.e
Onderwerp: MCEV nota over aftappen OTT diensten
Bijlagen: 210218 nota aftappen_Over-The-Top_dienstverleners [3980].docx

Categorieën: Categorie Rood

Dag 5.1.2.e

Veel dank voor het prettige (kennismakings)gesprek zonet! En dank voor je bereidheid om outreach te doen naar je collega-PAs bij andere bewindspersonen. Zoals gezegd denken we goede argumenten te hebben om nu pas op de plaats te maken en te kiezen voor de Europese inventarisatie.

Bijgaand zoals besproken alvast de concept nota die we de lijn in zullen doen zodra we de MCEV-stukken binnen hebben. Denk dat de inhoud voor zich spreekt; sluit aan bij hetgeen we net hebben besproken. Mocht je nog vragen hebben, je weet me nu te vinden!

NB volgende week zal 5.1.2.e wrsch met de Stas naar de MCEV gaan; 5.1.2.e is immers met verlof. Ik ben er volgende week ook niet (probeer weekje Krokusvakantie te houden) maar wel bereikbaar.

Hartelijke groet,
5.1.2.e

5.1.2.e
Directie Digitale Economie
Ministerie van Economische Zaken en Klimaat

Tel: +31 6 5.1.2.e
Mail: 5.1.2.e @minezk.nl
Web: Telecommunicatie | Rijksoverheid.nl

Van: 5.1.2.e
Aan: 5.1.2.e Secretariaat DE;5.1.2.e
Onderwerp: Bhm aftappen Over-The-Top dienstverleners
Datum: donderdag 18 februari 2021 15:54:38
Bijlagen: DOMUS-21047718-Bhm_aftappen_Over-The-Top_dienstverleners.ZZZ.DRF

Dit stuk heeft onze directie verlaten.

Van: StasEZK
Verzonden: vrijdag 19 februari 2021 17:25
Aan: 5.1.2.e
CC: StasEZK; 5.1.2.e Secretariaat DE; secretariaatDGBI; 5.1.2.e
Onderwerp: BWO inzake 'aftappen Over-The-Top dienstverleners + vooroverleg

Categorieën: Categorie Rood

Goedemiddag,

Wij hebben een BWO ingepland met de Staatssecretaris en Minister J&V inzake 'aftappen Over-The-Top dienstverleners' **op donderdag 25 februari van 11:00-11:30 uur via Webex.**

Tevens hebben we op donderdagochtend 09:30 uur een overleg ingepland om dit voor te spreken.

Graag tijdig, iom BBR, de voorbereiding aanleveren. Ook horen we graag wie het BWO zal aansluiten.

Alvast dank!

Met vriendelijke groet,

5.1.2.e

.....
Ministerie van Economische Zaken en Klimaat
Bezuidenhoutseweg 73 | 2594 AC | Den Haag
Postbus 20401 | 2500 EK Den Haag
T: + 31 70 5.1.2.e
E: 5.1.2.e@minezk.nl

Werkzaam: dinsdag t/m vrijdag

Van: 5.1.2.e
Verzonden: woensdag 24 februari 2021 11:58
Aan: 5.1.2.e
Onderwerp: RE: 210224 NIEUWE LIJN STAS EZK
Bijlagen: 210224 NIEUWE LIJN STAS EZK 5.1.2. .docx

Categorieën: Categorie Rood

5.1 2.e ea
Zie hierbij mijn suggesties

Met vriendelijke groet,

5.1.2 e
Digitale Veiligheid / ePrivacy

T : +31-70 5.1.2.e
M : +31 6 - 5.1 2.e

Van: 5.1.2.e @minezk.nl>
Verzonden: woensdag 24 februari 2021 11:31
Aan: 5.1.2.e @minezk.nl>; 5.1.2.e @minezk.nl>; 5.1.2.e @minezk.nl>
Onderwerp: 210224 NIEUWE LIJN STAS EZK

Hierbij, check geel gearceerde zijn toevoegingen.

Van: 5.1.2.e
Verzonden: woensdag 24 februari 2021 12:03
Aan: 5.1.2.e
CC: 5.1.2.e
Onderwerp: aangepast blanco OTT aftap voor BWO
Bijlagen: 210224 NIEUWE LIJN STAS EZK SCHOON.docx

Hoi 5.1.2.e

Bijgaand een aangepaste blanco spreeklijn voor Stas voor haar gesprek met Grapperhaus zo.

Gr

5.1.2.e

5.1.2.e
Directoraat-Generaal Bedrijfsleven en Innovatie
.....
Ministerie van Economische Zaken
Bezuidenhoutseweg 73 | 2594 AC | Den Haag
Postbus 20401 | 2500 EK | Den Haag
.....
T: +31 5.1.2.e
E: 5.1.2.e @minez.nl
.....

Van: 5.1.2.e
Verzonden: woensdag 24 februari 2021 16:07
Aan: 5.1.2.e
Onderwerp: RE: volgend BWO

Categorieën: Categorie Rood

Het voorstel leidt dan ook tot een lager niveau van bescherming van encryptie. JenV meent echter dat dit voldoende bescherming biedt wanneer er waarborgen worden toegepast.

- Hier zit de crux: zijn die waarborgen dusdanig dat kwaadwillende er niet bij kunnen? Eerdere standpunt encryptie stelde van niet. Bewijslast ligt bij JenV om aan te geven waarom dat nu anders is. En dat zou ik vervolgens graag getoetst willen hebben bij onafhankelijke deskundigen

---

Van: 5.1.2.e @minezk.nl>
Verzonden: woensdag 24 februari 2021 16:04
Aan: 5.1.2.e @minezk.nl>; 5.1.2.e @minezk.nl>; 5.1.2.e @minezk.nl>
Onderwerp: RE: volgend BWO

Ja dat bedoel ik, excuus!

Van: 5.1.2.e @minezk.nl>
Verzonden: woensdag 24 februari 2021 16:04
Aan: 5.1.2.e @minezk.nl>; 5.1.2.e @minezk.nl>; 5.1.2.e @minezk.nl>
Onderwerp: RE: volgend BWO

Bedoel je dat Grapperhaus zijn mening niet klopt?

Verzonden vanuit Mail voor Windows 10

Van: 5.1.2.e
Verzonden: woensdag 24 februari 2021 16:00
Aan: 5.1.2.e
Onderwerp: volgend BWO
Urgentie: Hoog

Hoi 5.1.2.e

E2E-encryptie
Er is geen E2E mogelijk met het inbouwen van een 'speciale' sleutel. Dan is er weliswaar sprake nog van encryptie maar geen E2E encryptie, want inherent aan E2E is dat er geen sleutels in het bezit zijn van dienstverlener. Grapperhaus zijn mening dat E2E en aftappen verenigdbaar zijn klopt dus **niet**. 5.1.2.e gaf ook aan dat het voorstel betekent dat E2E niet meer zal blijven bestaan. Het voorstel leidt dan ook tot een lager niveau van bescherming van encryptie. JenV meent echter dat dit voldoende bescherming biedt wanneer er waarborgen worden toegepast.

NB ik krijg mijn contact bij NCSC niet te pakken (neemt niet op of is in gesprek!

Wcc3
JenV zal bij het volgende BWO aangeven dat de Wcc3 een ander instrument betreft (‘hacken’) dan aftappen. Het is een gericht instrument. Wcc3 wordt dit jaar geëvalueerd en naar verwachting komen er aanbevelingen die de drempels verlagen.
Er kleven nu zware procedurele waarborgen rondom Wcc3, slechts toepasbaar bij enstige delicten en er zijn zware toestemmingsvereisten (toetsing rechter-commissaris). Wcc3 is wel van toepassing op alle communicatiediensten.

5.1.2.e zal ondersteuning bieden bij het BWO morgen/overmorgen.

Groet,

5.1.2.e

Directoraat-Generaal Bedrijfsleven en Innovatie
.....
Ministerie van Economische Zaken
Bezuidenhoutseweg 73 | 2594 AC | Den Haag
Postbus 20401 | 2500 EK | Den Haag
.....
T: +31 5.1.2.e
E: 5.1.2.e @minez.nl
.....

Van: 5.1.2.e
Verzonden: woensdag 24 februari 2021 19:12
Aan: 5.1.2.e
CC: 5.1.2.e
Onderwerp: RE: 210224 NIEUWE LIJN STAS EZK SCHOON

Categorieën: Categorie Rood

Technologieverbod omdat via deze route de facto een verbod op end2end technologie zal gelden.

Punt is;
- Onze standpunt is altijd geweest dat wetgeving techniek neutraal moet zijn.
- Deze verplichting verbiedt end2end techniek. Maar willen we ook dat de toekomstige nieuwe innovatie encryptie vormen die er zeker aan zitten te komen - alleen al in het kader van Quantum - verboden worden omdat de traditionele werkmethodes van opsporing daar weinig of geen vat op hebben?

Evaluatie CCW3 kan wellicht mogelijkheden/openingen bieden, en toekomstvast. 5.2.1

Met vriendelijke groet,

5.1.2 e
Digitale Veiligheid / ePrivacy

T : +31-70 - 5.1.2.e
M : +31 6 - 5.1 2.e

Van: 5.1.2.e @minezk.nl>
Verzonden: woensdag 24 februari 2021 18:25
Aan: 5.1.2.e @minezk.nl>
CC: 5.1.2.e @minezk.nl>; 5.1.2.e @minezk.nl>
Onderwerp: Re: 210224 NIEUWE LIJN STAS EZK SCHOON
Urgentie: Hoog

Helder stuk, 5.1.2.e Weten we wat de positie van j&v is op deze punten. Neem jij daar nog contact over met ze op?

5.1.2.e

Ps wat bedoel je met technologieverbod?

Verstuurd vanaf mijn iPhone

> Op 24 feb. 2021 om 18:21 heeft 5.1.2.e @minezk.nl> het volgende geschreven:
>
> Kijken jullie even mee?
>
> 5.1.2.e
>
> Verstuurd vanaf mijn iPhone

Op 24 feb. 2021 om 17:35 heeft 5.1.2.e
@minezk.nl> het volgende geschreven:

Hoi 5.1 2.e

Hierbij nieuw stuk. Kijk maar even of je het punt van de symbolische werking okay verwoord vindt.

Gr

5.1.2.e
<210224 NIEUWE LIJN STAS EZK SCHOON.docx>

Van: 5.1.2.e
Verzonden: woensdag 24 februari 2021 19:46
Aan: 5.1.2.e
CC: 5.1.2.e
Onderwerp: RE: OTT dienstverleners aftappen aanvulling extra BWO

Categorieën: Categorie Rood

Hi 5.1.2.e

Dank hiervoor. Dat er een vervolg BWO gepland wordt was mij niet bekend. Ik heb het secr gevraagd morgenochtend gelijk met secr van J&V te schakelen om dit in te plannen. 5.1.2.e en 5.1.2.e zullen hier een uitnodiging voor ontvangen.

Groet,
5.1.2.e

Van: 5.1.2.e @minezk.nl>
Verzonden: woensdag 24 februari 2021 19:39
Aan: 5.1.2.e @minezk.nl>
CC: 5.1.2.e @minezk.nl>; 5.1.2.e @minezk.nl>; 5.1.2.e @minezk.nl>
Onderwerp: OTT dienstverleners aftappen aanvulling extra BWO

Hallo 5.1.2.e

Stas EZK en MinJenV hebben afgesproken om nog een extra BWO te houden voor de MCEV. Dit zou morgen of vrijdag plaatsvinden. Weet jij al wanneer dit gaat plaatsvinden?

In dit BWO wordt specifiek ingegaan op de volgende punten:
1) kan end-2-end encryptie nog toegepast worden door OTT-dienstverleners indien de aftapverplichting ingevoerd wordt? Antwoord is nee (zie bijlage)
2) wat zijn de volgens JenV mogelijkheden van de 'hack-bevoegdheid' Wet computer criminaliteit iii ?

Bijgaand de aanvulling tekst hiervoor. 5.1.2.e zal bij het BWO ondersteuning bieden samen met 5.1.2.e

Groet,

5.1.2.e

Directoraat-Generaal Bedrijfsleven en Innovatie
.....
Ministerie van Economische Zaken
Bezuidenhoutseweg 73 | 2594 AC | Den Haag
Postbus 20401 | 2500 EK | Den Haag
.....
T: +31 5.1.2.e
E: 5.1.2.e @minez.nl
.....

Van: 5.1.2.e
Verzonden: woensdag 24 februari 2021 19:52
Aan: 5.1.2.e
Onderwerp: Fwd: OTT dienstverleners aftappen aanvulling extra BWO
Bijlagen: 210224 AANVULLENDE LIJN STAS EZK SCHOON v2.docx

Verstuurd vanaf mijn iPhone

Begin doorgestuurd bericht:

Van: 5.1.2.e @minezk.nl>
Datum: 24 februari 2021 om 19:39:20 CET
Aan: 5.1.2.e @minezk.nl>
Kopie: 5.1.2.e @minezk.nl>, 5.1.2.e @minezk.nl>, 5.1.2.e @minezk.nl>
Onderwerp: OTT dienstverleners aftappen aanvulling extra BWO

Hallo 5.1.2.e

Stas EZK en MinJenV hebben afgesproken om nog een extra BWO te houden voor de MCEV. Dit zou morgen of vrijdag plaatsvinden. Weet jij al wanneer dit gaat plaatsvinden?

In dit BWO wordt specifiek ingegaan op de volgende punten:
1) kan end-2-end encryptie nog toegepast worden door OTT-dienstverleners indien de aftapverplichting ingevoerd wordt? Antwoord is nee (zie bijlage)
2) wat zijn de volgens JenV mogelijkheden van de 'hack-bevoegdheid' Wet computer criminaliteit iii ?

Bijgaand de aanvulling tekst hiervoor. 5.1.2.e zal bij het BWO ondersteuning bieden samen met 5.1.2.e

Groet,

5.1.2.e

Directoraat-Generaal Bedrijfsleven en Innovatie
.....
Ministerie van Economische Zaken
Bezuidenhoutseweg 73 | 2594 AC | Den Haag
Postbus 20401 | 2500 EK | Den Haag
.....
T: +31 5.1.2.e
E: 5.1.2.e @minez.nl
.....

Van: 5.1.2.e
Verzonden: zaterdag 27 februari 2021 14:05
Aan: 5.1.2.e
CC: 5.1.2.e
Onderwerp: RE: overleg Mona

Categorieën: Categorie Rood

Kwam ook nog dit tegen:
Brengt nieuwe Crypto War de EU aan het wankelen? | Computable.nl

En **Bert-Jaap Koops van Tilburg University** heeft ook interessant artikel dat wijst naar hacking bevoegdheden als weg vooruit (is wat wij ook suggereerden als alternatief):
Looking for some light through the lens of "cryptowar" history: Policy options for law enforcement authorities against "going dark" - ScienceDirect

Verzonden vanuit Mail voor Windows 10

Van: 5.1.2.e
Verzonden: zaterdag 27 februari 2021 13:54
Aan: 5.1.2.e
CC: 5.1.2.e)
Onderwerp: RE: overleg Mona

5.1.2.e kwam met de volgende namen:

5.1.2.e (TUD)
5.1.2.e (KU Leuven)
5.1.2.e (Radboud Universiteit)

Er is (nog steeds) wetenschappelijke consensus dat toegang leidt tot verzwakking, zo bevestigde hij. Vraag voor selectie lijkt dus belangrijk wie het met autoriteit kan brengen en het helder kan uitleggen.

Gr 5.1.2.e

Verzonden vanuit Mail voor Windows 10

Van: 5.1.2.e
Verzonden: vrijdag 26 februari 2021 17:01
Aan: 5.1.2.e
CC: 5.1.2.e
Onderwerp: Re: overleg Mona

5.2.1

5.2.1

Verstuurd vanaf mijn iPhone

Op 26 feb. 2021 om 16:31 heeft 5.1.2.e @minezk.nl> het volgende geschreven:

5.2.1

Verstuurd vanaf mijn iPhone

Op 26 feb. 2021 om 13:27 heeft 5.1.2.e @minezk.nl> het volgende geschreven:

5.2.1

Verstuurd vanaf mijn iPhone

Op 26 feb. 2021 om 13:04 heeft 5.1.2.e @minezk.nl> het volgende geschreven:

5.2.1

Met vriendelijke groet,

5.1.2 e
Digitale Veiligheid / ePrivacy

T : +31-70 5.1.2.e
M : +31 6 - 5.1 2 e

Van: 5.1.2.e @minezk.nl>
Verzonden: vrijdag 26 februari 2021 12:53
Aan: 5.1.2.e @minezk.nl>
CC: 5.1.2.e @minezk.nl>; 5.1.2.e @minezk.nl>; 5.1.2.e @minezk.nl>
Onderwerp: Re: overleg Mona

5.2.1

Verstuurd vanaf mijn iPhone

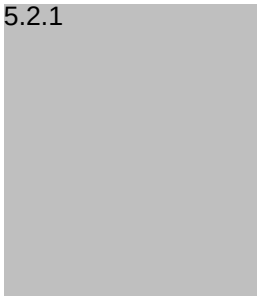
Op 26 feb. 2021 om 12:16 heeft 5.1.2.e @minezk.nl> het volgende geschreven:

5.2.1

Verstuurd vanaf mijn iPhone

Op 26 feb. 2021 om 11:20 heeft 5.1.2.e @minezk.nl> het volgende geschreven:

5.2.1



5.2.1

Verstuurd vanaf mijn iPhone

Op 26 feb. 2021 om 10:43 heeft 5.1.2.e
@minezk.nl> het volgende geschreven:

5.2.1

Verstuurd vanaf mijn iPhone

Op 26 feb. 2021 om 10:32 heeft 5.1.2.e
@minezk.nl> het volgende geschreven:

5.1.2.e

5.2.1

[redacted]

Met vriendelijke groet,

5.1.2 e [redacted]
Digitale Veiligheid / ePrivacy

T
:
+
3
1
-
7
0
-
5

5.1.2.e

M

:

+

3

1

6

-

5.1.2.e

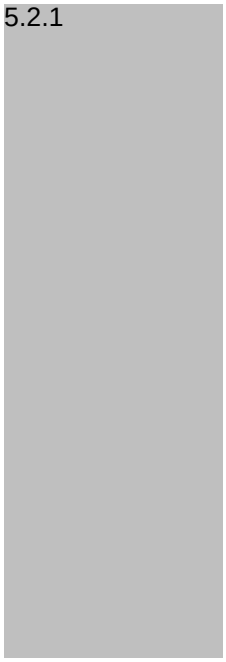
Van: 5.1.2.e @minezk.nl >
Verzonden: vrijdag 26 februari 2021 08:53
Aan: 5.1.2.e @minezk.nl>
Onderwerp: Re: overleg Mona
Urgentie: Hoog

5.2.1

Verstuurd vanaf mijn iPhone

Op 25 feb. 2021 om 18:10 heeft 5.1.2.e @minezk.nl> het volgende geschreven:

5.2.1



5.1.2 e

Ministerie van Economische Zaken en Klimaat
Directoraat Generaal B&I
Directie

Digitale
Economie

Bezuidenhoutseweg

73259

4

AC

Den

Haag

Postbus

20401,

2500

EK

Den

Haag

T:

+

31-70-[redacted]

M: +316-[redacted]

Van: 5.1.2.e
Verzonden: zaterdag 27 februari 2021 15:42
Aan: 5.1.2.e
Onderwerp: Goed artikel
Bijlagen: SSRN-id3249238.pdf; ATT00001.txt

Categorieën: Categorie Rood

Hierbij stuk van 5.1.2.e in pdf. Vat het goed samen en benadrukt ook wat LA al wel kunnen en waar richting van oplossingen te zoeken.

Van: 5.1.2.e
Verzonden: maandag 1 maart 2021 17:10
Aan: 5.1.2.e)
Onderwerp: RE: Voor overleg 5.1.2.e met 5.1.2.e woensdag

Categorieën: Categorie Rood

Ha 5.1.2.e

Was op mijn verzoek (net aan 5.1.2.e gevraagd tijdens routine). 5.1.2.e ziet 5.1.2.e NCTV 5.1.2.e ; leek mij goed om 5.1.2.e daartoe wat punten mee te geven over ons favo dossier. NB 5.1.2.e was ook bij de MCEV als de +1 van Grapperhaus. Wil kijken of zij nog wat kunnen worden geactiveerd op deze materie.

5.1.2.e

5.1.2.e
Directie Digitale Economie
Ministerie van Economische Zaken en Klimaat

Tel: +31 6 5.1.2.e
Mail: 5.1.2.e @minezk.nl
Web: Telecommunicatie | Rijksoverheid.nl

Van: 5.1.2.e
Verzonden: maandag 1 maart 2021 17:03
Aan: 5.1.2.e
CC: 5.1.2.e)
Onderwerp: RE: Voor overleg 5.1.2.e met 5.1.2.e woensdag

Ja

Van: 5.1.2.e @minezk.nl>
Verzonden: maandag 1 maart 2021 17:04
Aan: 5.1.2.e @minezk.nl>
CC: 5.1.2.e @minezk.nl>
Onderwerp: Re: Voor overleg 5.1.2.e met 5.1.2.e woensdag

Ha 5.1.2.e

Is voor een bila met NCTV?

Gr

5.1.2.e

Verstuurd vanaf mijn iPhone

Op 1 mrt. 2021 om 16:59 heeft 5.1.2.e [redacted]@minezk.nl> het volgende geschreven:

Wetsvoorstel aftappen OTT

- In MCEV is dit wetsvoorstel geagendeerd waarbij het dilemma is geschetst tussen het willen aftappen van OTT diensten tbv opsporing en de consequenties daarvan voor een algehele verzwakking van de beveiliging (cybersecurity) van het berichtenverkeer. Waardoor ook andere statelijke actoren makkelijker toegang krijgen tot berichtenverkeer. 5.2.1 [redacted]
- Eerder is dit dilemma ook geschetst in het encryptiestandpunt dat door NCTV in 2016 naar de TK is gestuurd.
- Het kabinetsstandpunt van 2016 inzake encryptie onderstreept het belang van sterke encryptie. Zo staat er: "Op dit moment is er geen zicht op mogelijkheden om in algemene zin, bijvoorbeeld via standaarden, encryptie producten te verzwakken zonder daarmee de veiligheid van digitale systemen die van encryptie gebruik maken te compromitteren." Het kabinetsstandpunt biedt geen ruimte om afwijkende maatregelen te nemen zonder de encryptie ernstig af te zwakken.
- Het kabinetstandpunt is helder: de "door een technische ingang in een encryptie product te introduceren die het voor opsporingsinstanties mogelijk zou maken versleutelde bestanden in te zien, kunnen digitale systemen kwetsbaar worden voor bijvoorbeeld criminelen, terroristen en buitenlandse inlichtingendiensten. Dit kan onwenselijke gevolgen hebben voor de beveiliging van gecommuniceerde en opgeslagen informatie, en de integriteit van ICT-systemen, die in toenemende mate van belang zijn voor het functioneren van de samenleving."
- 5.2.1 [redacted]

Van: 5.1.2.e
Verzonden: maandag 1 maart 2021 17:32
Aan: 5.1.2.e
Onderwerp: FW: jouw telefoonnr.

Categorieën: Categorie Rood

-----Oorspronkelijk bericht-----
Van: 5.1.2.e @tudelft.nl>
Verzonden: maandag 1 maart 2021 17:28
Aan: 5.1.2.e @minezk.nl>
Onderwerp: FW: jouw telefoonnr.

Voor je vrienden aan de Turfmarkt had ik al eens iets gecomponeerd.... Wellicht nog bruikbaar. De aankondiging van een legal intercept verplichting in Australia schijnt behoorlijk wat economische schade berokkend te hebben, omdat allerlei bedrijven uit voorzorg vertrokken of zich bedachten tot maar niet naar Australie te komen om zich te vestigen.

En dat is nog maar de aankondiging. De wet is nog niet ingevoerd.

We gaan het zien....

--5.1.2.e

> -----Oorspronkelijk bericht-----
> Van: 5.1.2.e
> Verzonden: maandag 23 november 2020 21:11
> Aan: 5.1.2.e @ncsc.nl>
> Onderwerp: RE: jouw telefoonnr.
>
> Hoi 5.1.2.e
>
> Ik hoorde net je voicemail. Ik ben er mee bezig, maar vooralsnog lijkt
> de richting om homomorphic encryption en differential privacy toe te
> passen voor lawful intercept niet plausibel. De toepassingen waar
> mensen in mijn omgeving over gehoord hebben (zoals IDS over HTTPS)
> vereisen toch dat je iets doet met key management om het mogelijk te
> maken -- simpel gezegd, de gebruiker moet meewerken aan het mogelijk maken van de legal intercept.
> Dat is natuurlijk geen werkbare opzet als je doel is om intercept te
> doen bij criminelen c.s. Er zijn wel degelijk doorbraken in homomorphic encryption.
> Google en Mastercard hebben toepassingen gebouwd hiervan, maar die
> zijn voor andere use cases.
>
> Ik heb nog niet iemand gevonden die zich voldoende deskundig voelt om
> jullie hierover meer diepgaand te informeren. Er staan nog een paar
> vragen uit. Als ik daar een antwoord op krijg, laat ik het je weten.
> Ik zoek verder, maar ik zou je aanraden om aan te nemen dat dit geen begaanbare route is.
>
> Terzijde: wat is er ooit geworden van de Australische poging om
> dienstverleners te dwingen om toegang te verschaffen tot versleutelde
> communicatie?
> https://www.bbc.com/news/world-australia-46463029

> https://www.theguardian.com/australia-news/2020/aug/07/anti-encrytion-
> laws-yet-to-be-used-by-asio-or-afp-to-compel-tech-firms-help-inquiry-
> told?CMP=Share_iOSApp_Other
> Ik meen dat die AABill nog niet is aangenomen, maar ik weet het niet zeker.
> Zou vermoedelijk alleen Australische techbedrijven wegjagen. Facebook
> en anderen zouden het negeren, voor zover ik kan zien.
>
> Met vriendelijke groet,
>
5.1.2.e
> Faculteit Techniek, Bestuur en Management TU Delft Jaffalaan 5, 2628BX
> Delft Kamer 5.1.2.e https://www.tudelft.nl/cybersecurity/
5.1.2.e @tudelft.nl
> 015 5.1.2.e
>
>
>
> > -----Oorspronkelijk bericht-----
> > Van: 5.1.2.e @minjenv.nl>
> > Verzonden: maandag 23 november 2020 16:50
> > Aan: 5.1.2.e @tudelft.nl>
> > CC: 5.1.2.e @ncsc.nl>
> > Onderwerp: jouw telefoonnr.
> >
> > Beste 5.1.2.e
> >
> >
> >
> > Mag ik jouw tel.nr.? 5.1.2.e (in c.c.) wil even verder met je
> > overleggen over een cyber security onderwerp waar jullie eerder over
> spraken.
> >
> >
> >
> > Alvast dank en groeten,
> >
> > 5.1.2.e
> >
> >
> >
> > 5.1.2.e
> >
> >
> >
> > 5.1.2.e
> >
> > Unit Samenwerking en Kennisuitwisseling
> >
> > .....
> > Nationaal Cyber Security Centrum
> >
> > Ministerie van Justitie en Veiligheid Postbus 117 | 2501 CC | Den
> > Haag
> >
> > .....
> > National Cyber Security Centre
> >
> > Ministry of Justice and Security

> > P.O. Box 117 | 2501 CC | The Hague | The Netherlands
> > .....
> > T +31 70 5.1.2.e
> >
> > M +31 6 5.1.2.e
> >
> > 5.1.2.e @minjenv.nl
> > https://www.ncsc.nl
> >
> >
> >
> > _____
> >
> >
> > Dit bericht kan informatie bevatten die niet voor u is bestemd.
> > Indien u niet de geadresseerde bent of dit bericht abusievelijk aan
> > u is toegezonden, wordt u verzocht dat aan de afzender te melden en
> > het bericht te verwijderen. De Staat aanvaardt geen
> > aansprakelijkheid voor schade, van welke aard ook, die verband houdt
> > met risico's verbonden aan het elektronisch verzenden van berichten.
> >
> > Ministerie van Justitie en Veiligheid
> >
> > This message may contain information that is not intended for you.
> > If you are not the addressee or if this message was sent to you by
> > mistake, you are requested to inform the sender and delete the
> > message. The State accepts no liability for damage of any kind
> > resulting from the risks inherent in the electronic transmission of messages.
> >
> > Ministry of Justice and Security
> >

Van: 5.1.2.e
Verzonden: dinsdag 2 maart 2021 22:53
Aan: 5.1.2.e
Onderwerp: Fwd: Concept opzet briefing MCEV 12 maart 2021 versie 02032021
Bijlagen: Concept opzet briefing MCEV 12 maart 2021 versie 02032021.docx

Categorieën: Categorie Rood

Zie bijlage. Moeten we nog wel flink aan schaven denk ik zo. Commentaar welkom, liefst zsm zodat ik snel kan reageren naar 5.1.2.e Zou 5.1.2.e voor willen zijn.

5.1.2.e

Verstuurd vanaf mijn iPhone

Begin doorgestuurd bericht:

Van: 5.1.2.e @minaz.nl>
Datum: 2 maart 2021 om 22:15:36 CET
Aan: "5.1.2.e @minjenv.nl>, 5.1.2.e @minjenv.nl, 5.1.2.e @minezk.nl>
Kopie: 5.1.2.e @minaz.nl>
Onderwerp: Concept opzet briefing MCEV 12 maart 2021 versie 02032021

Heren,

Zoals beloofd, hierbij een eerste concept opzet voor de briefing MCEV. Ben zelf (nog) geen expert op dit gebied, dus hoop niet dat ik met bepaalde woordkeuze een gevoelige snaar raak of een oude wond weer open haal ;)
Zou willen voorstellen even met z'n vieren te kijken of we dit concept een stap verder kunnen brengen, voordat het breder gedeeld wordt.

Zullen we elkaar donderdagochtend 9:00 uur even spreken hierover? Dan kunnen we ook afstemmen of het handig is om dit onderwerp nog in de ACEV van die middag aan de orde te stellen.

In de tussentijd zie ik graag jullie opmerkingen tegemoet,

Hartelijke groet,
5.1.2.e

Van: 5.1.2.e
Verzonden: donderdag 4 maart 2021 12:12
Aan: 5.1.2.e
Onderwerp: RE: Concept opzet briefing MCEV 12 maart 2021 versie 02032021

Categorieën: Categorie Rood

5.1.2.e thx,

Je hebt daar'n hoop werk aan gehad zo te zien
5.2.1

m.a.w. het zou wel chiquer zijn als 5.1.2.e intro doet, NFI J&V oplossing schets zoals J&V in gedachte had en vervolgens 5.1.2.e daar o.m. op reflecteert.
In omgekeerde volgorde wordt 5.1.2.e verhaal door NFI anders geïnterpreteerd (wetenschap en operationele praktische toepassing) en gekneed of vervormd tot dan centraal gepositioneerde oplossing van NFI.

5.2.1

Gr. 5.1.2.e

Met vriendelijke groet,

5.1.2 e
Digitale Veiligheid / ePrivacy

T : +31-70 - 5.1.2.e
M : +31 6 - 5.1 2.e

Van: 5.1.2.e @minezk.nl>
Verzonden: donderdag 4 maart 2021 10:55
Aan: 5.1.2.e @minezk.nl>; 5.1.2.e @minezk.nl>; 5.1.2.e @minezk.nl>; 5.1.2.e @minezk.nl>
Onderwerp: RE: Concept opzet briefing MCEV 12 maart 2021 versie 02032021

Korte recap: Heb hard teruggeduwd op 2 experts. Wordt nu NFI, geen 5.1.2.e (die wordt wrsch de +1 van Ollongren). Verder ook de centrale vraag die 5.1.2.e bovenaan invoegde van tafel gekregen, en ook de punten aan het eind bij de wrap-up zijn er uit (gaat deels naar de intro).

Enige waar ik denk dat we moeten meebewegen is de volgorde: JenV insisteert nu op eerst 5.1.2.e dan 5.1.2.e dan het NFI. Heb gezegd dat wij liever andersom zien, maar dat ik hier nader naar zal kijken.

Heb tot slot nog gevraagd om de NFI presentatie. Gaat 5.1.2.e achteraan.

Kortom: wordt vervolgd…

/5.1.2.e

5.2.1

Van: 5.1.2.e @minezk.nl>
Verzonden: donderdag 4 maart 2021 09:30
Aan: 5.1.2.e @minezk.nl>; 5.1.2.e @minezk.nl>; 5.1.2.e @minezk.nl>; 5.1.2.e @minezk.nl>
Onderwerp: RE: Concept opzet briefing MCEV 12 maart 2021 versie 02032021

Bij deze, ik zie veel herhaling qua inbreng tussen 5.1.2.e en NFI. Lijkt me niet oke. Mogen wij ook 2 experts, wellicht wil Mona dat ook graag.

Van: 5.1.2.e @minezk.nl>
Verzonden: donderdag 4 maart 2021 09:10
Aan: 5.1.2.e @minezk.nl>; 5.1.2.e @minezk.nl>; 5.1.2.e @minezk.nl>; 5.1.2.e @minezk.nl>
Onderwerp: FW: Concept opzet briefing MCEV 12 maart 2021 versie 02032021

Hierbij de JenV comments. Als jullie nu wat reacties hebben, laat het weten dan maak ik daar gebruik van in de call! Graag pr mail.

Van: 5.1.2.e @minjenv.nl>
Verzonden: donderdag 4 maart 2021 07:48
Aan: 5.1.2.e @minezk.nl>; 5.1.2.e @minaz.nl>; 5.1.2.e @minjenv.nl>
CC: 5.1.2.e @minaz.nl>
Onderwerp: RE: Concept opzet briefing MCEV 12 maart 2021 versie 02032021

En hierbij met mijn aanvullingen. Ligt ook nog bij een paar personen voor, dus onder voorbehoud.
Tot zo.

Groet,

5.1.2.e

Van: 5.1.2.e @minezk.nl>
Verzonden: woensdag 3 maart 2021 22:42
Aan: 5.1.2.e @minaz.nl>; 5.1.2.e @minjenv.nl>; 5.1.2.e @minjenv.nl>
CC: 5.1.2.e @minaz.nl>
Onderwerp: RE: Concept opzet briefing MCEV 12 maart 2021 versie 02032021

Dank 5.1.2.e

Mooie voorzet! Bijgaand aantal aanpassingen van mijn kant. Doen we morgen weer een webex? Zag nog geen uitnodiging. Anders met de good-old Iphone.

Tot morgen,
5.1.2.e

Van: 5.1.2.e @minaz.nl>
Verzonden: dinsdag 2 maart 2021 22:16
Aan: 5.1.2.e @minjenv.nl>; 5.1.2.e @minjenv.nl>; 5.1.2.e @minezk.nl>
CC: 5.1.2.e @minaz.nl>
Onderwerp: Concept opzet briefing MCEV 12 maart 2021 versie 02032021

Heren,

Zoals beloofd, hierbij een eerste concept opzet voor de briefing MCEV. Ben zelf (nog) geen expert op dit gebied, dus hoop niet dat ik met bepaalde woordkeuze een gevoelige snaar raak of een oude wond weer open haal ;)
Zou willen voorstellen even met z'n vieren te kijken of we dit concept een stap verder kunnen brengen, voordat het breder gedeeld wordt.

Zullen we elkaar donderdagochtend 9:00 uur even spreken hierover? Dan kunnen we ook afstemmen of het handig is om dit onderwerp nog in de ACEV van die middag aan de orde te stellen.

In de tussentijd zie ik graag jullie opmerkingen tegemoet,

Hartelijke groet,
5.1.2.e

Van: 5.1.2.e
Verzonden: donderdag 4 maart 2021 15:01
Aan: 5.1.2.e
Onderwerp: Doorst: Tweede concept opzet briefing MCEV
Bijlagen: Concept opzet briefing MCEV 12 maart 2021 versie 04032021.docx

Categorieën: Categorie Rood

5.1.2.e

Zie onder en in bijlage. Ik denk dat we een heel eind zijn. Wil graag constructief opereren richting AZ, 5.2.1 Maar wil ook weten van jullie of dit ok is zo. Schroom dus niet te piepen als er nog onoorbare dingen in staan.

Hoor graag,
5.1.2.e

Van: 5.1.2.e @minaz.nl>
Datum: 4 maart 2021 om 13:25:13 CET
Aan: 5.1.2.e @minjenv.nl>, 5.1.2.e @minezk.nl>, 5.1.2.e @minjenv.nl>
CC: 5.1.2.e @minaz.nl>
Onderwerp: Tweede concept opzet briefing MCEV

Heren,

Zie svp bijgaand een aangepaste versie. Graag jullie reactie (of beter nog akkoord ☺).

Ik teken hierbij aan dat we het volgende hebben besproken:

- Drie sprekers is gezien de beperkte tijd en de aandacht spanne een goed aantal;
- De volgorde van sprekers wordt wellicht op hoger dek nog even over gediscussieerd (mooier zou natuurlijk zijn dat wij het op basis van de inhoud eens kunnen worden over een logische volgorde);
- AZ beziet of het nodig is geheimhoudingsverklaring te ondertekenen;
- De briefing voor PJA wordt gezamenlijk voorbereid;
- Ook de andere briefings (NFI en 5.1.2.e worden van te voren met elkaar gedeeld;
- Het belang van de opsporings- en inlichtingendienst bij het kunnen aftappen van communicatie staat niet ter discussie (partijen die zich melden om ook wat te willen zeggen kan je doorverwijzen naar ondergetekende).

Hoor graag van jullie,

Hartelijke groet,

5.1.2.e

Van: 5.1.2.e
Verzonden: donderdag 4 maart 2021 15:35
Aan: 5.1.2.e
Onderwerp: FW: BoF || AAN discussie mbt encryptie.

Categorieën: Categorie Rood

t.i.

Via AAN (Anti Abuse Coalitie) bereikte me de onderstaande mail inz. encryptie. 5.2.1 5.2.1

Met vriendelijke groet,

5.1.2.e
Digitale Veiligheid / ePrivacy

T : +31-70 -5.1.2.e
M.: +31 6 -5.1.2.e

Van: 5.1.2.e @ams-ix.net>
Verzonden: donderdag 4 maart 2021 15:23
Aan: 5.1.2.e @fox-it.com>
CC: 5.1.2.e @ecp.nl>; 5.1.2.e @eokm.nl; 5.1.2.e @divd.nl; 5.1.2.e @sidn.nl; 5.1.2.e @divd.nl; 5.1.2.e @nl.ibm.com; 5.1.2.e @a2b-internet.com; 5.1.2.e @sidn.nl; 5.1.2.e @schubergphilis.com; 5.1.2.e @nbip.nl; 5.1.2.e @minezk.nl>; 5.1.2.e @minezk.nl>; 5.1.2.e @uva.nl; 5.1.2.e @nldigital.nl; 5.1.2.e @ecommercefoundation.org; 5.1.2.e @pmpartners.nl; 5.1.2.e @verenigingvanregistrars.nl; 5.1.2.e @cyberveilignederland.nl; 5.1.2.e @tudelft.nl; 5.1.2.e @t-mobile.nl; 5.1.2.e @nlconnect.org; 5.1.2.e @ripe.net; 5.1.2.e @bureau42.nl; 5.1.2.e @gmail.com; 5.1.2.e @sidnfonds.nl; 5.1.2.e @gmail.com; 5.1.2.e @dinl.nl; 5.1.2.e @nbip.nl; 5.1.2.e @dhpa.nl; 5.1.2.e @minezk.nl>; 5.1.2.e @connect2trust.nl; 5.1.2.e @vodafoneziggo.com; 5.1.2.e @ispconnect.nl; 5.1.2.e @cyso.group; 5.1.2.e @sidn.nl; 5.1.2.e @abuse.io; 5.1.2.e @tudelft.nl; 5.1.2.e @dutchdatacenters.nl; 5.1.2.e @bit.nl; 5.1.2.e @bitsoffreedom.nl>
Onderwerp: BoF || AAN discussie mbt encryptie.

Dag Allemaal (minus OM.nl, Politie.nl en V&J.nl)

Zojuist sprak ik 5.1.2.e van Bits of Freedom (BoF). (in de CC) o.a. n.a.v. de recente ontwikkelingen mbt encryptie.

BoF blijkt bezig met o.a. DINL, Google, Apple, Microsoft en Facebook om nog voor de verkiezingen een website te lanceren waar ze stelling nemen tegen beperkingen van (het gebruik van) encryptie. Ze graag willen een zo breed mogelijk palet aan relevante organisaties/personen vragen de oproep te ondersteunen.

5.1.2.e vraagt dus of AAN (en/of individuele AAN leden) mee wil tekenen? AMS-IX gaat in elk geval meedoen, en het zou denk ik goed zijn als we dit zowel individueel alsmede als AAN ook zouden kunnen en willen doen.

Ik begreep dat er enige haast bij is omdat ze één en ander ruim voor de verkiezingen live willen hebben staan. 5.1.2.e vertelde dat hij naast genoemde partijen het verzoek uit heeft staan bij onder andere Amnesty, 5.1.2.e , Consumentenbond, etcetera. Op de site komt slechts één zin te staan zodat er geen discussie zou kunnen ontstaan tussen ondertekenaars over de plek van een komma of de inhoud van een bijzin. Die zin is:

"Ondertekenaars, die een brede groep uit onze samenleving representeren, roepen het volgende kabinet op de ontwikkeling, beschikbaarheid en de
toepassing van alle vormen van encryptie te stimuleren."

Mocht je vragen hebben, 5.1.2.e zit in de CC.

Best regards,

5.1.2.e | Regulatory, Risk, Compliance | AMS-IX
Frederiksplein 42, 1017 XN Amsterdam, The Netherlands
M +31 6 5.1.2.e | T +31 20 5.1.2.e
ams-ix.net

Van: 5.1.2.e
Verzonden: donderdag 4 maart 2021 19:53
Aan: 5.1.2.e
Onderwerp: Berichten

Categorieën: Categorie Rood

Veel berichten op social media en internet over NOS bericht.

5.2.1

Met name zie ik (niet verrassend) onze argumenten benoemd (zie o.a. security.nl).
"Er staan genoeg open source alternatieven klaar om dit plan direct de das om te draaien. De boeven zitten dadelijk nog veilig achter encryptie en de politie leest mee in de groepsapp van het gezin"

5.1.2.e

Ministerie van Economische Zaken en Klimaat
Directoraat-Generaal Bedrijfsleven en Innovatie | Directie Digitale Economie
Bezuidenhoutseweg 73 | Postbus 20401 | 2500 EK | Den Haag

T (+31 70 5.1.2.e b.g.g. secretariaat (+31 70 5.1.2.e

Van: 5.1.2.e
Verzonden: donderdag 4 maart 2021 23:43
Aan: 5.1.2.e@cs.ru.nl'
Onderwerp: Presentatie 12/3
Bijlagen: Concept opzet briefing MCEV 12 maart 2021 versie 04032021.docx; DOMUS-21047733-v1-210217_TK-kabinetsstandpunt-encryptie.pdf; KAMERBRIEF_tk-raadsconclusies-over-rechtmatige-toegang-tot-versleuteld-bewijs.pdf

Geachte 5.1.2.e beste 5.1.2.e

Dank nog voor het goede gesprek dat we gisteravond hadden. In vervolg daarop stuur ik bijgaand een concept opzet voor de expert briefing mee die op 12/3 in de Ministeriële Commissie Economie en Veiligheid is voorzien, met jou als één van de twee experts. NB dit is nog work in progress; de spelregels en te bespreken vragen zijn op zichzelf al voer voor discussie, dus het kan zijn dat het nog wat verandert.

==>**Mijn vraag aan jou: ziet dit er qua opzet OK uit, in het bijzonder natuurlijk het deel waarvoor jij zelf aan de lat staat?** Graag hoor ik dat zsm van je zodat ik eventueel nog kan inzetten op aanpassing van het een en ander.

5.2.1

Naast de concept opzet van de briefing heb ik het kabinetsstandpunt van 2016 als ook de Kamerbrief van 1 december 2020 over de EU raadsconclusies inzake encryptie bijgevoegd. Deze laatste brief is door de Kamer controversieel verklaard na de val van het kabinet.

Tot slot ben ik uiteraard benieuwd of de presentatie al vorm begint te krijgen; zoals gezegd ben ik beschikbaar als sparring partner, uiteraard vanuit de premisse dat het echt jouw presentatie is. Het gaat ons immers om het onafhankelijke perspectief!

Ik zie uit naar je reactie.
Nogmaals dank en hartelijke groet,

5.1.2.e
Ministerie van Economische Zaken en Klimaat

Bezuidenhoutseweg 73 | 2594 AC | Den Haag
Postbus 20401 | 2500 EK | Den Haag

T +31 6 5.1.2.e
E 5.1.2.e @minezk.nl
W Telecommunicatie | Rijksoverheid.nl

Van: 5.1.2.e
Verzonden: maandag 8 maart 2021 22:41
Aan: 5.1.2.e
Onderwerp: RE: concept nota MCEV 12 maart expertsessie
Bijlagen: DOMUS-21064074-v1-MCEV_12_maart_expertsessie_[4661].docx

Categorieën: Categorie Rood

Ha 5.1.2.e

Mooie nota! Sieht gut aus.
Heb in het licht van de inkorting tot 30 minuten wat tracks en comments. Zie bijlage. Kan jij verwerken?

Bvd
5.1.2.e

Van: 5.1.2.e
Verzonden: maandag 8 maart 2021 11:20
Aan: 5.1.2.e
Onderwerp: concept nota MCEV 12 maart expertsessie

Hallo 5.1.2.e

Bijgaand vast eerste aanzet nota voor MCEV expertsessie, uiteraard zijn we nog in afwachting van definitieve programma. Maar leek me handig om vast wat op papier te zetten.

Stuk is afgestemd met 5.1.2.e en 5.1.2.e

Gr

5.1.2.e

98a

Ministerie van Economische Zaken en Klimaat

TER INFORMATIE

Aan de Staatssecretaris

Directoraat-generaal Bedrijfsleven & Innovatie
Directie Digitale Economie

Auteur
5.1.2.e
T 070 5.1.2.e
5.1.2.e @minezk.nl

Datum
4 maart 2021

Kenmerk
DGBI-DE / 21064074

BHM 21068166

Kopie aan
5.1.2.e

Bijlage(n)

nota

MCEV 12 maart expertsessie: OTT en aftappen

Parafenroute
5.1.2.e

Aanleiding

Tijdens de MCEV van 26 februari jl. is inzake het agendapunt aftappen van OTT-dienstverleners besloten om een extra MCEV in te plannen, omdat er verschillende opvattingen zijn inzake de gevolgen van het voorstel voor (1) end-to-end encryptie en (2) de effecten op beveiliging van de digitale infrastructuur. Op vrijdag 12 maart (09:30 – 10:00 uur) vindt er dan ook een expertsessie in de MCEV plaats waarin hier nader op ingegaan wordt. Na deze sessie zal er op 23 maart een volgende MCEV plaatsvinden waarbij er een besluit wordt genomen over de opties uit de nota die al voorlag in de MCEV van 26 februari jl.
Hieronder treft u de opzet aan van deze expertsessie. U zult ondersteund worden door 5.1.2.e 5.1.2.e .

Advies

U kunt kennis nemen van de nota.

Kernpunten

- Zowel EZK als JenV hebben voor deze bijeenkomst elk een deskundige aangewezen om een presentatie te geven op de MCEV.
- EZK draagt prof. dr. 5.1.2.e voor. Hij is 5.1.2.e aan de Radboud Universiteit Nijmegen en 5.1.2.e 5.1.2.e was recent ook 5.1.2.e . De heer 5.1.2.e zal ingaan op de gevolgen van het voorstel voor de end-to-end encryptie en de consequenties hiervan. In de toelichting treft u het profiel van dhr. 5.1.2.e aan.
- Namens JenV zal dhr. 5.1.2.e van het Nederlands Forensisch Instituut (hierna: NFI) ingaan op het belang van het voorstel tot ontsleuteling voor de opsporing. Daarbij zal het NFI trachten aan te tonen dat er voldoende technische mogelijkheden zijn bij het voorstel om toch het communicatieverkeer te kunnen beschermen. Het NFI is een uitvoeringsorganisatie van JenV.
- Aansluitend op de beide expert briefings is beperkt ruimte voor het stellen van vragen. In de toelichting treft u een aantal mogelijke vragen aan.

Ontvangen BBR

Directoraat-generaal
Bedrijfsleven & Innovatie
Directie Digitale Economie

Kenmerk
DGBI-DE / 21064074

- Na deze expertsessie zal er op 23 maart a.s. weer een MCEV plaatsvinden waarin definitieve besluitvorming plaatsvindt over de follow-up o.b.v. de nota die reeds in de MCEV van 6 februari voorlag.

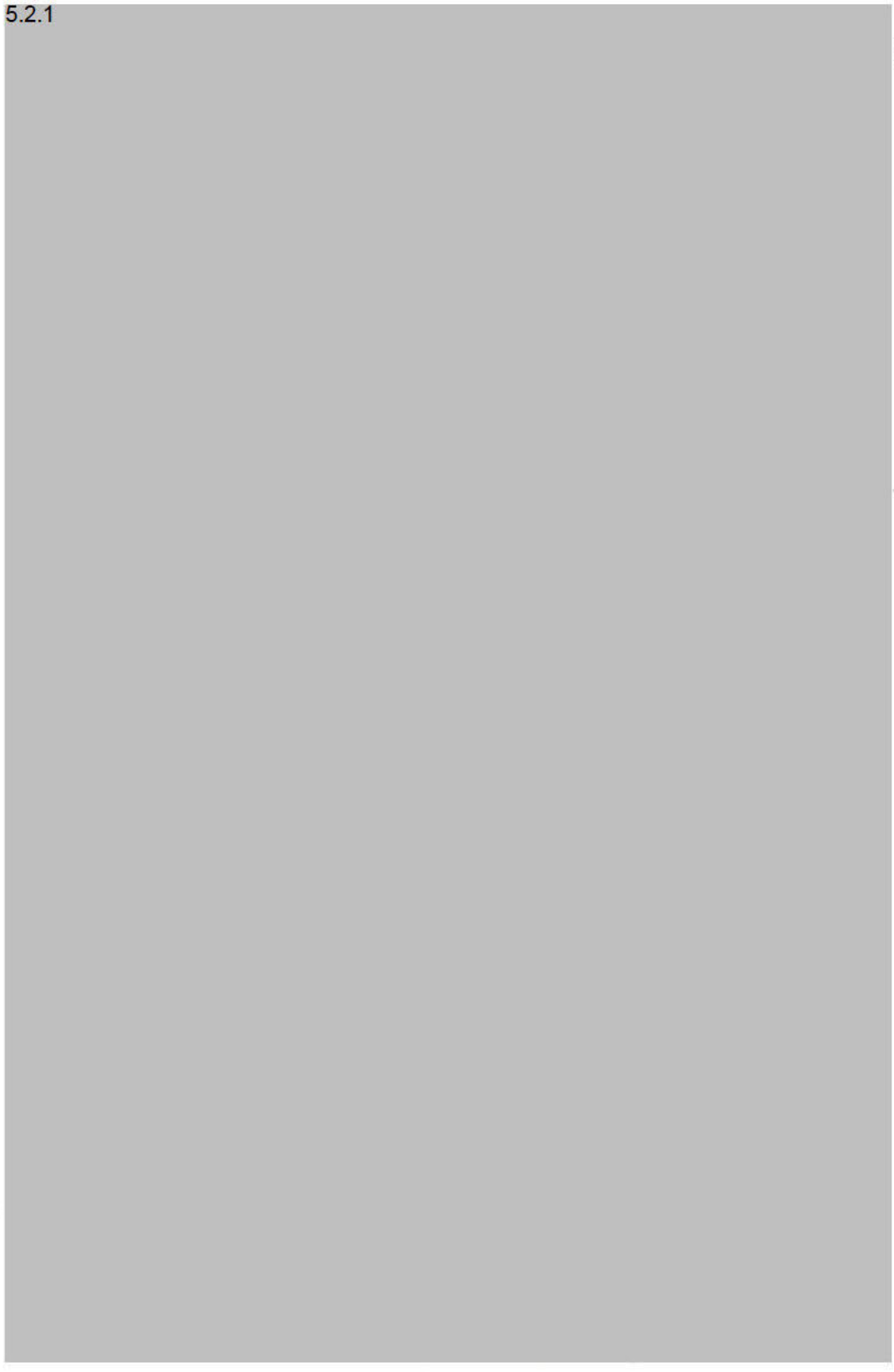
Toelichting
Opzet MCEV expertsessie 12 maart 2021

Onderdeel	**Inhoud**
09:30 – 09:35 uur Introductie, 5.1.2.e	Waartoe heeft MCEV in mei 2020 besloten? Welk dilemma doet zich voor? (belang opsporing en (nationale) veiligheid versus belang veilige encryptie van communicatieverkeer)
09:35 – 09:45 uur Risico's van aftappen OTT-diensten, 5.1.2.e	Wat is het belang van veilige (end-to-end) encryptie? Wat zijn de gevolgen voor end-to-end encryptie van het aftapbaar maken van OTT-communicatiediensten? Wat zijn de bredere consequenties hiervan? Zijn er (technische) alternatieven? Wat zijn relevante internationale ontwikkelingen?
09:45 – 09:55 uur Gevolgen voor opsporings- en veiligheidsdiensten, NFI (5.1.2.e	Korte toelichting belang aftappen OTT-communicatiediensten voor opsporings- en veiligheidsdiensten. Welke (technische) alternatieven zijn er en zijn die werkbaar voor de opsporings- en inlichtingendiensten? Inclusief reactie op suggesties vorige spreker. Welke technische ontwikkelingen zijn er op dit gebied?
09:55 – 10:00 uur Vragen en afsluiting	

Directoraat-generaal
Bedrijfsleven & Innovatie
Directie Digitale Economie

Kenmerk
DGBI-DE / 21064074

5.2.1



Directoraat-generaal
Bedrijfsleven & Innovatie
Directie Digitale Economie

5.2.1 [redacted]

Kenmerk
DGBI-DE / 21064074

Verdere informatie, oa. over wetenschappelijke activiteiten is te vinden op het webadres van 5.1.2.e: http://www.cs.ru.nl 5.1.2.e en ook op https://privacybydesign.foundation/

Bijlagen:
- behandelmap MCEV 26 februari 2021 aftappen Over-The-Top dienstverleners
- Beantwoording Kamervragen inzake het verzwakken van encryptie door de minister van Justitie en Veiligheid (8 maart 2021)

Van: 5.1.2.e
Verzonden: dinsdag 9 maart 2021 13:51
Aan: 5.1.2.e
CC: 5.1.2.e
Onderwerp: input OTT's aftappen bila 5.1.2.e Facebook

Ha 5.1.2.e

Hierbij inbreng voor de bila 5.1.2.e – Facebook mbt aftappen OTT's.

Kort
Naar verwachting zal Facebook informatie willen inwinnen naar de vertrouwelijke behandeling van dit dossier in de aanstaande MCEV's (12 en 23 maart) en meer willen weten omtrent de verhoudingen tussen EZK en JenV hierop. Dit kunnen wij nu **niet** delen, want dit is vertrouwelijk. Overigens is Facebook opvallend goed geïnformeerd omtrent de interdepartementale verhoudingen en voorbereidingen op dit dossier.

Instructie:
5.2.1

Kernpunten
- J&V ontwerpt een wetsvoorstel welke de huidige aftapmogelijkheden dient te borgen bij de invoering van 5G. In dit wetsvoorstel wil J&V ook een verruiming van de bevoegdheden, namelijk het kunnen aftappen van Over-The-Top-(OTT) dienstverleners. OTT-dienstverleners dienen daarbij de opgevraagde communicatie te ontsleutelen.
- EZK erkent dat er een rol is van OTT-dienstverleners inzake aftappen dan wel de digitale opsporing. Echter indien dit ook voor OTT- dienstverleners een verlichting tot ontsleuteling omhelst heeft dit negatieve effecten: namelijk een afzwakking van de encryptie. Daarmee wordt afgeweken van het kabinetsstandpunt van 2016 waarin is geconcludeerd dat een wettelijke inperking van het gebruik van encryptie niet mogelijk is zonder de veiligheid van digitale systemen die van encryptie gebruik maken te compromitteren. EZK kan hier dan ook niet mee akkoord gaan.
- Wat EZK (en een Kamermeerderheid) betreft is het kabinetsstandpunt uit 2016 nog steeds actueel. Daar komt bij dat er recentelijk twee nieuwe ontwikkelingen zijn:
    - eind 2020 zijn er EU-Raadsconclusies over dit specifieke thema aangenomen, waarin de lidstaten de Europese Commissie hebben gevraagd om samen met internet dienstverleners en de wetenschap een inventarisatie uit te voeren naar technische mogelijkheden voor rechtmatige toegang tot versleuteld bewijs, zonder de veiligheid van encryptie te compromitteren;
    - de Kamer heeft het onderwerp kort na de val van het kabinet controversieel verklaard.
- Vanwege dit verschil van inzicht is er een discussie gaande tussen JenV en EZK omtrent het al dan niet opnemen van een ontsleutelingsplicht in het wetgevingstraject.

Beleidsinhoudelijk:
- EZK onderschrijft de doelstelling om digitale opsporing waar nodig te versterken, gezien veranderingen in hoe mensen communiceren. Zoals het feit dat steeds meer communicatie via OTT-dienstverleners laten verlopen.
- Voor EZK is het daarbij echter van belang dat het beschermingsniveau niet wordt aangetast. Het kabinetsstandpunt van 2016 inzake encryptie onderstreept niet voor niets het belang van sterke encryptie. Door het inbouwen van een ontsleutelplicht bij OTT dienstverleners wordt de communicatie niet alleen makkelijker toegankelijk gemaakt voor opsporingsdiensten, maar ook voor kwaadwillenden zoals cybercrimlnelen en spionagediensten uit derde landen.

- Afzwakking of inperking van sterke encryptie impliceert zodoende de acceptatie van disproportionele veiligheidsrisico's. Het vormt bovendien een aantasting van de privacy en het communicatiegeheim voor consumenten en bedrijven. Goedwillende afnemers zullen hier ernstig hinder van ondervinden en het ondermijnt het vertrouwen in het digitale communicatieverkeer. Deze zorgen leven ook nadrukkelijk in de Tweede Kamer.
- De aftapverplichting houdt namelijk in dat OTT-dienstverleners de opgevraagde communicatie moeten ontsleutelen, terwijl zij niet zelf over de sleutel beschikken (het betreft nl, zogenaamde end-to-end encryptie). Een dergelijke ontsleutelplicht betekent dat OTT dienstverleners een andere encryptievorm moeten aanbieden die makkelijk toegankelijk is en dus resulteert in een afzwakking van adequate encryptie.
- Een bepaling die leidt tot zwakke encryptie zal bovendien tot veel onrust en weerstand leiden onder het maatschappelijk middenveld en bedrijfsleven. De gevolgen hiervan komen voor rekening van EZK, aangezien de Telecommunicatiewet onder de verantwoordelijkheid van EZK valt.
- Gegeven het bovenstaande is, mede op verzoek van de lidstaten, een Europese inventarisatie aangekondigd naar de technische mogelijkheden voor de rechtmatige toegang tot versleuteld bewijs. Gelet op het grensoverschrijdende karakter van OTT-dienstverlening en de wenselijkheid van een Europees gelijk speelveld, heeft een Europese aanpak dan ook sterk de voorkeur. Er is dan ook geen reden om de onlangs aangekondigde Europese technische inventarisatie te negeren en alvast op nationaal niveau wettelijke maatregelen te treffen.

Kabinetstandpunt encryptie
Het kabinetsstandpunt van 2016 inzake encryptie (zie bijgaand) onderstreept het belang van sterke encryptie. Zo staat er: "Op dit moment is er geen zicht op mogelijkheden om in algemene zin, bijvoorbeeld via standaarden, encryptie producten te verzwakken zonder daarmee de veiligheid van digitale systemen die van encryptie gebruik maken te compromitteren." Het kabinetsstandpunt biedt geen ruimte om afwijkende maatregelen te nemen zonder de encryptie ernstig af te zwakken.
Het kabinetstandpunt is helder: de 'door een technische ingang in een encryptie product te introduceren die het voor opsporingsinstanties mogelijk zou maken versleutelde bestanden in te zien, kunnen digitale systemen kwetsbaar worden voor bijvoorbeeld criminelen, terroristen en buitenlandse inlichtingendiensten. Dit kan onwenselijke gevolgen hebben voor de beveiliging van gecommuniceerde en opgeslaoen informatie, en de integriteit van ICT-svstemen, die in toenemende mate van belang ziin voor het functioneren van de samenleving."

Politiek-procedureel:
- Encryptie (in bijzonder maatregelen die encryptie aantasten) ligt uitermate gevoelig in de Kamer. Een meerderheid in de Kamer, inclusief coalitiepartij D66, hecht veel waarde aan encryptie, privacy en borging van betrouwbaarheid van communicatiesystemen en heeft november jl. nog een motie aangenomen welke het belang van sterke encryptie voor communicatie tussen burgers onderschrijft.
- De Minister van]enV onderstreept bovendien zelf in de bijgaande, recente TK-brief d.d. 14 december jl. dat een Europese aanpak prevaleert voor dit vraagstuk en dat het van groot belang is om technische mogelijkheden en effecten te onderzoeken, onder meer wegens het belang van sterke encryptie voor onze digitale economie en maatschappij. Dit heeft de minister van JenV recentelijk nogmaals bevestigd in het AO Cybersecurity. In dat AO heeft JenV nog medegedeeld dat goedwillende eindgebruikers van volledige encryptie moeten zijn voorzien. Deze publieke signalen stroken dan ook niet met het voornemen om toch een nationale aftapverplichting voor encryptiediensten op te nemen.
- Daarbij is de genoemde Kamerbrief van JenV d.d. 14 december jl. omtrent versleuteld bewijs controversieel verklaard. Gelet hierop, is het dan ook politiek uitermate risicovol dat een demissionair kabinet toch het politieke besluit neemt om een aftapverplichting op te nemen: de kans dat de Kamer het kabinet terugfluit is zeer reëel.

In geval van opmerkingen/vragen hoor ik het wel.

Gr

5.1.2.e

5.1.2.e
[redacted]
Directoraat-Generaal Bedrijfsleven en Innovatie
.....
Ministerie van Economische Zaken
Bezuidenhoutseweg 73 | 2594 AC | Den Haag
Postbus 20401 | 2500 EK | Den Haag
.....
T: +31 5.1.2.e
E: 5.1.2.e [redacted] @minez.nl
.....

Van: 5.1.2.e
Verzonden: woensdag 10 maart 2021 18:07
Aan: 5.1.2.e)
CC: 5.1.2.e
Onderwerp: RE: Kamerbrief Grapperhaus over OTT
Bijlagen: 210310 Brief OTT briefing 5.1.2.e .docx

Bijgaand mijn suggesties

Met vriendelijke groet,

5.1.2 e
Digitale Veiligheid / ePrivacy

T : +31-70 - 5.1.2.e
M : +31 6 - 5.1 2.e

Van: 5.1.2.e @minezk.nl>
Verzonden: woensdag 10 maart 2021 17:59
Aan: 5.1.2.e @minezk.nl>; 5.1.2.e @minezk.nl>; 5.1.2.e @minezk.nl>
CC: 5.1.2.e @minezk.nl>
Onderwerp: RE: Kamerbrief Grapperhaus over OTT

Hallo allemaal,

Bijgaand enkele toevoegingen en suggestie inzake de toon.

Gr

5.1 2.e

Van: 5.1.2.e @minezk.nl>
Verzonden: woensdag 10 maart 2021 17:51
Aan: 5.1.2.e @minezk.nl>; 5.1.2.e @minezk.nl>; 5.1.2.e @minezk.nl>
CC: 5.1.2.e @minezk.nl>
Onderwerp: RE: Kamerbrief Grapperhaus over OTT

Sorry nu met bijlage.

Van: 5.1.2.e
Verzonden: woensdag 10 maart 2021 17:48
Aan: 5.1.2.e @minezk.nl>; 5.1.2.e @minezk.nl>; 5.1.2.e @minezk.nl>
CC: 5.1.2.e @minezk.nl>
Onderwerp: Kamerbrief Grapperhaus over OTT

Allen,

Net met 5.1.2.e gebeld. Ere is idd een brief, zie bijlage.
Graag jullie snelle blik. Ik zou hier geen stammenstrijd over willen gaan voeren, maar we moten natuurlijk wel even kijken of r gen gekke dingen in staan. Heb zelf al een paar vragen/opmerkingen voor jullie in de kantlijn gehangen; fijn als jullie daar ieg naar kunnen kijken.

Grt,
5.1.2.e

Van: 5.1.2.e
Verzonden: woensdag 10 maart 2021 19:58
Aan: 5.1.2.e
Onderwerp: Doorst: Brief OTT briefing
Bijlagen: Brief OTT briefing.docx

Categorieën: Categorie Rood

Allen,

Dit is de def versie zoals die bij Grapperhaus (en 5.1.2.e voorligt. Alle ezk voorstellen zijn overgenomen. NB iom 5.1.2.e heb ik nog wat zitten wieden in de tracks die jullie voorstelden met focus op de hoofdpunten, om niet meteen weer in een heen en weer met JenV te belanden.

@5.1.2.e zullen we deze nog even aan stas, 5.1.2.e en bbr mailen?

Fijne avond!
5.1.2.e

Van: 5.1.2.e @minjenv.nl>
Datum: 10 maart 2021 om 19:24:22 CET
Aan: 5.1.2.e @minezk.nl>
CC: 5.1.2.e @minjenv.nl>
Onderwerp: RE: Brief OTT briefing

Dankjewel 5.1.2.e

Ik heb de tracks overgenomen! Zie de bijlage voor de versie zoals hij bij de MJenV en SG ligt. Qua verzending was de hoop vanavond, maar het wordt morgen(ochtend).

Met vriendelijke groet,

5.1.2.e

M 06 5.1.2.e
5.1.2.e @minvenj.nl

Van: 5.1.2.e @minezk.nl>
Verzonden: woensdag 10 maart 2021 18:44
Aan: 5.1.2.e @minjenv.nl>
CC: 5.1.2.e @minjenv.nl>
Onderwerp: RE: Brief OTT briefing

Dank 5.1.2.e

Mooie brief en grotendeels akkoord vanuit ons. Ik heb een viertal feitelijke tracks waar wij wel aan hechten. Hopelijk akkoord voor jullie.

Kan je me laten weten wanneer jullie deze brief willen versturen? Hier bestaat ook interesse hoger in de lijn.

Grt,

5.1.2.e

Van: 5.1.2.e @minjenv.nl>
Verzonden: woensdag 10 maart 2021 17:36
Aan: 5.1.2.e @minezk.nl>
CC: 5.1.2.e @minjenv.nl>
Onderwerp: Brief OTT briefing

Van: 5.1.2.e
Verzonden: donderdag 11 maart 2021 13:30
Aan: 5.1.2.e
CC: 5.1.2.e
Onderwerp: RE: Aftapbaarheid OTT-diensten versie 2 schoon

Categorieën: Categorie Rood

5.1.2.e e.a.,

5.2.1

Mbt aftapbaarheid,

5.2.1

In praktijk gaat het over bestoten, door geavanceerde technologieën super goed afgeschermde, criminele netwerken. Niet over algemene diensten waardoor ook onschuldige burgers (Europeanen) geraakt worden.

Met vriendelijke groet,

5.1.2 e
Digitale Veiligheid / ePrivacy

T : +31-70 -5.1.2.e
M : +31 6 -5.1 2.e

Van: 5.1.2.e @minezk.nl>
Verzonden: donderdag 11 maart 2021 13:01
Aan: 5.1.2.e @minezk.nl>; 5.1.2.e @minezk.nl>; 5.1.2.e @minezk.nl>
CC: 5.1.2.e @minezk.nl>
Onderwerp: FW: Aftapbaarheid OTT-diensten versie 2 schoon

Allen,

JenV heeft tracks op de eigen brief. Wrsch op verzoek van 5.1 2.e zelf. Graag zsm jullie blik, heb zelf al paar suggesties gedaan. Svp vanuit het motto: less is more!

5.1.2.e

Van: 5.1.2.e @minjenv.nl>
Verzonden: donderdag 11 maart 2021 12:14
Aan: 5.1.2.e @minezk.nl>
CC: 5.1.2.e @minjenv.nl>
Onderwerp: FW: Aftapbaarheid OTT-diensten versie 2 schoon

Hallo 5.1.2.e

Hierbij de nieuwe versie.

Met vriendelijke groet,

5.1.2.e

M 065.1.2.e
5.1.2.e @minvenj.nl

Van: 5.1.2.e
Verzonden: donderdag 11 maart 2021 12:12
Aan: 5.1.2.e @minjenv.nl>; 5.1.2.e @minjenv.nl>; 5.1.2.e @minjenv.nl>; 5.1.2.e @nctv.minjenv.nl>; 5.1.2.e @nctv.minjenv.nl>; 5.1.2.e @minjenv.nl>
CC: 5.1.2.e @minjenv.nl>
Onderwerp: FW: Aftapbaarheid OTT-diensten versie 2 schoon

Excuus voor spam. Laatste versie.

Met vriendelijke groet,

5.1.2.e
5.1.2.e

M 06 5.1.2.e
5.1.2.e @minvenj.nl

Van: 5.1.2.e
Verzonden: donderdag 11 maart 2021 12:07
Aan: 5.1.2.e @minjenv.nl>
Onderwerp: Aftapbaarheid OTT-diensten versie 2 schoon

Hallo 5.1.2.e

Hierbij de brief.

Met vriendelijke groet,

5.1.2.e

M 06 5.1.2.e
5.1.2.e @minvenj.nl

Van: 5.1.2.e
Verzonden: donderdag 11 maart 2021 17:34
Aan: 5.1.2.e
CC: 5.1.2.e
Onderwerp: RE: Nieuwe OTT brief
Bijlagen: Aftapbaarheid OTT-diensten versie 4.docx

Dank! Overgenomen. Zie bijlage. Dit ligt nu bij 5.1.2.e en BBR. Stuur zo ook naar JenV.

Van: 5.1.2.e @minezk.nl>
Verzonden: donderdag 11 maart 2021 17:13
Aan: 5.1.2.e @minezk.nl>; 5.1.2.e @minezk.nl>; 5.1.2.e @minezk.nl>
CC: 5.1.2.e @minezk.nl>
Onderwerp: RE: Nieuwe OTT brief

Zie suggesties.5.2.1
5.2.1
Lijkt me overigens wel goed dat wij zijn aangesloten bij zijn gesprekken met sector.

Van: 5.1.2.e @minezk.nl>
Verzonden: donderdag 11 maart 2021 17:01
Aan: 5.1.2.e @minezk.nl>; 5.1.2.e @minezk.nl>; 5.1.2.e @minezk.nl>
CC: 5.1.2.e @minezk.nl>
Onderwerp: Nieuwe OTT brief
Urgentie: Hoog

Allen,

Hierbij een compleet nieuwe brief. Heel veel druk om nu snel akkoord te gaan. Zie mijn tracks in bijlage. 5.2.1

Graag ook jullie visie. Mis ik nog wat? I hope not…
NB ivm de tijdsdruk heb ik BBR alvast mijn tracks gestuurd.

5.1.2.e

Van: 5.1.2.e
Verzonden: donderdag 11 maart 2021 17:42
Aan: 5.1.2.e
CC: 5.1.2.e
Onderwerp: RE: Aftapbaarheid OTT-diensten poging 4
Bijlagen: Aftapbaarheid OTT-diensten versie 4.docx

Dag 5.1.2.e et al.,

Bijgaand ons commentaar op de brief, gaat nu parallel bij ons de lijn in. Voor de goede orde: de oorspronkelijke brief vonden we een stuk gebalanceerder. Deze nieuwe versie is met stoom en kokend water tot stand gekomen; brief (en zeker het proces hierbij) had wat ons betreft echt anders mogen. We hechten sterk aan tenminste deze wijzigingen; zonder die aanpassingen wordt medeondertekening van de stas een moeilijk verhaal.

Horen dus graag of deze tracks akkoord zijn. En andersom geldt dat zodra wij reactie hebben van de stas op deze versie, we jullie informeren.

Groet,
5.1.2.e

Van: 5.1.2.e @minjenv.nl>
Verzonden: donderdag 11 maart 2021 15:38
Aan: 5.1.2.e @minezk.nl>
CC: 5.1.2.e @minjenv.nl>; 5.1.2.e @minjenv.nl>
Onderwerp: RE: Aftapbaarheid OTT-diensten poging 4
Urgentie: Hoog

Hallo 5.1.2.e

Hierbij de versie zoals geaccordeerd door de minister. Tov versie 3 enkele nuance verschillen, deze heb ik inzichtelijk gemaakt in bijgevoegde TC versie.

Nogmaals excuses voor de verschillende versies. De spoed is bij je bekend, zou je kunnen laten weten wanneer de SEZK er naar kan kijken en met welk advies jullie de brief voorleggen?

Alvast bedankt.

Met vriendelijke groet,

5.1.2.e

M 06 5.1.2.e
5.1.2.e @minvenj.nl

Van: 5.1.2.e
Verzonden: donderdag 11 maart 2021 14:21
Aan: 5.1.2.e @minezk.nl>
Onderwerp: FW: Aftapbaarheid OTT-diensten poging 3

Hallo 5.1.2.e

Hierbij de nieuwe versie.

Met vriendelijke groet,

5.1.2.e

M 06 5.1.2.e
5.1.2.e @minvenj.nl

Van: 5.1.2.e
Verzonden: donderdag 11 maart 2021 14:17
Aan: 5.1.2.e @minjenv.nl>; 5.1.2.e @minjenv.nl>; 5.1.2.e @minjenv.nl>; 5.1.2.e @nctv.minjenv.nl>; 5.1.2.e @nctv.minjenv.nl>; 5.1.2.e @minjenv.nl>; 5.1.2.e @nctv.minjenv.nl>
CC: 5.1.2.e @minjenv.nl>; 5.1.2.e @minjenv.nl>
Onderwerp: Aftapbaarheid OTT-diensten poging 3

Nav overleg met de minister de derde versie.

Met vriendelijke groet,

5.1.2.e

M 06 5.1.2.e
5.1.2.e @minvenj.nl

Van: 5.1.2.e
Verzonden: donderdag 11 maart 2021 12:12
Aan: 5.1.2.e @minjenv.nl>; 5.1.2.e @minjenv.nl>; 5.1.2.e @nctv.minjenv.nl>; 5.1.2.e @nctv.minjenv.nl>; 5.1.2.e @minjenv.nl>

CC: 5.1.2.e @minjenv.nl>
Onderwerp: FW: Aftapbaarheid OTT-diensten versie 2 schoon

Excuus voor spam. Laatste versie.

Met vriendelijke groet,

5.1.2.e

M 06 5.1.2.e
5.1.2.e @minvenj.nl

Van: 5.1.2.e
Verzonden: donderdag 11 maart 2021 12:07
Aan: 5.1.2.e @minjenv.nl>
Onderwerp: Aftapbaarheid OTT-diensten versie 2 schoon

Hallo 5.1.2.e

Hierbij de brief.

Met vriendelijke groet,

5.1.2.e

M 06 5.1.2.e
5.1.2.e @minvenj.nl

Van: 5.1.2.e @minjenv.nl>
Verzonden: vrijdag 12 maart 2021 11:04
Aan: 5.1.2.e
CC: 5.1.2.e)
Onderwerp: Brief
Bijlagen: TK Aftapbaarheid OTT-diensten.docx

Ha 5.1.2.e

Bijgaande brief is naar de kamer gestuurd, is dus de versie geworden van voor de afstemming.

Laten we begin volgende week even met elkaar bekijken hoe verder te gaa.

Groet, 5.1.2.e

Verzonden met BlackBerry Work
(www.blackberry.com)

<hr size=2 width="100%" align=center>

Concept opzet briefing MCEV 12 maart 2021 versie 4 maart 2021

9:00 – 9:10 Introductie (lijn nota MCEV) 5.1.2.e

- Waar hebben we het over? (Wat zijn OTT-communicatiediensten, Wat is end-to-end encryptie?)
- Waartoe heeft MCEV in mei 2020 besloten?
- Welk dilemma doet zich voor? (belang opsporing en (nationale) veiligheid versus belang veilige encryptie van communicatieverkeer)Welk besluit ligt 23 maart op tafel bij MCEV?

9:10 – 9.20 Risico's van aftappen OTT-diensten 5.1.2.e

- Wat is het belang van veilige (end-to-end) encryptie?
- Wat zijn de gevolgen voor end-to-end encryptie van het aftapbaar maken van OTT-communicatiediensten?
- Wat zijn de bredere consequenties hiervan?
- Zijn er (technische) alternatieven?
- Wat zijn relevante internationale ontwikkelingen?

9:20-9:30 Gevolgen voor opsporings- en veiligheidsdiensten *NFI*

- Korte toelichting belang aftappen OTT-communicatiediensten voor opsporings- en veiligheidsdiensten.
- Welke (technische) alternatieven zijn er en zijn die werkbaar voor de opsporings- en inlichtingendiensten? Inclusief reactie op suggesties vorige spreker.
- Welke technische ontwikkelingen zijn er op dit gebied?

Aansluitend: vragen en discussie

Van: 5.1.2.e
Verzonden: vrijdag 19 maart 2021 18:06
Aan: 5.1.2.e
CC: 5.1.2.e)
Onderwerp: FW: Gesprek met partijen encryptie
Bijlagen: Inventarisatie partijen.docx; Aanbiedingsnota.docx

Categorieën: Categorie Rood

5.1.2.e

Zoals al aangekondigd in post mortem overleg met ons gisteren heeft JenV een nota in voorbereiding over hoe nu verder. Vooral procesmatig ingestoken. Feit dat nu serieus het gesprek wordt gestart is wmb positief.

@5.1.2.e : benieuwd naar jullie mening, inclusief over hoe jullie op de sessie gisteren terugkijken.

Bon weekend!!
5.1.2.e

Van: 5.1.2.e @minjenv.nl>
Datum: 19 maart 2021 om 16:54:22 CET
Aan: 5.1.2.e @minezk.nl>, 5.1.2.e @minezk.nl>
CC: 5.1.2.e @minezk.nl>
Onderwerp: FW: Gesprek met partijen encryptie

Hallo 5.1.2.e en 5.1.2.e

Bijgevoegd vinden jullie mijn voorstel dat ik intern heb gedeeld. Vinden jullie hier nog iets van? Zouden jullie hier dinsdag op willen reageren?

Fijn weekend,

5.1.2.e

Met vriendelijke groet,

5.1.2.e

M 06 5.1.2.e
5.1.2.e @minvenj.nl

107a

Oproep aan kabinet: stimuleer encryptie (stimuleer-encryptie.nl)

"Wij roepen het volgende kabinet op de ontwikkeling, de beschikbaarheid en de toepassing van alle vormen van encryptie te stimuleren."

Techbedrijven	Cybersecurity	Maatschappelijk middenveld	Wetenschap
A2B Internet	Cyberveilig Nederland Belangenvereniging voor zo'n 60 bedrijven in de cybersecurity sector	Amnesty International	ACCSS Vereniging voor wetenschappers die actief zijn op het terrein van cybersecurity
AMS-IX	Dutch Institute for Vulnerability Disclosure (DIVD)	Bits of Freedom	5.1.2.e Universiteit van Amsterdam
Apple	Fox-IT	Expertisecentrum Online Kindermisbruik (EOKM)	5.1.2.e Vrije Universiteit Amsterdam
BIT	ISOC NL	Free Press Unlimited	5.1.2.e Universiteit Leiden
Facebook	Secura	Kennisnet	5.1.2.e Universiteit van Amsterdam
Freedom Internet	5.1.2.e 5.1.2.e NWO; 5.1.2.e dcypher en 5.1.2.e ACCSS	Open State Foundation	5.1.2.e 5.1.2.e Hogeschool Utrecht
Google	5.1.2.e 5.1.2.e IAB en IESG best current practice over encryptie technologie	Privacy Management Partners	5.1.2.e TU Eindhoven
KPN	5.1.2.e 5.1.2.e	Qiy Foundation	5.1.2.e Radboud Universiteit
Leaseweb Global	5.1.2.e	Stichting NLnet	5.1.2.e Universiteit van Tilburg
Microsoft		Transparency International	5.1.2.e Universiteit van Amsterdam
NXP Semiconductors		Vrijschrift	5.1.2.e TU Eindhoven
Procolix		Waag	5.1.2.e

			Universiteit Leiden en 5.1.2.e 5.1.2.e
SIDN		5.1.2.e Internet Society	5.1.2.e Universiteit van Amsterdam
Schuberg Philis		**BRANCHORGANISATIES**	5.1.2.e (CSR) Universiteit Leiden
T-Mobile		Vereniging van Onderzoeksjournalisten (VVOJ) Vereniging van zo'n 600 onderzoeksjournalisten	5.1.2.e Universiteit Twente
VodafoneZiggo		SURF Vereniging van zo'n 100 onderwijs- en onderzoeksinstellingen	5.1.2.e Universiteit Leiden
Voys en VoIPGRID		NDP Nieuwsmedia Brancheorganisatie van nieuwsmedia	5.1.2.e Open Universiteit
WhatsApp		Nederlandse Vereniging van Journalisten (NVJ) Vereniging van zo'n 8.000 journalisten en mediamakers	5.1.2.e (CSR) TU Delft
BRANCHEORGANISATIES		Dutch Startup Association	5.1.2.e Universiteit van Amsterdam
DINL Coalitie van organisaties voor een sterke digitale infrastructuur		Consumentenbond	5.1.2.e Universiteit Twente
Dutch Cloud Community Brancheverenigingen voor zo'n 80 hostingbedrijven (v/h DHPA en ISPConnect)		American Chamber of Commerce in the Netherlands	5.1.2.e Radboud Universiteit
Dutch Data Center Association Brancheorganisatie voor zo'n 120 datacenters			
NLconnect			

Brancheorganisatie van zo’n 80 bedrijven in de breedbandindustie			
NLdigital Brancheorganisatie van zo'n 600 ICT-bedrijven			
Nationale Beheersorganisatie Internet Providers (NBIP)			
Vereniging van Registrars Brancheorganisatie voor zo'n 1.250 .nl-registrars			

107b

Ministerie van Justitie en Veiligheid

MJenV

Directoraat-Generaal Rechtspleging en Rechtshandhaving
Directie Rechtshandhaving en Criminaliteitsbestrijding
Criminaliteit en Veiligheid

Turfmarkt 147
2511 DP Den Haag
Postbus 20301
2500 EH Den Haag
www.rijksoverheid.nl/jenv

Contactpersoon
5.1.2.e

T 06 5.1.2.e
E 5.1.2.e @minjenv.nl

Datum
19 maart 2021

Projectnaam
Encryptie / OTT

Ons kenmerk

nota

Gesprek ondertekenaars oproep encryptie

1 Doel nota

Akkoord op de vormgeving van het gesprek met de ondertekenaars van de oproep die het volgende kabinet aanspoort de ontwikkeling, beschikbaarheid en toepassing van alle vormen van encryptie te stimuleren.

U wordt geadviseerd om conform uw toezegging zo snel mogelijk in gesprek te gaan met een selectie van ondertekenaars van de oproep en parallel uw ambtenaren de opdracht te geven om een bredere groep ondertekenaars uit te nodigen.

Het voorstel is om ook Stas EZK uit te nodigen voor het overleg met de MJenV en ambtelijk EZK bij de ambtelijke overleggen.

U te informeren dat u op korte termijn een adviesnota ontvangt over het mogelijke vervolgproces – MCEV, formatie e.d. – voor het wetsvoorstel 5G en interceptie van OTT-communicatiediensten.

2 Aanleiding, gevraagde actie(s) en advies

In totaal hebben 75 partijen de oproep ondertekend. U heeft aangeven: "Om mogelijke misverstanden te voorkomen over ons onderzoek ben ik voornemens om nog deze maand in gesprek te gaan met vertegenwoordigers van de organisaties die hun zorgen hebben geuit."

Het advies is om met een vertegenwoordiger per belang om tafel te gaan, plus een aanvullende brancheverenigingen van de technologiesector. Daarnaast stellen we voor ook een vertegenwoordiging van de behoeftestellers(OM, politie, IenV-diensten) uit te nodigen zodat er een start kan worden gemaakt met de discussie over de mogelijkheden die er zijn en hoe passend die zijn. Ambtelijk kunnen we met meerdere vertegenwoordigers om tafel in verschillende gesprekken.

Een eerste ambtelijk overleg wordt gepland in de eerste week van april, het gesprek met de MJenV en de Stas EZK in de tweede week van april en het laatste ambtelijk overleg in de derde week van april. EZK zal ook hieraan deelnemen, gelet op de verantwoordelijkheid voor communicatieverkeer en de Telecomwet.

Voor techbrijven zou dat Facebook als OTT zijn en de brancheverenigingen NLdigital als mede initiator van de oproep. Voor cybersecurity kan 5.1.2.e worden uitgenodigd (hij was tevens aanwezig bij het gesprek in februari 2020 met dhr. 5.1.2.e Vanuit het maatschappelijk middenveld kan Bits of Freedom worden

uitgenodigd als mede initiator van de oproep, en vanuit de wetenschap 5.1.2.e 5.1.2.e

Directoraat-Generaal Rechtspleging en Rechtshandhaving
Directie Rechtshandhaving en Criminaliteitsbestrijding
Criminaliteit en Veiligheid

Datum
19 maart 2021

Ons kenmerk

3 Toelichting op het advies

Er zijn alternatieve manieren om vorm te geven aan het gesprek u kunt eerst uw ambtenaren opdracht geven om met een bredere groep ondertekenaars te spreken zodat een grotere groep belanghebbenden gehoord wordt door het ministerie. Uitkomsten van dit gesprek kunnen dienen voor het vervolggesprek met de MJenV. Gevolg is dat het gesprek met de MJenV verder in de toekomst ligt. Tevens kunnen ondertekenaars op basis van de brief een gesprek met de MJenV verwachten. Door deze twee typen gesprekken parallel te houden wordt de vaart in het traject gehouden en wordt recht gedaan aan de toezegging.

De insteek van de gesprekken is primair om de zorgen uit het veld aan te horen en deze waar mogelijk te adresseren en deze mee te nemen in de besluitvorming over de invulling van het verdere traject. Secundair, wordt meer toelichting gegeven bij de zorgvuldige aanpak waarin de verschillende belangen moeten worden gewaarborgd en in evenwicht worden gebracht. Op deze manier kan de minister zijn vertrekpunt, aanpak en wenselijk einddoel schetsen. Tot slot kunnen de gesprekken worden gebruikt om met de verschillende stakeholders te bezien of er (alternatieve) technologische mogelijkheden zijn die de moeite van het verkennen waard zijn.

4 Dilemma's

Wanneer een selectie wordt gemaakt van de ondertekenaars kunnen partijen het gevoel hebben niet te worden gehoord, tegelijkertijd kan geen contact met 75 partijen tegelijkertijd worden onderhouden. Voor de ambtelijke gesprekken is gekozen voor een groep belangen die (op andere beleidsterreinen) al regelmatig contact hebben met de overheid. Zie hiervoor de bijlage.

Ook is overwogen om eerst de ambtelijke gesprekken af te wachten voor het gesprek met de minister te plannen, maar naast bovengenoemde gevolgen in de toelichting zou dit ook tot het gevolg kunnen hebben dat men het gevoel heeft niet te worden uitgenodigd bij de MJenV vanwege hun houding in het ambtelijke gesprek.

5 Politieke en bestuurlijke context

Het gesprek met de belanghebbenden is een voorwaarde voor het vervolg van het traject voor de aftapbaarheid van OTT-communicatiediensten en de rechtmatige toegang tot versleuteld bewijs. Dit is een politiek gevoelig traject en op bestuurlijk vlak raakt die vele belangen (fundamentele rechten, cybersecurity, de technologiesector, buitenlands beleid, opsporing en nationale veiligheid). Het is noodzaak dat de gevoelde urgentie gepaard gaat met de nodige zorgvuldigheid waar de betrokken belangen zich gehoord en vertegenwoordigd voelen. Het betrekken van deze belangen komt een weloverwogen besluitvorming ten goede. In het vervolgtraject kunnen wetenschap, bedrijfsleven en behoeftestellers periodiek worden betrokken. In dat kader is ook de Europese dimensie relevant, aangezien in de Raadsconclusies van 14 december jl. de Commissie is gevraagd samen met het bedrijfsleven en de wetenschap een inventarisatie uit te voeren naar technische mogelijkheden voor rechtmatige toegang tot versleuteld bewijs.

6 Communicatie

Directoraat-Generaal Rechtspleging en Rechtshandhaving
Directie Rechtshandhaving en Criminaliteitsbestrijding
Criminaliteit en Veiligheid

Datum
19 maart 2021

Ons kenmerk

Media aandacht wordt verwacht indien de inhoud van de gesprekken naar buiten komt.

7 Afstemming
NCTV, EZK

8 Bijlagen

1) Voorstel deelnemers ambtelijke overleggen:

Er worden twee gesprekken gepland waarbij elk gesprek 10 personen worden uitgenodigd en waar een gemixte vertegenwoordiging zit van de betrokken belangen. Genodigden zijn:

Tech bedrijven
1 Apple
2 Facebook (tevens bij MJenV)
3 Google
4 Microsoft
5 KPN
6 Tmobile
7 VodafoneZiggo
8 NLdigital (tevens bij MJenV, initiator oproep)
9 DINL (coalitie van organisaties voor een sterke digitale infrastructuur)

Cybersecurity
1 Cyberveilig Nederland (Belangenvereniging voor zo'n 60 bedrijven in de cybersecurity sector)
2 5.1.2.e (tevens bij MJenV)
3 Fox IT

Maatschappelijk middenveld
1 Amnesty international
2 Bits of Freedom (tevens bij MJenV)
3 Expertisecentrum Online Kindermisbruik
4 5.1.2.e Internet Society
5. NLNet (stichting die tot doel heeft: het bevorderen van elektronische informatie-uitwisseling en al hetgeen daarmee verband houdt of daartoe bevorderlijk kan zijn.

Wetenschap
1 5.1.2.e CSR, tevens bij MJenV, Radboud Universiteit)
2 5.1.2.e (Universiteit Tilburg)
3 5.1.2.e (CSR, Leiden Universiteit)
4 5.1.2.e (CSR, Technische Universiteit Delft)

2) Overzicht ondertekenaars oproep in aparte bijlage

Directoraat-Generaal Rechtspleging en Rechtshandhaving
Directie Rechtshandhaving en Criminaliteitsbestrijding
Criminaliteit en Veiligheid

Datum
19 maart 2021

Ons kenmerk

Van: 5.1.2.e @minjenv.nl>
Verzonden: dinsdag 30 maart 2021 15:21
Aan: 5.1.2.e
CC: 5.1.2.e
Onderwerp: Afstemmen fiche interceptie OTT
Bijlagen: VERTROUWELIJK 200330 Concept fiche OTT interceptie.docx

Categorieën: Categorie Rood

Dag heren,

5.1.2 e en ik hebben bijgesloten fiche opgesteld over de interceptie van communicatie via OTT-communicatiediensten, omdat we de kans reëel achten dat het onderwerp in de formatie aan bod kan komen. Dat stemmen we hierbij graag met jullie af. Het voorstel - verkennen van technische oplossingen - is denken wij in ook in lijn met het vervolg dat jullie voor ogen hebben.

Ik hoor graag uiterlijk aanstaande vrijdag of vanuit EZK het fiche kan worden gesteund.

Dank!

Groet,

5.1.2.e

Van: 5.1.2.e
Verzonden: donderdag 1 april 2021 18:07
Aan: 5.1.2.e
CC: 5.1.2.e
Onderwerp: RE: VERTROUWELIJK 200330 Concept fiche OTT interceptie
Bijlagen: VERTROUWELIJK 200330 Concept fiche OTT interceptie (002) 5.1.2 [6557].docx

Categorieën: Categorie Rood

Thx all,

Tot slot ook mijn inbreng. Denk dat we mooi op één lijn zitten!

@5.1.2 e kan je alle comments even nalopen en onze interne reacties op elkaar samensmeden tot steeds één comment per relevante passage? Daarna kan ie wmb door.

Grt en dank,
5.1.2.e

PS Ik cc ook 5.1.2.e even omdat hij onze vriend 5.1.2.e nog wel eens tegen het lijf loopt, fysiek dan wel virtueel.

Van: 5.1.2.e
Verzonden: woensdag 31 maart 2021 15:20
Aan: 5.1.2.e
CC: 5.1.2.e
Onderwerp: RE: VERTROUWELIJK 200330 Concept fiche OTT interceptie

En de mijne

Van: 5.1.2.e @minezk.nl>
Verzonden: woensdag 31 maart 2021 12:15
Aan: 5.1.2.e @minezk.nl>; 5.1.2.e @minezk.nl>; 5.1.2.e @minezk.nl>
CC: 5.1.2.e @minezk.nl>
Onderwerp: RE: VERTROUWELIJK 200330 Concept fiche OTT interceptie

Bijgaand mijn feedback.

Met vriendelijke groet,

5.1.2 e
Digitale Veiligheid / ePrivacy

T : +31-70 5.1.2.e
M : +31 6 - 5.1.2.e

Van: 5.1.2.e @minezk.nl>
Verzonden: woensdag 31 maart 2021 11:07
Aan: 5.1.2.e @minezk.nl>; 5.1.2.e @minezk.nl>; 5.1.2.e @minezk.nl>
CC: 5.1.2.e @minezk.nl>
Onderwerp: VERTROUWELIJK 200330 Concept fiche OTT interceptie

Ha collega's,

Hierbij mijn feedback op het formatie-fiche van JenV m.b.t. aftappen OTT's. Lukt het jullie om morgen hiernaar te kijken. Vrijdag wil JenV dit afronden.

Dank.

Groet,

5.1.2.e

Van: 5.1.2.e @minjenv.nl>
Verzonden: vrijdag 2 april 2021 11:12
Aan: 5.1.2.e
CC: 5.1.2.e
Onderwerp: WODC impact encryptie op de opsporing
Bijlagen: EZK WODC onderzoek.docx

Categorieën: Categorie Rood

Hallo 5.1.2.e en 5.1.2.e

Ik wil jullie graag op de hoogte stellen van de startnotitie die is gemaakt door het WODC in samenwerking met ons. Het is een gelaagd onderzoek. Ten behoeve van de afbaking worden onderzoekers gevraagd zaken te bestuderen waarin digitale opsporingsinformatie van grote relevantie kan zijn (of daar weer een onderscheid in te maken). Daarna wordt gekeken naar hoe vaak men versleuteld materiaal tegenkomt, of dit kan worden omzeild of doorbroken (en via welke bevoegdheden) en vervolgens wat dit betekent voor het opsporingsonderzoek. Uiteindelijk moet hier een beeld uit voorkomen wat het effect van encryptie is in de opbrengt van opsporingsonderzoeken.

Dit voorstel verstuurt het WODC naar offranten (academici, onderzoeksbureau's), zij kunnen nog aanpassingen doen in de onderzoeksopzet. In de uitvoering van het onderzoek en wie zij daar bij betrekken zijn de onderzoekers onafhankelijk. Er wordt wel een begeleidingscommissie gevormd. Namen die worden gesuggereerd zijn onder andere 5.1.2.e DRC en het WODC nemen ook deel aan de begeleidingscommissie. Deze namen zijn vertrouwelijk en een indicatie waar het WODC aan denkt om uit te nodigen. De daadwerkgelijke commissie kan dus (sterk) verschillen van deze namen.

Het WODC heeft mij gevraagd om de startnotitie niet in zijn geheel te verspreiden dus ik heb een overzicht van de hoofdpunten van de startnotitie voor jullie samengesteld. Uiteraard het verzoek om dit niet verder te verspreiden. Het WODC heeft ook gevraagd om te benadrukken dat dit een voorstel is dat aan verandering onderhevig kan zijn. Bij het presenteren van het onderzoek kunnen elementen zijn toegevoegd of afgevoerd.

Fijne dagen.

Groeten,

5.1.2 e

Van: 5.1.2.e @minjenv.nl>
Verzonden: vrijdag 9 april 2021 12:18
Aan: 5.1.2.e
CC: 5.1.2.e
Onderwerp: RE: Afstemmen fiche interceptie OTT
Bijlagen: 210409 VERTROUWELIJK Concept fiche OTT interceptie.docx; 210409 VERTROUWELIJK Concept fiche OTT interceptie_schoon.docx

Categorieën: Categorie Rood

Ha 5.1.2.e ea,

Ook dank. Zie bijgesloten versie met track changes, en een geschoonde versie. Daarin zijn ook de verzoeken tot aanpassingen meegenomen die we nog van enkele andere betrokken partijen hebben gekregen.
We ontvangen de komende week vast nog wat meer wijzigingsverzoeken en suggesties voor aanvulling. En volgende de week hoop ik ook de onderbouwde kostenraming voor het onderzoek/de verkenning toe te kunnen voegen. Als we een nieuwe versie hebben mail ik die weer ter afstemming.

Lijkt me prima om af te spreken dat het ook daarna een levend document blijft binnen het kader dat het wel om echte nieuwe inzichten of afspraken moet gaan, bijvoorbeeld uit de gesprekken van de bewindspersonen met de opstellers van de petitie.

Fijn weekend!

Groet,

5.1.2.e

Van: 5.1.2.e @minezk.nl>
Verzonden: woensdag 7 april 2021 16:34
Aan: 5.1.2.e @minjenv.nl>; 5.1.2.e @minjenv.nl>
CC: 5.1.2.e @minjenv.nl>; 5.1.2.e @minezk.nl>; 5.1.2.e @minezk.nl>
Onderwerp: RE: Afstemmen fiche interceptie OTT

Beste 5.1.2.e en collega's,

Dank voor het aangepaste stuk. Vanuit onze kant nog bijgaand een aantal aanvullende tracks. Wij zouden graag willen afspreken dat we het fiche als een levend werkdocument kunnen beschouwen, waarbij we bijvoorbeeld ook de mogelijkheid krijgen om de nodige aanvullingen te kunnen doen n.a.v. de stakeholders-sessies die gaan plaatsvinden op korte termijn.

Veel dank vast.

Groet,

5.1.2.e

Van: 5.1.2.e @minjenv.nl>
Verzonden: dinsdag 6 april 2021 09:37
Aan: 5.1.2.e @minezk.nl>; 5.1.2.e @minjenv.nl>
CC: 5.1.2.e @minjenv.nl>; 5.1.2.e @minezk.nl>; 5.1.2.e @minezk.nl>
Onderwerp: RE: Afstemmen fiche interceptie OTT

Dag 5.1.2.e e.a.,

Dank, fijn dat jullie het fiche willen steunen. Het merendeel van de tekstvoorstellen kunnen we zo overnemen. Bij een paar heb ik nog een reactie / uitleg geplaatst, zie bijlage.

Mooi ook dat jullie de commissie als gepaste optie zien. 5.2.1

We willen graag benadrukken dat we inderdaad een belang hebben bij een goede technische oplossing, maar dat dit belang uit noodzaak is geboren op basis van kennis van de opsporingspraktijk. We pleiten niet voor een oplossing omdat we nu eenmaal van de opsporing zijn. Het liefst zouden wij ook encryptie hebben waar niemand toegang toe heeft behalve de gebruikers. Kennis vanuit de praktijk leert ons echter dat dit dusdanige negatieve gevolgen kan hebben dat we gedwongen zijn om te kijken of we verschillende belangen kunnen waarborgen. De uitkomst moet aan het einde van de rit het brede maatschappelijk belang dienen.

Groet,

5.1 2.e

Van: 5.1.2.e @minezk.nl>
Verzonden: donderdag 1 april 2021 20:47
Aan: 5.1.2.e @minjenv.nl>; 5.1.2.e @minezk.nl>
CC: 5.1.2.e @minjenv.nl>; 5.1.2.e @minjenv.nl>; 5.1.2.e @minezk.nl>
Onderwerp: RE: Afstemmen fiche interceptie OTT

Hallo 5.1.2.e

Hierbij onze input op het concept-fiche. Indien onze tracks worden opgenomen kunnen wij het fiche steunen.

Goed Paasweekend vast allemaal.

Groet,

5.1.2.e

Van: 5.1.2.e @minjenv.nl>
Verzonden: dinsdag 30 maart 2021 15:21
Aan: 5.1.2.e @minezk.nl>; 5.1.2.e @minezk.nl>
CC: 5.1.2.e @minjenv.nl>; 5.1.2.e @minjenv.nl>
Onderwerp: Afstemmen fiche interceptie OTT

Dag heren,

5.1.2 e en ik hebben bijgesloten fiche opgesteld over de interceptie van communicatie via OTT-communicatiediensten, omdat we de kans reëel achten dat het onderwerp in de formatie aan bod kan komen. Dat stemmen we hierbij graag met jullie af. Het voorstel - verkennen van technische oplossingen - is denken wij in ook in lijn met het vervolg dat jullie voor ogen hebben.

Ik hoor graag uiterlijk aanstaande vrijdag of vanuit EZK het fiche kan worden gesteund.

Dank!

Groet,

5.1.2.e

Van: 5.1.2.e @minjenv.nl>
Verzonden: dinsdag 20 april 2021 17:55
Aan: 5.1.2.e
CC: 5.1.2.e
Onderwerp: RE: Gesprek met partijen encryptie

Categorieën: Categorie Rood

Hallo 5.1.2.e

Het lijkt ons ook een goed idee om op korte termijn weer even bij elkaar te komen en stil te staan bij waar we staan in het traject en het gesprek met de ondertekenaars van de petitie te bespreken.

Zoals je wellicht al hebt vernomen heeft de minister aangegeven dit gesprek graag zelf te willen voeren. Dit kunnen we in het gesprek nader toelichten. Ik zal voor as donderdag een voorstel doen voor een gesprek tussen jou, 5.1.2.e en mij.

Met vriendelijke groet,

5.1.2.e

Met vriendelijke groet,

5.1.2.e

M 06 5.1.2.e
5.1.2.e @minvenj.nl

Van: 5.1.2.e @minezk.nl>
Verzonden: dinsdag 20 april 2021 16:43
Aan: 5.1.2.e @minjenv.nl>; 5.1.2.e @minjenv.nl>; 5.1.2.e @minjenv.nl>
CC: 5.1.2.e @minezk.nl>; 5.1.2.e @minezk.nl>; 5.1.2.e @minezk.nl>
Onderwerp: RE: Gesprek met partijen encryptie

Hallo 5.1.2.e

Heb jij voor ons nog actuele informatie over het verloop van het voorbereidende traject inzake de stakeholdersessies? Is de nota inmiddels geaccordeerd en zijn er nog eventuele aanpassingen aangebracht?

Vanuit EZK lijkt het ons een goed idee om eerdaags weer even te overleggen over de verdere aanpak.

Ik heb overigens vernomen van BZ dat zij nu ook aangehaakt zijn, dat vinden wij positief. Dank daarvoor.

Groet,

5.1.2.e

Van: 5.1.2.e @minjenv.nl>
Verzonden: donderdag 8 april 2021 19:15
Aan: 5.1.2.e @minezk.nl>; 5.1.2.e @minjenv.nl>; 5.1.2.e @minjenv.nl>
CC: 5.1.2.e @minezk.nl>; 5.1.2.e @minezk.nl>
Onderwerp: RE: Gesprek met partijen encryptie

Hallo 5.1.2.e

De minister had een vraag en die heb ik beantwoord. Het stuk ligt nu weer bij hem. Zodra hij akkoord is laat ik het je weten.

Lijkt mij zeker goed om de verdere vormgeving te bespreken. Laten we dat doen nadat het stuk is geaccordeerd dan kunnen we eea combineren.

Fijne avond.

Met vriendelijke groet,

5.1.2.e

M 065.1.2.e
5.1.2.e @minvenj.nl

Van: 5.1.2.e @minezk.nl>
Verzonden: woensdag 7 april 2021 17:42
Aan: 5.1.2.e @minjenv.nl>; 5.1.2.e @minjenv.nl>; 5.1.2.e @minjenv.nl>
CC: 5.1.2.e @minezk.nl>; 5.1.2.e @minezk.nl>; 5.1.2.e @minezk.nl>
Onderwerp: RE: Gesprek met partijen encryptie

Beste 5.1.2.e en collega's,

Heb jij al meer informatie m.b.t. het organiseren van de ambtelijke en politieke sessie? Wanneer zal de eerste sessie op ambtelijk niveau gaan plaatsvinden? M.b.t. de sessie op politiek niveau zullen wij namelijk ook de agenda van Stas EZK vroegtijdig moeten vastleggen.

Wat ik verder graag wil meegeven is dat wij – in het kader van samenwerking - vanuit EZK graag betrokken willen zijn bij het verder vormgeven van (de inhoudelijke voorbereiding) deze sessie, en uiteraard ook de verdere interactie met de stakeholders. Wat EZK betreft zorgen wij ervoor dat de

uitkomsten op een gedegen manier worden meegenomen in vervolgstappen, maar dat willen we natuurlijk graag ook in gesprek met Jenv uitvoeriger bespreken.

Zullen wij hiertoe op korte termijn een overleg in plannen, waarbij we ook bespreken hoe we de het doel en uitkomsten van de sessies meenemen en hoe wij de verdere interactie met het veld gaan vormgeven?

Dank vast.

Groet,

5.1.2.e

Directoraat-Generaal Bedrijfsleven en Innovatie
.....
Ministerie van Economische Zaken
Bezuidenhoutseweg 73 | 2594 AC | Den Haag
Postbus 20401 | 2500 EK | Den Haag
.....
T: +31 65.1.2.e
E: 5.1.2.e @minez.nl
.....

Van: 5.1.2.e @minjenv.nl>
Verzonden: dinsdag 30 maart 2021 17:04
Aan: 5.1.2.e @minezk.nl>
Onderwerp: RE: Gesprek met partijen encryptie

Hey 5.1.2.e

Kleine update. Door een technische fout in ons systeem voor lijnstukken heeft de nota langer bij de 5.1.2.e gelegen dan wenselijk (het stuk was niet zichtbaar in zijn werkvoorraad). De nota is vandaag doorgezet naar de MJenV.

Groeten,

5.1.2.e

Van: 5.1.2.e @minezk.nl>
Verzonden: donderdag 25 maart 2021 12:24
Aan: 5.1.2.e @minjenv.nl>; 5.1.2.e @minezk.nl>
CC: 5.1.2.e @minezk.nl>; 5.1.2.e @minjenv.nl>; 5.1.2.e @minjenv.nl>
Onderwerp: RE: Gesprek met partijen encryptie

Hallo 5.1.2.e

Dank voor je reactie. En wij kunnen ons ook goed vinden in de door jou voorgestelde passage.

Wij kijken uit naar het vervolg, houd je ons hiervan op de hoogte s.v.p.? Veel dank.

Groet,

5.1.2.e

[redacted]
Directoraat-Generaal Bedrijfsleven en Innovatie
.....
Ministerie van Economische Zaken
Bezuidenhoutseweg 73 | 2594 AC | Den Haag
Postbus 20401 | 2500 EK | Den Haag
.....
T: +31 6[redacted]
E: [redacted]@minez.nl
.....

Van: [redacted]@minjenv.nl>
Verzonden: woensdag 24 maart 2021 17:44
Aan: [redacted]@minezk.nl>; [redacted]@minezk.nl>
CC: [redacted]@minezk.nl>; [redacted]@minjenv.nl>; [redacted]@minjenv.nl>
Onderwerp: RE: Gesprek met partijen encryptie

Ha [redacted]

Dankjewel, ik heb de voorstellen overgenomen. Op twee punten geef ik graag even een toelichting: Mbt. De politieke en bestuurlijke context heb ik de onderstaande passage toegevoegd.
Het betrekken van deze belangen komt een weloverwogen besluitvorming ten goede. In het vervolgtraject kunnen wetenschap, bedrijfsleven en behoeftestellers periodiek worden betrokken. In dat kader is ook de Euroese dimensie relevant, aangezien in de Raadsconclusies van 14 december jl. de Commissie is gevraagd samen met het bedrijfsleven en de wetenschap een inventarisatie uit te voeren naar technische mogelijkheden voor rechtmatige toegang tot versleuteld bewijs.
In jouw tekstsuggestie geef je aan dat 'het vervolgtraject moet worden vormgegeven in samenhang met …'. Daar wordt mogelijk ook in gelezen dat we het vervolgtraject samen met het bedrijfsleven en wetenschap moeten vormgeven, maar volgens mij zijn wij als bestuur verantwoordelijk voor het proces en moeten we hen daar een goede plek in geven. Het verschil zit er dus in dat als wij bijvoorbeeld een idee willen uitwerken we geen toestemming nodig hebben van de partijen die we nu aanschrijven.
Direct in antwoord op jouw vraag blijft het wat mij betreft niet bij dit ene gesprek. Tegelijkertijd moeten we ook in relatieve rust en vertrouwelijkheid verschillende onderdelen van de inventarisatie kunnen uitvoeren. Daar moeten we even een goede modus in vinden, ook afhankelijk van de voortgang… er moet immers wel iets te bespreken zijn.

Mbt. Nav jouw voorstel heb ik NLnet opgenomen in de lijst met partijen waarmee gesproken wordt, alleen niet met de minister. Als stichting vallen ze onder het maatschappelijk middenveld en daar lijkt mij Bits of Freedom de aangewezen partij als initiator van de oproep.

Met vriendelijke groet,

5.1.2.e

M 06 5.1.2.e
5.1.2.e @minvenj.nl

Van: 5.1.2.e @minezk.nl>
Verzonden: dinsdag 23 maart 2021 15:57
Aan: 5.1.2.e @minjenv.nl>; 5.1.2.e @minezk.nl>
CC: 5.1.2.e @minezk.nl>
Onderwerp: RE: Gesprek met partijen encryptie

Hallo 5.1.2.e

Dank voor het stuk. Hierbij onze aanvullingen en nog een opmerking aan de zijlijn.

Mocht je nog hierover nader willen spreken dan horen wij het graag.

Groet,

5.1.2.e

Van: 5.1.2.e @minjenv.nl>
Verzonden: vrijdag 19 maart 2021 16:54
Aan: 5.1.2.e @minezk.nl>; 5.1.2.e
@minezk.nl>
CC: 5.1.2.e @minezk.nl>
Onderwerp: FW: Gesprek met partijen encryptie

Hallo 5.1.2.e en 5.1.2.e

Bijgevoegd vinden jullie mijn voorstel dat ik intern heb gedeeld. Vinden jullie hier nog iets van? Zouden jullie hier dinsdag op willen reageren?

Fijn weekend,

5.1.2.e

Met vriendelijke groet,

5.1.2.e

M 06 5.1.2.e
5.1.2.e @minvenj.nl

Van: 5.1.2.e
Verzonden: vrijdag 19 maart 2021 13:20
Aan: 5.1.2.e @minjenv.nl>; 5.1.2.e @nctv.minjenv.nl>
CC: 5.1.2.e @minjenv.nl>; 5.1.2.e @nctv.minjenv.nl>
Onderwerp: Gesprek met partijen encryptie

Hallo 5.1.2.e en 5.1.2.e

De minister wilt deze maand in gesprek met verschillende partijen die de oproep hebben ondertekend. Ik heb de partijen verdeeld in vier onderdelen: techbedrijven, cybersecurity, maatschappelijk middenveld en wetenschap.

Voor het gesprek met de minister stel ik voor om per categorie 1 persoon uit te nodigen en voor de techbedrijven nog een branchevereniging te betrekken om recht te doen aan hun aandeel in de oproep. Als ik, leunend op parate kennis, een schifting maak van prominente vertegenwoordigers in hun categorieën/vertegenwoordigers van een bepaald belang kom ik tot de volgende verdeling.

Tech bedrijven
-Facebook als OTT
-NLdigital (initiator oproep)

Cybersecurity
5.1.2.e

Maatschappelijk middenveld
-Bits of Freedom (initiator oproep)

Wetenschap
5.1.2.e (CSR)

Het voorstel is om een eerste ambtelijk overleg te plannen in de eerste week van april, het gesprek met de MJenV in de tweede week van april en het laatste ambtelijk overleg in de derde week van april. Voorstel is om ook ambtelijk EZK aan te laten sluiten bij de gesprekken.

Kunnen jullie dinsdag op dit voorstel reageren? Dan kan het nog mee in de daaropvolgende weekendtas.

Met vriendelijke groet,

5.1.2.e

M 06 5.1.2.e
5.1.2.e @minvenj.nl

Van: 5.1.2.e @nctv.minjenv.nl>
Verzonden: maandag 26 april 2021 09:57
Aan: 5.1.2.e @minbzk.nl; 5.1.2.e @mindef.nl'; 5.1.2.e @belastingdienst.nl'; 5.1.2.e
CC: 5.1.2.e
Onderwerp: RE: Fiche OTT-communicatiediensten.

Categorieën: Categorie Rood

Beste 5.1 2.e

Wat mij betreft een uitstekende beschrijving van het dilemma en de thans voorstaande opties!

Groetjes,

5.1.2.e

Van: 5.1.2.e @minjenv.nl>
Verzonden: maandag 26 april 2021 08:51
Aan: 5.1.2.e @minezk.nl>; 5.1.2.e @om.nl>; 5.1.2.e @minbzk.nl; 5.1.2.e @minbzk.nl>; 5.1.2.e @mindef.nl' 5.1.2.e @mindef.nl>; 5.1.2.e @minbuza.nl>; 5.1.2.e @politie.nl>; 5.1.2.e @nctv.minjenv.nl>; 5.1.2.e @om.nl>; 5.1.2.e @belastingdienst.nl' 5.1.2.e @belastingdienst.nl>; 5.1.2.e @politie.nl>; 5.1.2.e @om.nl>
CC: 5.1.2.e @minjenv.nl>; 5.1.2.e @minjenv.nl>; 5.1.2.e @minjenv.nl>; 5.1.2.e @nctv.minjenv.nl>; 5.1.2.e @minjenv.nl>
Onderwerp: Fiche OTT-communicatiediensten.

Dag collega's,

Bijgesloten vinden jullie het definitieve fiche OTT-communicatiediensten.
Deze is nu ambtelijk afgestemd met alle daarin genoemde partijen. Nogmaals dank voor alle feedback.

Hierbij wil ik jullie vragen om me uiterlijk donderdag te laten weten of we deze versie kunnen indienen namens jullie organisaties; indien gevraagd door de formerende partijen. Daarna doe ik het hier de lijn in en leg ik het voor aan onze afdeling FEZ. Met de collega's van EZK heb ik afgesproken dat we eventuele relevante nieuwe inzichten uit het overleg half mei met de ondertekenaars van de encryptie-petitie nog kunnen verwerken.

Mochten we het fiche kunnen indienen en als het gehonoreerd wordt, dan zullen we in nauwe afstemming met jullie de invulling ter hand nemen. Ik kan me voorstellen dat we er dan een interdepartementale werkgroep en stuurgroep omheen vormen.

Dank!

Groet,

5.1.2.e

[redacted]
[redacted]
Tel: 06 5.1.2.e

Van: 5.1.2.e
Verzonden: maandag 26 april 2021 17:56
Aan: 5.1.2.e
Onderwerp: RE: 260420 VERTROUWELIJK Fiche OTT interceptie (002)

Categorieën: Categorie Rood

Goeie vraag 5.1.2.e Of dit in het fiche aan de orde moet komen weet ik alleen niet; fiche spreekt zich niet over de governance en als je dat er ook nog aanhangt wordt dit toch al veel te lange fiche 5.2.1) helemaal een gedrocht. Maar we kunnen het zeker suggereren.

Overigens is het ook een optie om dit doaaier straks ipv mcev in een onderraad digitalisering te agenderen (als die er komt).

Van: 5.1.2.e @minezk.nl>
Datum: 26 april 2021 om 14:42:11 CEST
Aan: 5.1.2.e @minezk.nl>, 5.1.2.e @minezk.nl>
CC: 5.1.2.e @minezk.nl>
Onderwerp: RE: 260420 VERTROUWELIJK Fiche OTT interceptie (002)

Hi 5.1.2.e
Paar kleine dingen.

In het doc staan betrokken organisaties vermeld maar niet hoe dit cruciaal het proces geregiseerd wordt.
Is er ihkv MCEV (AZ) nergens vermeld dat J&V samen met EZK hier werk van moeten maken ? dus dat EZK bewindspersoon weldegelijk betrokken moet zijn, te meer hier telecom/eprivacy aan de orde is ?
Met vriendelijke groet,

5.1.2 e
Digitale Veiligheid / ePrivacy
T : +31-70 - 5.1.2.e
M : +31 6 5.1 2.e

Van: 5.1.2.e @minezk.nl>
Verzonden: maandag 26 april 2021 14:09
Aan: 5.1.2.e @minezk.nl>
CC: 5.1.2.e @minezk.nl>
Onderwerp: 260420 VERTROUWELIJK Fiche OTT interceptie (002)

Ha collega's,

Hierbij mijn laatste punten bij het fiche.

Gr

5.1 2.e

Van: 5.1.2.e @minjenv.nl>
Verzonden: donderdag 29 april 2021 16:48
Aan: 5.1.2.e
CC: 5.1.2.e
Onderwerp: RE: OTT fiche inbreng EZK
Bijlagen: 260420 VERTROUWELIJK Fiche OTT interceptie EZK_JenV.docx

Dag 5.1.2.e

Dank, hierbij alvast een reactie op de feedback. 5.1.2.e zal begin volgende week, als we alle input binnen hebben, nog een voorlopige eindversie maken en versturen naar alle partijen.

Groet,

5.1.2.e

Van: 5.1.2.e @minezk.nl>
Verzonden: donderdag 29 april 2021 12:09
Aan: 5.1.2.e @minjenv.nl>; 5.1.2.e @minjenv.nl>
CC: 5.1.2.e @minezk.nl>; 5.1.2.e @minezk.nl>; 5.1.2.e @minezk.nl>
Onderwerp: OTT fiche inbreng EZK

Hallo 5.1.2.e en 5.1.2.e

Hierbij de inbreng van EZK. AT zal zoals besproken maandag mogelijk nog feedback geven.

Groet,

5.1.2.e

5.1.2.e
Directoraat-Generaal Bedrijfsleven en Innovatie
.....
Ministerie van Economische Zaken
Bezuidenhoutseweg 73 | 2594 AC | Den Haag
Postbus 20401 | 2500 EK | Den Haag
.....
T: +31 6 5.1.2.e
E: 5.1.2.e @minez.nl
.....

Van: 5.1.2.e)
Verzonden: dinsdag 11 mei 2021 22:15
Aan: 5.1.2.e
Onderwerp: FW: reactie EZK VERTROUWELIJK Fiche OTT interceptie EZK_JenV aang
Bijlagen: 110521 VERTROUWELIJK Fiche OTT interceptie.docx

Ha allen,

Hierbij nieuwe fiche n.a.v. overleg van vanmiddag. Onze belangrijkste punten (1. aftappen leidt tot verzwakking end-to-end en 2. grote criminele organisaties zullen niet getroffen worden door regelgeving) zijn erin verwerkt. We kunnen dit morgenochtend bespreken, wat mij betreft zijn wij akkoord.

Gr

5.1.2.e

Verzonden vanuit Mail voor Windows 10

Van: 5.1.2.e
Verzonden: dinsdag 11 mei 2021 15:11
Aan: 5.1.2.e)
CC: 5.1.2.e)
Onderwerp: RE: reactie EZK VERTROUWELIJK Fiche OTT interceptie EZK_JenV aang
Urgentie: Hoog

Hallo 5.1.2.e en 5.1.2.e

Goed om elkaar weer te hebben gesproken.

We stellen voor om bijgevoegde versie in onze lijnen aan te bieden en te horen wat daar uit komt.

Akkoord op dit proces?

Met vriendelijke groet,

5.1.2.e

M 06 5.1.2.e
5.1.2.e @minvenj.nl

Van: 5.1.2.e @minezk.nl>
Verzonden: maandag 10 mei 2021 16:25
Aan: 5.1.2.e @minjenv.nl>

CC: 5.1.2.e @minjenv.nl>; 5.1.2.e @minezk.nl>
Onderwerp: RE: reactie EZK VERTROUWELIJK Fiche OTT interceptie EZK_JenV aang

Hallo 5.1.2.e

Dank voor je reactie. Een goed idee om morgen even in de samenwerkingsmodus het fiche door te nemen.

We willen morgen graag ook de voorbereidingen voor het gesprek van 19 mei aankaarten.

5.1.2.e kan overigens pas om 12:00 uur, kunnen jullie dan ook?

Gr.,

5.1.2.e

Van: 5.1.2.e @minjenv.nl>
Verzonden: maandag 10 mei 2021 08:29
Aan: 5.1.2.e @minezk.nl>
CC: 5.1.2.e @minjenv.nl>; 5.1.2.e @agentschaptelecom.nl>; 5.1.2.e @minezk.nl>; 5.1.2.e @minezk.nl>; 5.1.2.e @minezk.nl>; 5.1.2.e @minjenv.nl>
Onderwerp: RE: reactie EZK VERTROUWELIJK Fiche OTT interceptie EZK_JenV aang

Hallo 5.1.2.e

Dankjewel! Ik denk dat het goed is om deze voorstellen even te bespreken. We hebben meer beeld en geluid nodig bij waarom deze punten op dit punt in het proces nog zo prangend voor jullie zijn.

De punten die jullie aandragen komen voor mij over als preciseringen of een specificering op elementen die al wel benoemd zijn, wat een detailniveau oplevert die niet past bij een fiche. Er staan ook wat dingen dubbel op in.

Ook lijk je ons een opdracht voor te schrijven met het aankondigen van een zwaardere inzet op het verkennen van andere instrumenten. Dit voelt onprettig in de samenwerking en kan lezers het valse idee geven dat we dit traject in isolement doorlopen. De aandacht voor de verschillende instrumenten is er altijd en ook de toekomstige potentie wordt altijd meegenomen in de afweging of een instrument toegevoegde waarde heeft. Hier is geen zwaardere inzet voor nodig.

Voor ons overleg wil ik nog wel vragen om je begrip. Je ziet de grote hoeveelheid aan betrokken partners, velen zijn al akkoord. Afstemmen met zoveel partners is geen sinecure. Gezien de diversiteit aan partners moeten we tevreden zijn wanneer men zich voor zo'n 70%-80% in het fiche herkent. Het blijft een compromis.

Met vriendelijke groet,

5.1.2.e

M 06 5.1.2.e
5.1.2.e @minvenj.nl

Van: 5.1.2.e @minezk.nl>
Verzonden: donderdag 6 mei 2021 10:31
Aan: 5.1.2.e @minjenv.nl>
CC: 5.1.2.e @minjenv.nl>; 5.1.2.e @agentschaptelecom.nl>; 5.1.2.e @minezk.nl>; 5.1.2.e @minezk.nl>; 5.1.2.e @minezk.nl>
Onderwerp: reactie EZK VERTROUWELIJK Fiche OTT interceptie EZK_JenV aang

Hallo 5.1.2.e

N.a.v. laatste aanpassingen van 5.1.2.e in het fiche tref je hierbij onze comments en tracks aan. Wij hebben dat deze verwerkt kunnen worden zodat we een gezamenlijk stuk hebben.

Ik CC ook AT zodat AT op de hoogte is van onze reactie. Wat is nu de planning van het fiche voor de komende weken?

Groet,

5.1.2.e

Directoraat-Generaal Bedrijfsleven en Innovatie
.....
Ministerie van Economische Zaken
Bezuidenhoutseweg 73 | 2594 AC | Den Haag
Postbus 20401 | 2500 EK | Den Haag
.....
T: +31 65.1.2.e
E: 5.1.2.e @minez.nl
.....

Van: 5.1.2.e
Verzonden: woensdag 12 mei 2021 09:11
Aan: 5.1.2.e
Onderwerp: FW: Outline gesprek MJenV 19 mei

Verzonden vanuit Mail voor Windows 10

Van: 5.1.2.e
Verzonden: woensdag 12 mei 2021 09:05
Aan: 5.1.2.e
CC: 5.1.2.e
Onderwerp: Outline gesprek MJenV 19 mei

Hallo 5.1.2.e en 5.1.2.e

Ik zou nog even de outline sturen van het overleg volgende week woensdag:

Het advies is om deze spreeklijn aan te houden:
-uitgangspunt kabinet: sterke encryptie voor het beveiligen van communicatie en het in vrijheid uitoefenen van fundamentele rechten.
-voorbeelden van waar de opsporing tegen aanloopt: online handel in illegale goederen, drugshandel en grooming.
-veelbelovende technische oplossingen willen we onderzoeken, voorbeeld GCHQ. Voordelen afwegen tov de nadelen.
-Forward looking, inclusief traject, gekoppeld aan het EU-traject: in gezamenlijkheid met bedrijfsleven, academici en maatschappelijk middenveld.

Deelnemers kan worden meegegeven dat het bij voorbaat uitsluiten van het opsporingsbelang in de encryptie discussie een weloverwogen besluitvorming niet ten goede komt. De gevoelde urgentie in de opsporing is daarvoor te groot. Voor het zorgvuldig afwegen van de belangen is een inventarisatie van mogelijke oplossingen nodig. Op deze manier kunnen de gunstige effecten voor de opsporing worden afgezet tegen de gevreesde effecten die vanuit de hoek van cybersecurity en privacy worden vernomen. Twee belangen waar u als minister ook verantwoordelijkheid voor draagt.

Met vriendelijke groet,

5.1.2.e

M 06 21 5.1.2.e
5.1.2.e @minvenj.nl

Van: 5.1.2.e
Verzonden: vrijdag 14 mei 2021 09:00
Aan: 5.1.2.e
Onderwerp: Fwd: COSI 19 mei next steps on encryptie deadline maandag 1300
Bijlagen: 6. Dossiernotitie - Next steps on Encryption.docx; 6. Next steps on Encryption (st08519.en21).docx

Verstuurd vanaf mijn iPhone

Begin doorgestuurd bericht:

Van: 5.1.2.e @minjenv.nl>
Datum: 13 mei 2021 om 17:06:37 CEST
Aan: 5.1.2.e @minbuza.nl>, 5.1.2.e @minezk.nl>, 5.1.2.e @minezk.nl>, 5.1.2.e @minbzk.nl>, 5.1.2.e @om.nl)" 5.1.2.e @om.nl>, 5.1.2.e 5.1.2.e @politie.nl>, 5.1.2.e @mindef.nl, 5.1.2.e @mindef.nl, 5.1.2.e @nctv.minjenv.nl>, 5.1.2.e @minjenv.nl>
Kopie: 5.1.2.e @minjenv.nl>, 5.1.2.e @minbuza.nl, 5.1.2.e @minjenv.nl>, 5.1.2.e @minjenv.nl>
Onderwerp: COSI 19 mei next steps on encryptie deadline maandag 1300

Hallo allen,

Het Portugees vzs heeft een paper aangeboden aan COSI van 19 mei over de EU inventarisatie. Onze internationale afdeling heeft ons tot maandag 13:00 gegeven. Het is een vrij bescheiden verzoek aan de LS: steun en bijdrage aan de inzet.

Essentie boodschap

- U kunt uw steun uitspreken voor het gebalanceerde paper dat is opgesteld en de oproep om actief een bijdrage te leveren aan het aankomende proces.

Spreektekst

- *There is a great need for proportional technical solutions for lawful access to encrypted data for our investigatory powers based on domestic criminal law. We support the call presented in the paper.*
- *We underline that protecting privacy, fundamental rights and the security of communications, but also minimizing the risk of abuse by repressive regimes, should be part of the search and the possible technical solution.*
- *Also, we acknowledge the need for including private sector and academia into this effort.*

Krachtenveld

- De raadsresolutie van december 2020 is unaniem aangenomen binnen de JBZ-raad.

Samenvatting / achtergrond

- Inhoudelijk verschilt dit document niet van de raadsresolutie van december 2020 over rechtmatige toegang tot versleutelde data. Er wordt alleen van lidstaten steun en een bijdrage gevraagd voor het identificeren van mogelijke opties voor de 'way forward' en de Commissie wordt gevraagd om de delegaties periodiek te informeren.
- Sinds de publicatie van de raadsverklaring in december 2020 is de noodzaak van toegang tot versleuteld bewijs opgenomen in diverse strategieën, maar tot nu toe is via officiële kanalen weinig van de Europese Commissie vernomen.
- Waarschijnlijk wordt daarom deze oproep in COSI gepresenteerd. Via officieuze kanalen is vernomen dat aan het einde van deze maand de CIE een werkgroep opzet en vragenlijsten verspreidt.

118a

COSI
19/05/21

6. Next steps on Encryption

Dossierhouder	5.1.2.e
Document nr.	8519/21
Gevraagde handeling	Ondersteunen

Essentie boodschap

- U kunt uw steun uitspreken voor het gebalanceerde paper dat is opgesteld en de oproep om actief een bijdrage te leveren aan het aankomende proces.

Spreektekst

- *There is a great need for proportional technical solutions for lawful access to encrypted data for our investigatory powers based on domestic criminal law. We support the call presented in the paper.*
- *We underline that protecting privacy, fundamental rights and the security of communications, but also minimizing the risk of abuse by repressive regimes, should be part of the search and the possible technical solution.*
- *Also, we acknowledge the need for including private sector and academia into this effort.*

Krachtenveld

- De raadsresolutie van december 2020 is unaniem aangenomen binnen de JBZ-raad.

Samenvatting / achtergrond

- Inhoudelijk verschilt dit document niet van de raadsresolutie van december 2020 over rechtmatige toegang tot versleutelde data. Er wordt alleen van lidstaten steun en een bijdrage gevraagd voor het identificeren van mogelijke opties voor de 'way forward' en de Commissie wordt gevraagd om de delegaties periodiek te informeren.
- Sinds de publicatie van de raadsverklaring in december 2020 is de noodzaak van toegang tot versleuteld bewijs opgenomen in diverse strategieën, maar tot nu toe is via officiële kanalen weinig van de Europese Commissie vernomen.
- Waarschijnlijk wordt daarom deze oproep in COSI gepresenteerd. Via officieuze kanalen is vernomen dat aan het einde van deze maand de CIE een werkgroep opzet en vragenlijsten verspreidt.

Van: 5.1.2.e
Verzonden: maandag 17 mei 2021 14:02
Aan: 5.1.2.e
Onderwerp: FW: Fiche OTT-communicatiediensten.
Bijlagen: VERTROUWELIJK Fiche OTT interceptie 17 mei.docx

Ha collega's,

Ter info, het fiche zoals is opgesteld en wordt doorgezet. Onze belangrijkste punten zijn erin vermeld nu.

Gr

5.1.2.e

Van: 5.1.2.e @minjenv.nl>
Verzonden: maandag 17 mei 2021 13:53
Aan: 5.1.2.e @minezk.nl>; 5.1.2.e @minjenv.nl>; 5.1.2.e 5.1.2.e @om.nl>; 5.1.2.e @minbzk.nl' 5.1.2.e @minbzk.nl>; 5.1.2.e @minbzk.nl>; 5.1.2.e @mindef.nl' 5.1.2.e @mindef.nl>; 5.1.2.e @minbuza.nl>; 5.1.2.e @politie.nl>; 5.1.2.e @nctv.minjenv.nl>; 5.1.2.e @om.nl>; 5.1.2.e @belastingdienst.nl' 5.1.2.e @belastingdienst.nl>; 5.1.2.e @politie.nl>; 5.1.2.e @om.nl>; 5.1.2.e @agentschaptelecom.nl>
CC: 5.1.2.e @minjenv.nl>; 5.1.2.e @minjenv.nl>; 5.1.2.e @minjenv.nl>; 5.1.2.e @nctv.minjenv.nl>; 5.1.2.e @minjenv.nl>
Onderwerp: RE: Fiche OTT-communicatiediensten.

Dag allen,

Naar aanleiding van vorige versie zijn er nog wat opmerkingen en aanvullingen binnen gekomen en is er nog het nodige overleg geweest. De meeste wijzigingen in de tekst heb ik geel gearceerd. De bijgesloten versie ga ik zo de lijn in doen, waarna we die hopelijk definitief hebben. Enkelen van jullie gaan deze ook nog in jullie eigen lijn afstemmen begreep ik.

Dank nogmaals voor jullie input en ongeduld. Het was een zware bevalling, maar ik denk dat we een goed compromis in de tekst hebben bereikt. Ik informeer jullie als de lijn hier ook akkoord is.

Groet,

5.1 2.e

Van: 5.1.2.e
Verzonden: maandag 26 april 2021 08:51

Aan: 5.1.2.e @minezk.nl>; 5.1.2.e @om.nl>;5.1.2.e @minbzk.nl; 5.1.2.e @minbzk.nl>; 5.1.2.e @mindef.nl' 5.1.2.e @mindef.nl>; 5.1.2.e @minbuza.nl>; 5.1.2.e @politie.nl>; 5.1.2.e @nctv.minjenv.nl>; 5.1.2.e @om.nl>; 5.1.2.e @belastingdienst.nl' 5.1.2.e @belastingdienst.nl>;5.1.2.e @politie.nl>; 5.1.2.e @om.nl>
CC: 5.1.2.e @minjenv.nl>; 5.1.2.e 5.1.2.e @minjenv.nl>; 5.1.2.e @minjenv.nl>; 5.1.2.e 5.1.2.e @nctv.minjenv.nl>; 5.1.2.e 5.1.2.e @minjenv.nl>
Onderwerp: Fiche OTT-communicatiediensten.

Reeds beoordeeld in dit verzoek

Van: 5.1.2.e
Verzonden: woensdag 26 mei 2021 10:11
Aan: 5.1.2.e
Onderwerp: FW: Flits CIE vergadering encryptie 25 mei 2021

Ter info. Vooraf heb ik contact met JenV hierover.

Van: 5.1.2.e @minjenv.nl>
Verzonden: dinsdag 25 mei 2021 17:29
Aan: 5.1.2.e @minjenv.nl>; 5.1.2.e @minezk.nl>; 5.1.2.e @minezk.nl>
Onderwerp: FW: Flits CIE vergadering encryptie 25 mei 2021

Van: 5.1.2.e @minbuza.nl>
Verzonden: dinsdag 25 mei 2021 16:52
Aan: 5.1.2.e @minbuza.nl>; 5.1.2.e @minbuza.nl>; 5.1.2.e @minbuza.nl>; 5.1.2.e @minbuza.nl>; 5.1.2.e @minbuza.nl>
CC: 5.1.2.e @minbuza.nl>; 5.1.2.e @minbuza.nl; 5.1.2.e @minjenv.nl>; 5.1.2.e @minjenv.nl>
Onderwerp: Flits CIE vergadering encryptie 25 mei 2021

Hoi allen,

Op 25 mei 2021 heeft de Commissie een vergadering georganiseerd om de plannen op het gebied van **encryptie** toe te lichten:

- **Doel:** CIE verwijst naar de EU Strategie Georganiseerde Misdaad waarin staat dat in 2022 een voorstel zal worden gedaan voor de te volgen weg voor de aanpak van het probleem van rechtmatige en doelgerichte toegang tot versleutelde informatie in het kader van strafrechtelijke onderzoeken en vervolgingen. Dit voorstel zal gebaseerd worden op een inventarisatie van de wijze waarop de lidstaten omgaan met versleuteling om de concrete opties (juridisch, ethisch en technisch) te onderzoeken en te beoordelen. CIE betrekt hierin eveneens allerlei andere belanghebbenden, waaronder NGO's, (tech)bedrijven, onderzoekers en academici (steun FRA, FIN, ZWE en NL) en poogt de juiste balans te vinden tussen efficiënte opsporingen en de bescherming van fundamentele rechten.

- **Proces**: CIE heeft twee aparte vragenlijsten aan LS gedistribueerd en om input verzocht voor de deadlines van respectievelijk 25 juni (vragenlijst 1) en 16 juli (vragenlijst 2). **DUI, FRA, FIN, ZWE, NL** en **BEL** steunen het proces in algemene zin. **DUI** wijst erop dat parallel werk vermeden moet worden (de vragenlijst zou niet moeten overlappen met een andere vragenlijst die vorige week in COSI besproken had moeten worden) en benadrukt transparantie te willen wat betreft de reacties van LS. **NL** stelt dat alle opties geanalyseerd dienen te worden en beaamt de noodzaak van transparantie. CIE doet hierop een voorstel om de antwoorden op niet-gevoelige vragen te delen onder LS (uiteraard met goedkeuring van LS).

- **Volgende stappen**: CIE zal de antwoorden op de vragenlijsten gedurende de zomer analyseren, waarna het in de herfst van dit jaar een tweede vergadering zal organiseren. Gedurende deze sessie kan verder besproken worden welke informatie exact gedeeld kan worden en met wie. CIE zal in de herfst ook starten met een consultatie richting andere belanghebbenden.

Vriendelijke groet,
5.1.2.e

[redacted]
Criminal justice, data protection, e-Justice

Permanent Representation of the
Kingdom of the Netherlands to the European Union
Avenue de Cortenbergh 4-10
1040 Brussels, Belgium

M: +32 5.1.2.e
Email: 5.1.2.e @minbuza.nl

Dit bericht kan informatie bevatten die niet voor u is bestemd. Indien u niet de geadresseerde bent of dit bericht abusievelijk aan u is toegezonden, wordt u verzocht dat aan de afzender te melden en het bericht te verwijderen. De Staat aanvaardt geen aansprakelijkheid voor schade, van welke aard ook, die verband houdt met risico's verbonden aan het elektronisch verzenden van berichten.

Ministerie van Justitie en Veiligheid

This message may contain information that is not intended for you. If you are not the addressee or if this message was sent to you by mistake, you are requested to inform the sender and delete the message. The State accepts no liability for damage of any kind resulting from the risks inherent in the electronic transmission of messages.

Ministry of Justice and Security

Van: 5.1.2.e
Verzonden: donderdag 3 juni 2021 17:40
Aan: 5.1.2.e
CC: 5.1.2.e
Onderwerp: RE: bouwstenen voor de ambtelijke sessies v2
Bijlagen: 210603 bouwstenen voor de ambtelijke sessies v2.docx

Categorieën: Categorie Rood

Hierbij mijn opmerkingen en tracks. NB heb me daarbij in hoige mate laten leiden door de opzet en formuleringen die we hanteerden in de agenda voor de briefing tijdens de MCEV dit vroege voorjaar, die uiteindelijk niet doorging. Ik zie dat zij die ook alks basis hanteren maar daar aan hebben gesleuteld. Ik zou willen vasthouden aan wat we toen hebben afgesproken (na intensief overleg…).

5.1.2.e

Van: 5.1.2.e @minezk.nl>
Verzonden: donderdag 3 juni 2021 14:59
Aan 5.1.2.e @minezk.nl>
CC: 5.1.2.e @minezk.nl>; 5.1.2.e @minezk.nl>
Onderwerp: bouwstenen voor de ambtelijke sessies v2

Ha 5.1.2.e

Hierbij versie 2 van de bouwstenen met daarin verwerkt opmerkingen van 5.1.2.e Er zijn nu 2 sessies voorzien ivm grootte deelnemerslijst.

Ik heb een aantal bespreekpunten geformuleerd (mede n.a.v. input 5.1.2.e die ik volgende week met JenV wil bespreken ter voorbereiding van de sessies.

Gr

5.1.2.e

Van: 5.1.2.e
Verzonden: donderdag 3 juni 2021 18:28
Aan: 5.1.2.e
Onderwerp: FW: ambtelijke sessies
Bijlagen: 210603 bouwstenen voor de ambtelijke sessies EZK JenV.docx

t.i.
gr. 5.1.2

Van: 5.1.2.e @minezk.nl>
Verzonden: donderdag 3 juni 2021 18:27
Aan: 5.1.2.e @minjenv.nl>; 5.1.2.e @minjenv.nl>
CC: 5.1.2.e @minezk.nl>
Onderwerp: ambtelijke sessies

Beste allen,

Bijgaand, zoals door 5.1.2.e eind verleden week gemaild, onze beelden/insteek mbt ambtelijke sessies. Zullen we volgende week een moment prikken ?

Groet,
5.1.2.e

Met vriendelijke groet,

5.1.2 e
Digitale Veiligheid / ePrivacy

T : +31-70 - 5.1.2.e
M : +31 6 - 5.1 2.e

Van 5.1.2.e @minezk.nl>
Verzonden: woensdag 2 juni 2021 15:49
Aan: 5.1.2.e @minjenv.nl>; 5.1.2.e @minjenv.nl>
CC: 5.1.2.e @minezk.nl>
Onderwerp: ambtelijke sessies

Ha 5.1.2.e en 5.1.2.e

Alvast een heads-up. Jullie ontvangen morgen enkele gedachtegangen mbt invulling van de ambtelijke sessies. Is het een idee om de week erop weer bijeen te komen?

Gr

5.1.2.e

Directoraat-Generaal Bedrijfsleven en Innovatie
.....
Ministerie van Economische Zaken
Bezuidenhoutseweg 73 | 2594 AC | Den Haag
Postbus 20401 | 2500 EK | Den Haag
.....
T: +31 5.1.2.e
E: 5.1.2.e @minez.nl
.....

Van: 5.1.2.e
Verzonden: woensdag 9 juni 2021 10:16
Aan: 5.1.2.e
Onderwerp: RE: reactie Stas en Staske

Helemaal mee eens,

Was ook mijn voorstel om hackbevoegdheid daarin mee te nemen.

Met vriendelijke groet,

5.1.2.e
Digitale Veiligheid / ePrivacy

T : +31-70 -5.1.2.e
M.: +31 6 -5.1.2.e

Van: 5.1.2.e @minezk.nl>
Verzonden: woensdag 9 juni 2021 09:59
Aan: 5.1.2.e @minezk.nl>; 5.1.2.e @minezk.nl>; 5.1.2.e @minezk.nl>
Onderwerp: reactie Stas en Staske

Collega's,

5.2.1

Gr

5.1.2.e

Directoraat-Generaal Bedrijfsleven en Innovatie
.....
Ministerie van Economische Zaken
Bezuidenhoutseweg 73 | 2594 AC | Den Haag
Postbus 20401 | 2500 EK | Den Haag
.....
T: +31 5.1.2.e
E: 5.1.2.e @minez.nl
.....

Van: 5.1.2.e
Verzonden: woensdag 9 juni 2021 10:17
Aan: 5.1.2.e
Onderwerp: RE: reactie Stas en Staske

Categorieën: Categorie Rood

Nuttige aanwijzingen. Kunnen we allebei inbrengen bij JenV. Fiche zou immers een levend document blijven. Morgen tijdens ons overlegje maar even over hebben.

5.1.2.e

Van: 5.1.2.e
Verzonden: woensdag 9 juni 2021 09:59
Aan: 5.1.2.e
Onderwerp: reactie Stas en Staske

Reeds beoordeeld in dit verzoek

Van: 5.1.2.e
Verzonden: donderdag 10 juni 2021 16:32
Aan: 5.1.2.e
Onderwerp: FW: Uitnodiging CSR Vergadering 17 juni 2021 - Agendapunt 'Encryptie'
Bijlagen: Bijlage 4.1 - Oplegnota Encryptie.pdf; Bijlage 4.2 - Achtergrond over tapbare digitale communicatie.pdf

Categorieën: Categorie Rood

Van: Secretariaat CSR
Verzonden: donderdag 10 juni 2021 11:19
Aan: 5.1.2.e
CC: 5.1.2.e Secretariaat CSR
Onderwerp: Uitnodiging CSR Vergadering 17 juni 2021 - Agendapunt 'Encryptie'

Geachte 5.1.2.e beste 5.1.2.e

Middels deze e-mail nodigen we je van harte uit voor het digitaal bijwonen van een gedeelte van de CSR Vergadering op donderdag 17 juni aanstaande.
Fijn dat je bereid bent om 5.1.2.e inhoudelijk te ondersteunen en het gesprek van de raad over dit onderwerp van input te voorzien.

Het agendapunt 'encryptie' begint op 17 juni as. rond 13.20 uur en zal circa 60 minuten duren. Ter voorbereiding is een oplegnota aan de leden verstuurd (zie bijgevoegd). Het agendapunt is als volgt opgebouwd:

- 5.1.2.e heeft een neutrale achtergrondpaper over de thematiek geschreven (zie ook bijgevoegd). Hij zal een korte toelichting geven ter inleiding.
- DGRR geeft een korte inleiding
- Ter opening van de discussie geeft 5.1.2.e een korte reactie
- Vrije discussie tussen de raadsleden
- De raad eindigt met het trekken van conclusies en het bepalen van een mogelijke rol of standpunt.

De ervaring leert dat het fijn is als we externe genodigden een bericht kunnen sturen zodra zij welkom zijn de vergadering digitaal te betreden. Ik ontvang daarom graag je telefoonnummer zodat we je dit kunnen laten weten.

Een outlook invite en webex-uitnodiging ontvang je z.s.m. Deze geldt voor de gehele vergadering. Het vriendelijke verzoek is om niet in te loggen voordat je een bericht daartoe hebt ontvangen.

Mocht je nog vragen, neem dan vooral even contact op!

Met hartelijke groet,

5.1.2.e

.....
Ministerie van Justitie en Veiligheid

Cyber Security Raad
Turfmarkt 147 | 2511 DP | Den Haag
Postbus 16950 | 2500 BZ | Den Haag
.....
M 06 5.1.2.e
5.1.2.e @cybersecurityraad.nl
https://www.cybersecurityraad.nl/
.....

CSR Cyber Security Raad

Oplegnota Encryptie

Inleiding

Tijdens de CSR-vergadering van 25 maart jl. heeft demissionair minister Grapperhaus de raad verzocht zich te buigen over het onderwerp encryptie en bij te dragen aan oplossingen. Dit is de aanleiding om dit onderwerp te agenderen voor de vergadering van 17 juni. De bespreking in de raad heeft een oriënterend karakter.

Ter voorbereiding op de vergadering heeft 5.1.2.e een neutrale notitie over dit onderwerp opgesteld. Deze notitie is meegestuurd met de vergaderstukken.

Om kennis te kunnen nemen van de verschillende invalshoeken zijn voor dit agendapunt twee gasten uitgenodigd. Het onderwerp encryptie is binnen het ministerie van Justitie en Veiligheid belegd bij het Directoraat-Generaal Rechtspleging en Rechtshandhaving (DRRR). Namens DGRR is 5.1.2.e uitgenodigd en zij zal een korte inleiding geven. Vanuit het ministerie van Economische Zaken en Klimaat neemt 5.1.2.e voor dit onderdeel deel aan de vergadering.

Opzet dialoog

De dialoog over encryptie wordt ingeleid door 5.1.2.e gevolgd door 5.1.2.e waarna vervolgens de dialoog start. Het gesprek wordt afgesloten met de belangrijkste conclusies, waaronder de beantwoording van de vraag wat de raad met dit onderwerp wil.

Gevraagde beslissing:

- *Wil de raad een officieel standpunt innemen over dit onderwerp?*

Achtergrond over tapbare digitale communicatie

Door: 5.1.2.e

Inleiding voor CSR, 17 juni 2021

In de fysieke wereld kan een burger niet echt iets voor de overheid geheimhouden wanneer die alle beschikbare machtsmiddelen in mag zetten. Met snijbranders en slijptollen is meestal wel toegang tot een brandkast te krijgen. Het bij de betrokkene opeisen van de sleutel van de brandkast mag niet, vanuit het *nemo tenetur*-beginsel: niemand is gehouden tegen zichzelf bewijs te leveren. Er mag wel gezocht worden naar de sleutel. In de digitale wereld daarentegen kan iedereen met eenvoudige digitale middelen een "brandkast" voor een geheim maken, via versleuteling/encryptie waar niemand bij kan, behalve degene die de (cryptografische) sleutel bezit. De laagdrempelige beschikbaarheid van zulke sterke versleuteling heeft voor- en nadelen, waar we als samenleving mee moeten leren leven. Voor zowel de *good guys* als de *bad guys* is versleuteling essentieel geworden, voor de eigen bescherming. Afgedwongen verzwakking van bepaalde vormen van versleuteling zal het gebruik van andere (eigen) vormen van encryptie bevorderen. In 2016 heeft het kabinet het brede belang van versleuteling erkend.

Bij traditionele telefonie is er sprake van centrale knooppunten, onder controle van telecomaanbieders, waar alle communicatie voorbij komt en waar taps geplaatst kunnen worden, onder nationale jurisdictie. Daar zijn telefoniecentrales voor ingericht, via internationale standaarden. Moderne berichtendiensten, zoals WhatsApp, Signal, Telegram en iMessage, werken via internet en zijn zogenaamde *over-the-top* (OTT) diensten, waardoor er geen nationale tappunten zijn. Bovendien gebruiken ze sinds een paar jaar allemaal *end-to-end-encryption* (E2EE). Het tapbaar maken van zulke OTT-diensten vereist bijzondere technische en organisatorische maatregelen.

De versleuteling van Signal is open source en werkt transparant. Dat is essentieel voor het vertrouwen van gebruikers. WhatsApp heeft deze (open) aanpak gekopieerd. Technisch zijn er wel mogelijkheden te verzinnen om zulke versleuteling gericht tapbaar te maken – bijv. via *golden keys* of via *partial key escrow* – maar daar zal eerst brede overeenstemming over moeten ontstaan tussen overheden, bedrijven en academici. Zulke technieken moeten in internationale open standaarden opgenomen worden. Dat vergt misschien wel tien jaar. Maar stel dat dat technisch allemaal lukt. Dan kunnen we een mondiale interceptie-infrastructuur bouwen. Is de mensheid daaraan toe? Is er overeenstemming te krijgen over welke landen deze tap-infrastructuur voor welke delicten mogen gebruiken? Wie beheert dat? Mogen China en Rusland, of Turkije, Israël en Polen er ook bij? Mag bewijs daaruit leiden tot doodstraffen? Mogen OTT-taps dan *wel* ingezet worden bij relatief oncontroversiële zaken als moord en doodslag en kinderporno, maar *niet* bij politiek gevoeligere beschuldigingen van terrorisme of staatsondermijnende activiteiten?

De aanpak van kinderporno en zware criminaliteit wordt vaak genoemd als argument om OTT-diensten tapbaar te maken. Maar harde informatie ontbreekt om de effectiviteit daarvan te onderbouwen. In Nederland gaat het WODC gaat eerst nog onderzoek doen. Producenten en consumenten van kinderporno lijken meer gebruik te maken van het *dark web* dan van WhatsApp – en zullen WhatsApp zeker niet gebruiken wanneer het tapbaar is. Tegen activiteiten op het *dark web* zijn andere methoden mogelijk effectiever, zoals hacken en/of infiltratie. De afgelopen jaren is duidelijk geworden dat zware criminelen vaak (zo dom zijn om) hun eigen crypto te gebruiken – zoals Ennetcom, Encrochat, IronChat, PGP-SAFE, Sky ECC – die vervolgens door internationaal samenwerkende politiediensten gebroken wordt. Aftapbaarheid van OTT-berichtendiensten zal deze criminelen bij die diensten wegjagen en het gebruik van eigen crypto alleen maar bevorderen.

De effectiviteit van alternatieven voor tapbaarheid van OTT-diensten kan verbeterd worden. Hacken wordt door de politie nog weinig gebruikt, onder andere door de vele regels en beperkingen. Volgens WhatsApp/Facebook staat Nederland onderaan in de lijstjes van opvragingen van metadata vanuit

Europese landen. Medewerking van betrokken bedrijven zou juridisch beter geregeld kunnen worden, bijv. met expliciete reactietermijnen. De wetgeving voor online infiltratie zou verruimd kunnen worden.

Inlichtingen- en Veiligheidsdiensten hebben een eigen positie en een eigen perspectief op deze materie. Internationaal hebben de *Five Eyes* aangedrongen op aftapbaarheid van OTT-diensten. Er lijkt echter weinig animo om voor toegang van hen of hun methoden afhankelijk te zijn. Als we iets willen op dit gebied, dan is een open, transparante en bredere regeling gewenst.

In het begin van 2021 ontstond het idee om bij herziening van de Nederlandse Telecomwet (vanwege 5G) een bepaling toe te voegen om OTT-dienstverleners te verplichten tot tapbaarheid. Dat gaf aanleiding tot veel onrust en leidde tot de website stimuleer-encryptie.nl, waarop een brede coalitie van maatschappelijke organisaties, bedrijven en individuen het volgende kabinet opriep tot het stimuleren van “de ontwikkeling, de beschikbaarheid en de toepassing van alle vormen van encryptie”. Opvallend is het grote belang dat ICT-bedrijven – naast privacy-organisaties – aan versleuteling hechten. Daarmee is het onderwerp niet alleen juridisch maar ook economisch relevant voor Nederland, als vestigingsland met een betrouwbare ICT-infrastructuur. De plannen voor een OTT-clausule in de Telecomwet verdwenen. Ondertussen is er informeel overleg gaande tussen verschillende partijen. Er lijkt daarbij overeenstemming te ontstaan dat een Nederlandse *alleingang* via nationale wetgeving zin/kansloos is en dat een internationale benadering en consensus noodzakelijk zijn. Tegelijkertijd moet de discussie niet alleen gaan over mogelijke technieken en hun risico’s, maar ook over wenselijkheid en effectiviteit van afgedwongen toegang tot versleutelde gegevens in relatie tot alternatieven, ten behoeve van effectieve rechtshandhaving en vervolging, en over de vereiste internationale arrangementen die benodigd zijn voor de mogelijke realisatie van OTT-interceptie.

Van: 5.1.2.e
Verzonden: maandag 5 juli 2021 15:20
Aan: 5.1.2.e
Onderwerp: FW: Uitnodiging ambtelijk overleg toegang tot opsporingsinformatie en encryptie

Ha collega's,

Zie hieronder de gecommuniceerde opzet voor de sessies van deze week. 5.1.2.e en ik zijn blij dat JenV dit ook gewoon als een aftrap ziet voor verdere samenwerking/sessies.

Gr.

5.1.2.e

Verzonden vanuit Mail voor Windows 10

Van: 5.1.2.e
Verzonden: maandag 5 juli 2021 14:35
Aan: 5.1.2.e @google.com'; 5.1.2.e @vodafoneziggo.com'; 5.1.2.e @eokm.nl'; 5.1.2.e @nlnet.nl'; 5.1.2.e @fgga.leidenuniv.nl'; 5.1.2.e 5.1.2.e 5.1.2.e 5.1.2.e @isoc.org'; 5.1.2.e @tilburguniversity.edu'
CC: 5.1.2.e 5.1.2.e
Onderwerp: RE: Uitnodiging ambtelijk overleg toegang tot opsporingsinformatie en encryptie

Beste genodigden,

Deze week spreken we over toegang tot opsporingsinformatie en encryptie. Wij zouden nog even terugkomen met wat punten waarvan wij hopen dat we deze kunnen bespreken. Het staat u uiteraard geheel vrij om zelf de punten naar voren te brengen die u wilt.

Ik zal beginnen met een toelichting op het proces dat we zijn ingegaan en de manier waarop we verschillende betrokken legitieme belangen, zoals cybersecurity, privacy en opsporing, benaderen. Vervolgens zouden wij de sessies van 7 en 8 juli graag willen benutten om te bespreken hoe we deze belangen kunnen dienen.

Het is hierbij belangrijk om onderscheid te maken in de verschillende toepassingen van encryptie, bijvoorbeeld de toegang tot een in beslaggenomen apparaat, interceptie van communicatie via een OTT-communicatiedienst of opgeslagen gegevens. Centraal in dit traject staat de interceptie van communicatie via OTT-communicatiediensten, maar indien u mogelijkheden ziet bij de andere toepassingen dan vernemen we deze graag.

Wij horen graag of en welke technische oplossingen u ziet om toegang tot versleutelde opsporingsinformatie mogelijk te maken, welke risico's er bestaan wanneer het gaat om het aanpassen van encryptie en of u ook alternatieven ziet om aan het opsporingsbelang tegemoet te komen.

Het overleg duurt een uur en is bedoeld als introductie. Op basis van de gesprekken zullen we nagaan of er behoefte is aan een vervolg en hoe hieraan het beste vorm kan worden gegeven.

We zullen geen voorstel rondje doen, deelnemers wordt gevraagd om de organisatie te noemen wanneer ze voor het eerst het woord nemen. De indeling is als volgt:

-introductie minJenV
-elke externe genodigde krijgt het woord en mogelijkheid tot vragen
-toelichting/beantwoording vragen
-mogelijkheid tot vervolgvragen via 'hand opsteken' voor alle genodigden
-afronding

We kijken uit naar een goed gesprek.

Met vriendelijke groet,

5.1.2.e

M 06 5.1.2.e
5.1.2.e @minvenj.nl

-----Oorspronkelijke afspraak-----
Van: 5.1.2.e
Verzonden: dinsdag 22 juni 2021 10:00
Aan: 5.1.2.e @google.com'; 5.1.2.e
5.1.2.e @vodafoneziggo.com'; 5.1.2.e @eokm.nl'; 5.1.2.e @nlnet.nl';
5.1.2.e @fgga.leidenuniv.nl'; 5.1.2.e
5.1.2.e @minezk.nl); 5.1.2.e
5.1.2.e @isoc.org'; 5.1.2.e @tilburguniversity.edu'
CC: 5.1.2.e
Onderwerp: Uitnodiging ambtelijk overleg toegang tot opsporingsinformatie en encryptie
Tijd: donderdag 8 juli 2021 13:00-14:00 (UTC+01:00) Amsterdam, Berlijn, Bern, Rome, Stockholm, Wenen.
Locatie: Webex

-- Do not delete or change any of the following text. --

When it's time, join your Dutch Government Video Meeting here.

Meeting number (access code): 175 484 0979
Meeting password: 5.1.2.e

Join meeting

Tap to join from a mobile device (attendees only)
+31-5.1.2.e ,,1754840979## Netherlands Toll
+1-6 5.1.2.e ,1754840979## United States Toll

Join by phone
+31-5.1.2.e Netherlands Toll
+1-650-5.1.2.e United States Toll
Global call-in numbers

Join from a video system or application
Dial 1754840979@rijksvideo.webex.com
You can also dial 62.109.219.4 and enter your meeting number.

Join using Microsoft Lync or Microsoft Skype for Business

Dial 1754840979.rijksvideo@lync.webex.com

If you are a host, click here to view host information.

Need help? Go to http://help.webex.com

Verslag - Ambtelijk overleg toegang tot opsporingsinformatie en encryptie 07/07/21

- JenV introduceert de insteek van de verkenningen die nu in EU verband en deels op nationaal niveau lopen. De nationale verkenning heeft aanleiding gegeven voor de petitie. Doel van de verkenning is het vinden en uitwerken van technische mogelijkheden voor toegang tot versleutelde informatie, waaronder communicatie via OTT-communicatiediensten, ten behoeve van de opsporing en vervolging en het afwegen van de voor- en nadelen daarvan. JenV geeft het vertrekpunt van de inventarisatie weer: data wordt dankzij de digitalisering steeds belangrijker voor de opsporing en vervolging, tegelijkertijd staat de toegang hiertoe onder druk door steeds betere versleuteling die vaak standaard wordt aangeboden. Daarbovenop zijn er aanpalende discussies die de toegang tot data beïnvloeden, zoals het beginsel van dataminimalisatie waardoor organisaties minder opslaan. De vraag is hoe we bestaande bevoegdheden effectief kunnen houden in het digitale domein. Daarbij worden de grote belangen van cybersecurity, privacy en opsporing meegenomen en gezocht naar mogelijkheden waarbij deze in balans zijn en worden gewaarborgd.
- Er is bij de partijen begrip voor het belang van de opsporing bij het kunnen krijgen van toegang tot versleutelde informatie en dat de overheid hier onderzoek naar doet.
- Partijen geven aan dat de oplossing om daarvoor de beveiliging/encryptie te laten aanpassen/verzwakken, te veel risico's met zich mee brengt en dus geen goede optie is. De volgende argumenten kwamen hierbij naar voren:
    - Malafide partijen zullen ook gebruik maken van de 'achterdeur' die wordt gecreëerd wanneer de beveiliging wordt verzwakt.
    - De technologie om end-to-end encryptie te bewerkstelligen is gemakkelijk te implementeren en veelvuldig beschikbaar. Criminelen kunnen daarmee eenvoudig hun communicatie versleutelen, dus het is deels een verschuiving van het probleem.
    - Het brengt grote risico's met zich mee wat betreft het waarborgen van privacy.
    - Het kan innovatie belemmeren.
    - In EU verband wordt ook het vraagstuk van Polen en Hongarije benadrukt.
    - Het tast het vertrouwen in die diensten aan, 'vertrouwen is key'.
    - De garantie dat geen derde partij meekijkt in de communicatiestroom is weg, hierbij is geen sprake meer van zuivere end-to-end versleuteling.
    - Wanneer verkeerde partijen aan de macht komen kan er misbruik van worden gemaakt.
    - Het is praktisch gezien moeilijk te bewerkstelligen.
- Mede om deze redenen is het initiatief stimuleer-encryptie.nl opgezet en gesteund, dit is breder dan alleen de bescherming van OTT-communicatie en steunt de versterking van encryptie in brede zin.
- Vanuit private organisaties luidt de wens om het probleem vanuit een ander perspectief te bekijken, waarbij het toegang krijgen door end-to-end encryptie te wijzigen/verzwakken niet als mogelijkheid wordt beschouwt. Er zijn veel alternatieve bevoegdheden die ook mogelijkheden bieden. Het ontsleutelen van berichten door de overheid zelf (hacken), zoals recentelijk bij PGP berichten is gebeurt, wordt als de belangrijkste optie gezien. Ook beschikbaarheid en analyse van meta-data wordt benoemd. Daarnaast wordt opgeroepen om via publiek-private-samenwerking te kijken naar wat nog meer mogelijk is qua alternatieven.
- Overheidspartijen reageren dat hacken zeker een middel is dat in potentie deels kan voorzien in het verkrijgen van toegang, maar geen volwaardig alternatief is. Zo kost het ontsleutelen veel tijd en middelen, moet er ook gebruik van zwakheden in de beveiliging worden gemaakt en is er geen betrouwbare en voorspelbare toegang. Het is dus zeker geen effectieve optie bij acute dreigingen. Wat meta-data betreft zien we een ontwikkeling dat die ook steeds minder beschikbaar is, omdat regelgeving om deze te bewaren steeds strenger wordt en een bewaarplicht juridisch niet kan. JenV benadruk dat deze inventarisatie tot doel heeft geïnformeerde besluitvorming mogelijk te maken. Het belang van de opsporing tot informatie, en daarmee ook versleutelde informatie, is een legitiem belang dat onderzocht moet kunnen worden.
- De deelnemers concluderen op basis van deze eerste gedachtewisseling dat er behoefte is aan een vervolgoverleg. Deelnemers roepen op dat er een neutrale inventarisatie van de mogelijkheden moet plaatsvinden om geïnformeerde besluitvorming en uiteindelijk draagvlak te garanderen. Er is bij alle deelnemers animo om hierover te zijner tijd nader van gedachten te wisselen en een bijdrage te leveren aan de verkenning. JenV zal daartoe het initiatief nemen op een gepast moment. Vermoedelijk zal dat in het najaar zijn.

Verslag - Ambtelijk overleg toegang tot opsporingsinformatie en encryptie 08/07/21

- JenV introduceert de insteek van de verkenningen die nu in EU verband en deels op nationaal niveau lopen. De nationale verkenning heeft aanleiding gegeven voor de petitie. Doel van de verkenning is het vinden en uitwerken van technische mogelijkheden voor toegang tot versleutelde informatie, waaronder communicatie via OTT-communicatiediensten, ten behoeve van de opsporing en vervolging en het afwegen van de voor- en nadelen daarvan. Daarbij worden de grote belangen van cybersecurity, privacy (en andere fundamentele rechten) en opsporing meegenomen en gezocht naar mogelijkheden waarbij deze allen gewaarborgd en in balans zijn.
- De petitie ondertekenaars geven aan dat de discussie al lange tijd loopt, meer dan 25 jaar, en al die tijd is er een vrees bij de opsporingsdiensten dat ze geen toegang meer hebben tot gegevens, en daarom willen ze achterdeuren inbouwen. Als je encryptie verzwakt, werkt het echter averechts. Het zorgt voor een vermindering van veiligheid van burgers en bedrijven en het werkt ook niet voor de effectievere opsporing van misdadigers. Alleen ´domme´ misdadigers zullen hierbij in het vizier komen. Expert criminelen zullen zelf end-to-end encryptie toepassingen maken en gebruiken. Het lost het probleem niet op: "er is geen probleem als er geen oplossing is". We hebben meer veiligheid door encryptie nodig, niet minder.
- Verder wordt de internationale component van het vraagstuk benoemd. Als je iets tot stand wil brengen moet het internationaal. Het probleem is dat landen zoals Hongarije, Polen en met repressieve regimes een dergelijk initiatief met open armen zullen ontvangen, maar dat andere landen hier niet zo enthousiast over zullen zijn.
- Aanpassing van de encryptie om toegang te kunnen krijgen ten behoeve van de opsporing is kortom naar de opvatting van de ondertekenaars van de petitie een zeer onwenselijke oplossing en creëert meer onveiligheid dan veiligheid. Daarvoor werden onder meer de volgende argumenten genoemd:
    - Malafide partijen zullen ook gebruik maken van de 'achterdeur' die wordt gecreëerd wanneer de beveiliging wordt verzwakt.
    - De technologie om end-to-end encryptie te bewerkstelligen is gemakkelijk te implementeren. Criminelen kunnen gemakkelijk hun communicatie versleutelen, dus het is slechts een verschuiving van het probleem.
    - Het brengt grote risico's met zich mee wat betreft het waarborgen van privacy.
    - Het kan innovatie belemmeren.
    - Het tast het vertrouwen in die diensten aan.
    - Wanneer verkeerde partijen aan de macht komen kan er misbruik van worden gemaakt.
    - Het is praktisch gezien moeilijk te bewerkstelligen, toegang kan niet worden beperkt tot de betrouwbare opsporingsdiensten.
- Mede om deze redenen is het initiatief stimuleer-encryptie.nl opgezet en gesteund, dit is breder dan alleen de bescherming van OTT-communicatie en steunt de versterking van encryptie in brede zin.
- Er moet gekeken worden naar andere manieren om bij versleutelde gegevens te komen. Enkele alternatieven die worden benoemd zijn:
    - Benut de beschikbare mogelijkheden zoals de hackbevoegdheid beter:
        - Investeer in de capaciteit daartoe bij de opsporingsdiensten.
        - Gebruik de zwakheden in (software) systemen, zoals hackers dit ook doen.
        - Binnen de vertrouwde hack-netwerken komen en op die manier informatie vergaren over de malafide partijen
    - Gebruik data sciences om criminelen op te sporen.
- Sleutelbeheer wordt door velen afgewezen als mogelijkheid, op basis van de volgende argumenten:
    - Het is een integraal onderdeel van encryptie. Je kunt niet zeggen dat je de encryptie niet verzwakt (omdat je bijvoorbeeld niets aan het onderliggende algoritme doet) als je tegelijkertijd ook sleutelt aan het sleutelbeheer of -configuratie. "Hackers don't break encryption, they find your keys."
    - Het is een van de meest complexe onderdelen van cryptografie, omdat het de plek is waar de menselijke rol het grootst is. Het is daarmee relatief fragiel. Er is een grotere risico op interventies die zwaktes uitbuiten in de menselijke component. Dat staat tegenover andere onderdelen van het cryptografische systeem, dat uit geheel geautomatiseerde toepassingen van wiskundige principes bestaat.

- Een partij ziet wel kansen voor sleutelbeheer, door gebruik te maken van een betrouwbare externe sleutelbeheer-partij.
- Overheidspartijen geven aan dat, ondanks dat het al jaren een terugkerend thema is, de problemen nog steeds niet opgelost zijn. Wat de oplossingen betreft is er wellicht niet veel veranderd, maar vanuit opsporingsperspectief is dit wel zo. De afgelopen 5 jaar is end-to-end encryptie steeds meer geïntroduceerd in populaire communicatiediensten en is encryptie steeds vaker standaard. Daarbovenop is met de digitalisering ook het belang van digitale data voor de opsporing enorm toegenomen. Tevens relevant voor de toegang tot gegevens in het algemeen zijn verschillende (juridische) ontwikkelingen in het privacydomein, zoals dataminimalisatie en beperkingen van een bewaarplicht, waardoor gegevens minder (mogen) worden opgeslagen door organisaties.
  De toegang tot versleutelde informatie ten behoeve van de opsporing is een legitiem belang, door het periodiek onderzoeken van de mogelijke oplossingen wordt invulling gegeven aan dit belang. Hierbij wordt zowel het belang van cybersecurity, privacy en de opsporing meegewogen. Reële opties worden uitgewerkt zodat de keuze geïnformeerd kan worden gemaakt. Aan veel alternatieven zitten ook haken en ogen, daarom moeten mogelijkheden worden onderzocht en afgewogen. Zo is bijvoorbeeld het gebruik en de handel in exploits en zero-days om telefoons en andere systemen binnen te komen niet een wenselijke ontwikkeling.
- Door samenwerking zullen de beste inzichten ontstaan. Het doel is niet om encryptie te verzwakken maar om tijdig en betrouwbaar rechtmatige toegang tot versleutelde informatie ten behoeve van de opsporing en vervolging te krijgen. Hoe kan je tot de informatie komen op een manier die niet afdoet aan het belang van beveiliging? Dat is de vraag die centraal staat. Een uitwisseling van zienswijze helpt aanzienlijk om meer inzicht te krijgen in elkaars vertrekpunten, zorgen en oplossingsrichtingen.
- De deelnemende organisaties erkennen de noodzaak dat de overheid zoekt naar oplossingen voor het vraagstuk van het krijgen van toegang tot versleutelde informatie ten behoeve van de opsporing. Indien wordt doorgegaan met het zoeken naar oplossingen moet dat onderzoek echter wel transparant en in samenwerking gebeuren:
    - Verricht een peer-reviewed onderzoek, ook naar de alternatieven; dit zal het debat helpen.
    - Betrek bij de toetsing alle partijen die hierbij belangen hebben, waaronder een civil society component.
- De deelnemende partijen ondersteunen dat dit overleg moet worden gezien als een startpunt voor een verder overleg. Doel daarvan is dat er wordt gekeken naar oplossingsrichtingen voor het vraagstuk en hoe de alternatieven ten opzichte van aanpassing van encryptie ten volste kunnen worden benut.
- Afgesproken wordt dat JenV het initiatief neemt voor een vervolg. Dat zal naar verwachting in het najaar zijn.

Van: 5.1.2.e
Verzonden: dinsdag 13 juli 2021 18:17
Aan: 5.1.2.e
CC: 5.1.2.e
Onderwerp: FW: Concept verslagen ambtelijke sessie toegang tot opsporingsinformatie en encryptie 7 en 8 juli
Bijlagen: Concept verslag sessie 7 juli 2021.docx; Concept verslag sessie 8 juli 2021.docx

Bijgaand de J&V concept verslagen van de ambtelijke sessie inz. opsporing met behoud van sterke encryptie

J&V wijst de geadresseerden er op dat J&V onlangs een WOB verzoek ontvangen heeft waar deze verslaglegging onderdeel van uitmaakt.

Ik vermoed dat deelnemende partijen met aanvullingen & comments komen.

Met vriendelijke groet,

5.1.2 e
Digitale Veiligheid / ePrivacy

T : +31-70 5.1.2.e
M : +31 6 - 5.1 2.e

Van: 5.1.2.e @minjenv.nl>
Verzonden: dinsdag 13 juli 2021 16:40
Aan: 5.1.2.e @kpn.com' 5.1.2.e @kpn.com>; 5.1.2.e @apple.com' 5.1.2.e @apple.com>; 5.1.2.e @microsoft.com' 5.1.2.e @microsoft.com>; 5.1.2.e @foxcrypto.com>; 5.1.2.e @dinl.nl' 5.1.2.e @dinl.nl>; 5.1.2.e 5.1.2.e @cyberveilignederland.nl>; 5.1.2.e @minezk.nl>; 5.1.2.e 5.1.2.e @minezk.nl>; 5.1.2.e 5.1.2.e @nctv.minjenv.nl>; 5.1.2.e @minjenv.nl>; 5.1.2.e 5.1.2.e @holmes.nl>; 5.1.2.e @foxcrypto.com>
CC: 5.1.2.e @minjenv.nl>; 5.1.2.e 5.1.2.e @minjenv.nl>
Onderwerp: Concept verslag ambtelijke sessie toegang tot opsporingsinformatie en encryptie 7 juli

Beste deelnemers,

Bijgesloten vindt u, met dank aan mijn collega 5.1.2.e , het beloofde concept verslag van ons overleg van vorige week woensdag 7 juli. Het verslag is zoals aangekondigd op hoofdlijnen en zo opgesteld dat de inbreng niet herleidbaar is tot personen of organisaties. Graag verneem ik deze week of u ten aanzien van hetgeen u heeft ingebracht eventueel nog punten mist of opmerkingen heeft. Begin volgende week zal ik dan het definitieve verslag rondsturen.
Hierbij wil ik u ook informeren dat we recent een WOB-verzoek hebben ontvangen dat onder meer ziet op dit verslag.

Wij vonden het een goed overleg, waarin hopelijk en basis is gelegd voor verdere+ discussie en samenwerking. Namens mijn collega's nogmaals dank voor uw deelname aan de bijeenkomst en (hopelijk) aan het vervolg.

Met vriendelijke groet,

5.1.2.e

.....
Ministerie van Justitie en Veiligheid
Directoraat-Generaal Rechtspleging en Rechtshandhaving
Turfmarkt 147 | 2511 DP | Den Haag |N20
Postbus 20301 | 2500 EH | Den Haag
.....
M 06 5.1.2.e
5.1.2.e @minjenv.nl
www.rijksoverheid.nl/venj

Van: 5.1.2.e - BD/DRC/FO 5.1.2.e @minjenv.nl>
Verzonden: woensdag 14 juli 2021 12:07
Aan: 5.1.2.e
CC: 5.1.2.e @tilburguniversity.edu'; 5.1.2.e @google.com'; 5.1.2.e @vodafoneziggo.com'; 5.1.2.e @nlnet.nl'; 5.1.2.e @isoc.org'; 5.1.2.e - BD/PIDS; 5.1.2.e (DBS)'; 5.1.2.e 5.1.2.e 5.1.2.e 5.1.2.e BD/KS; 5.1.2.e 5.1.2.e BD/DRC/CV; 5.1.2.e BD/DRC/FO
Onderwerp: RE: Concept verslag ambtelijke sessie toegang tot opsporingsinformatie en encryptie 8 juli

Categorieën: Categorie Rood

Beste 5.1.2.e

Dank voor je terugkoppeling. Ik zal je tekstvoorstellen hieronder overnemen in het verslag. En ook fijn om alvast te weten dat je geen bezwaar hebt tegen de openbaarmaking ihkv het WOB-verzoek.

Groet,

5.1.2.e

-----Oorspronkelijk bericht-----
Van: 5.1.2.e @bitsoffreedom.nl>
Verzonden: woensdag 14 juli 2021 11:11
Aan: 5.1.2.e BD/DRC/FO 5.1.2.e @minjenv.nl>
CC: 5.1.2.e @tilburguniversity.edu' 5.1.2.e @tilburguniversity.edu>; 5.1.2.e @google.com' 5.1.2.e @google.com>; 5.1.2.e @vodafoneziggo.com' 5.1.2.e @vodafoneziggo.com>; 5.1.2.e @nlnet.nl' 5.1.2.e @nlnet.nl>; 5.1.2.e @isoc.org' 5.1.2.e @isoc.org>; 5.1.2.e BD/PIDS 5.1.2.e @minjenv.nl>; 5.1.2.e (DBS)' 5.1.2.e @holmes.nl>; 5.1.2.e @minezk.nl>; 5.1.2.e 5.1.2.e @minezk.nl>; 5.1.2.e BD/KS 5.1.2.e @nctv.minjenv.nl>; 5.1.2.e @minbzk.nl>; 5.1.2.e BD/DRC/CV 5.1.2.e @minjenv.nl>; 5.1.2.e BD/DRC/FO 5.1.2.e @minjenv.nl>
Onderwerp: Re: Concept verslag ambtelijke sessie toegang tot opsporingsinformatie en encryptie 8 juli

Beste 5.1.2.e,

Dank je wel voor het verslag. Ik heb een kleine opmerking. Er staat in het verslag de tekst: "Sleutelbeheer wordt door velen afgewezen als mogelijkheid. Een partij ziet daarin wel kansen, door gebruik te maken van een betrouwbare externe sleutelbeheer-partij." Dat eerste punt heb ik ingebracht, maar ik heb dat veel scherper gedaan en met meer argumenten dan precies nul. Op basis van mijn eigen aantekeningen van het gesprek heb ik daarover het volgende gezegd:

---->
- Het is een integraal onderdeel van encryptie. Je kunt niet zeggen dat je de encryptie niet verzwakt (omdat je bijvoorbeeld niets aan het onderliggende algoritme doet) als je tegelijkertijd ook sleutelt aan het sleutelbeheer of -configuratie.
- Het is een van de meest complexe onderdelen van cryptografie, omdat het de plek is waar de menselijke rol het grootst is. Het is daarmee relatief fragiel. Er is een grotere risico op interventies die zwaktes uitbuiten in de menselijke component. Dat staat tegenover andere onderdelen van het cryptografische systeem, dat uit geheel geautomatiseerde toepassingen van wiskundige principes bestaat.
- "Hackers don't break encryption, they find your keys.
<----

Het is belangrijk dat dit goed overkomt bij Justitie en Veiligheid. Mag ik je vragen om aanpassing van het verslag. Wat mij betreft neem je bovenstaande tekst over, maar ik ben ook graag bereid om een kortere samenvatting ervan voor te stellen.

Verder begrijp ik dat iemand anders dan ikzelf een verzoek heeft gedaan op grond van de Wet openbaarheid van bestuur. Om jullie werk te besparen: mocht onze conversaties ook onder de reikwijdte vallen, dan stel ik op voorhand geen bezwaar te hebben tegen openbaarmaking daarvan. Dat bespaart jullie een verzoek aan een belanghebbende. :)

Met vriendelijke groet,
5.1.2.e

++ 13/07/21 15:18 +0000 - 5.1.2.e BD/DRC/FO:
Reeds beoordeeld in dit verzoek

>This message may contain information that is not intended for you. If you are not the addressee or if this message was sent to you by mistake, you are requested to inform the sender and delete the message. The State accepts no liability for damage of any kind resulting from the risks inherent in the electronic transmission of messages.
>
>Ministry of Justice and Security
>

--
5.1.2.e
Bits of Freedom | https://bitsoffreedom.nl
+31 6 5.1.2.e | @bitsoffreedom
5.1.2.e @bitsoffreedom.nl | 0x0994094621DBEFD4 _____

Van: 5.1.2.e
Verzonden: donderdag 2 september 2021 10:57
Aan: 5.1.2.e
Onderwerp: FW: Fiche OTT-communicatiediensten versie 2 na BWP
Bijlagen: 20210831 Fiche v2 OTT interceptie Def.docx

Ha collega's,

Ter info.

Gr.,

5.1.2.e

Van: 5.1.2.e @minjenv.nl>
Verzonden: woensdag 1 september 2021 17:37
Aan: 5.1.2.e @minezk.nl>; 5.1.2.e @minjenv.nl>; 5.1.2.e @minbuza.nl>; 5.1.2.e @nctv.minjenv.nl>; 5.1.2.e @agentschaptelecom.nl>
CC: 5.1.2.e @minjenv.nl>
Onderwerp: RE: Fiche OTT-communicatiediensten versie 2 na BWP

Dag allen,

Hierbij de schone versie van het definitieve OTT-fiche.
Dank voor de feedback!

Groet,

5.1 2.e

Van: 5.1.2.e
Verzonden: dinsdag 20 juli 2021 16:46
Aan: 5.1.2.e @minezk.nl>; 5.1.2.e @minjenv.nl>; 5.1.2.e @minbuza.nl>; 5.1.2.e @nctv.minjenv.nl>; 5.1.2.e @agentschaptelecom.nl>
CC: 5.1.2.e @minjenv.nl>
Onderwerp: Fiche OTT-communicatiediensten versie 2 na BWP

Dag allen,

Het OTT fiche is zowel door de MJenV en SEZK voorgelegd en daaruit zijn nog enkele wensen tot aanpassing gekomen. Deze zijn in bijgesloten versie 2 verwerkt.
De belangrijkste wensen van de BWP-en betreffen:

- SEZK: meenemen van alternatieven zoals de hackbevoegdheid bij de analyse van mogelijk oplossingen.
- MJenV: vond het te prijzig en te lang duren. Daarom stellen we een minder diepgaand onderzoek voor zonder technische PoC, dat is dan sneller klaar en

betaalbaarder. Op basis daarvan kan dan gekeken worden of een (duurdere) nadere technische uitwerking (PoC) gewenst en nuttig is.

Verder hebben we de brede onafhankelijke adviescommissie - die we in de eerste versie als alternatief hadden neergezet - nu een rol gegeven in het begeleiden van het onderzoek en het gevraagd en ongevraagd adviseren.

Aan jullie de vraag of jullie in de wijzigingen kunnen vinden.
Zouden jullie je reactie, i.v.m. mijn verlof - vanaf morgen tot en met 16 augustus - naar 5.1.2.e kunnen mailen?

Veel dank alvast, en een fijne vakantie voor wie nog weg gaat!

Groet,

5.1 2.e

Van: 5.1.2.e
5.1.2.e @cybersecurityraad.nl>
Verzonden: woensdag 15 september 2021 01:21
Aan: 5.1.2.e
CC: 5.1.2.e
Onderwerp: RE: inbreng EZK nav eerste overleg subcommissie

Categorieën: Categorie Rood

Beste 5.1.2.e

Hartelijk dank voor deze uitgebreide inbreng vanuit EZK. Tijdens de CSR vergadering as donderdag zal door 5.1.2.e een terugkoppeling op hoofdlijnen worden gegeven van de bijeenkomst van de subcommissie Encryptie. De aanpak die door de subcommisie is vastgesteld ligt grotendeels in lijn met jullie inbreng. De belangrijkste punten uit het overleg zullen ook zsm per mail onder de leden van de subcommissie worden verspreid.

Hartelijke groet,

5.1.2.e

Verzonden met BlackBerry Work
(www.blackberry.com)

Van: 5.1.2.e @minezk.nl>
Datum: dinsdag 14 sep. 2021 9:37 PM
Aan: Secretariaat CSR 5.1.2.e @cybersecurityraad.nl>, 5.1.2.e
@cybersecurityraad.nl>
Kopie: 5.1.2.e @minezk.nl>, 5.1.2.e @minezk.nl>,
5.1.2.e @minezk.nl>, H5.1.2.e
@cybersecurityraad.nl>
Onderwerp: inbreng EZK nav eerste overleg subcommissie

Beste secretariaat,

Wegens spoedoverleg kon 5.1.2.e helaas gisteren niet namens EZK deelnemen aan de startbijeenkomst van de subscommissie Encryptie. Indien mogelijk zou EZK toch graag van de gelegenheid gebruik willen maken om haar positie te delen binnen de subcommissie. Hieronder treft u enkele punten aan welke hopelijk kunnen worden meegenomen in het traject.

- Voor EZK ligt de toegevoegde waarde van de subcommissie met name in het verkennen van alternatieve opties die toegang tot communicatiediensten mogelijk maken (die toegang is immers het onderliggende doel) die niet ingrijpen op de end-to-end encryptie (dat dilemma gaat deze subcommissie immers niet oplossen). Wat betreft EZK dient de focus van de subcommissie dan ook op de alternatieve opties te liggen. Dergelijke alternatieve opties

kunnen worden ingebracht en meegenomen in het lopende nationale traject, hetgeen geleid wordt door JenV in samenwerking met EZK.

- In het kader van het verkennen van alternatieve opties kan EZK aangeven dat de voorkeur ernaar uitgaat dat er onder begeleiding van de subcommissie een technisch-juridische werkgroep, bestaande uit zowel cybersecurity- als juridische experts, wordt ingericht. De werkgroep kan (haalbare) alternatieve opties verkennen en zowel de technische als juridische aspecten in dit geheel meenemen. Hierbij zou wat EZK betreft in ieder geval het toepassen en mogelijk verbeteren van de 'hacking-bevoegdheid (als alternatieve methode) moeten worden meegenomen. NB EZK pleit voor toevoeging van de juridische invalshoek, om ook te bezien welke juridische en procedurele obstakels er eventueel bestaan bij alternatieve opties zoals hacking, en in hoeverre deze kunnen worden weggenomen.
- De resultaten van de werkzaamheden van de werkgroep doen recht aan de wens van stakeholders om dieper in te gaan op het verkennen van alternatieve opsporingsmethodes.
- Het voordeel van een technische (en juridische) werkgroep ten opzichte van het inschakelen van een externe partij (die een onderzoeksrapport schrijft) is dat de subcommissie regie heeft op de voortgang van diverse te verkennen opties en de nodige inzet qua expertise.
- Indien het merendeel van de deelnemers zijn voorkeur uitspreek voor een extern onderzoek dan dient vanuit EZK te worden meegegeven dat het essentieel is dat de subcommissie nauw betrokken is bij dit proces, en daartoe vanuit de subcommissie ook de nodige technische en juridische expertise vereist is.
- EZK kan instemmen met het continue rapporteren van CSR inzake de voortgang binnen de subcommissie. EZK acht het wel wenselijk dat binnen het kader van de CSR de subcommissie de regie behoudt op het traject.

Alvast heel veel dank.

Groet,

5.1.2.e

Directoraat-Generaal Bedrijfsleven en Innovatie
.....
Ministerie van Economische Zaken
Bezuidenhoutseweg 73 | 2594 AC | Den Haag
Postbus 20401 | 2500 EK | Den Haag
.....
T: +31 65.1.2.e
E: 5.1.2.e @minez.nl
.....

Van: 5.1.2.e
Verzonden: donderdag 28 oktober 2021 13:22
Aan: 5.1.2.e
Onderwerp: FW: Uitnodiging startbijeenkomst technisch-inhoudelijke werkgroep Encryptie - CSR

t.i.

Van: 5.1.2.e @cybersecurityraad.nl>
Verzonden: donderdag 28 oktober 2021 12:36
Aan: 5.1.2.e @cs.ru.nl' <5.1.2.e @cs.ru.nl>;5.1.2.e @tudelft.nl' 5.1.2.e @tudelft.nl>; 5.1.2.e @minbzk.nl' 5.1.2.e @minbzk.nl>;5.1.2.e @politie.nl' 5.1.2.e @politie.nl>; 5.1.2.e @kpn.com 5.1.2.e @kpn.com>; 5.1.2.e 5.1.2.e @minjenv.nl>; 5.1.2.e @minezk.nl>
CC: 5.1.2.e @tudelft.nl' 5.1.2.e @tudelft.nl>;5.1.2.e @cybersecurityraad.nl>; 5.1.2.e @cs.ru.nl' 5.1.2.e @cs.ru.nl>
Onderwerp: RE: Uitnodiging startbijeenkomst technisch-inhoudelijke werkgroep Encryptie - CSR

Geachte deelnemers aan de technisch-inhoudelijke werkgroep Encryptie,

Het startgesprek voor deze werkgroep zal plaatsvinden op **vrijdag 12 november, van 10.15 – 11.00 uur, via Webex**. Een outlook-invite volgt.
Tijdens dit startgesprek zal een kennismaking centraal staan, evenals de onderzoeksvraag en de te verdelen rollen en taken.

Deelnemers zijn:

- 5.1.2.e 5.1.2.e
- 5.1.2.e 5.1.2.e
- 5.1.2.e 5.1.2.e
- 5.1.2.e (Politie)
- 5.1.2.e (KPN)
- 5.1.2.e (Platform Interceptie Decryptie en Signaalanalyse - DGRR)
- 5.1.2.e (Digitale Veiligheid/ePrivacy - EZK)

Een agenda en eventuele vergaderstukken volgen tzt.

Met hartelijke groet,

5.1.2.e

.....
Ministerie van Justitie en Veiligheid
Cyber Security Raad
Turfmarkt 147 | 2511 DP | Den Haag
Postbus 16950 | 2500 BZ | Den Haag
.....
M 06 5.1.2.e

5.1.2.e @cybersecurityraad.nl
https://www.cybersecurityraad.nl/
.....

Van 5.1.2.e
Verzonden: donderdag 21 oktober 2021 11:58
Aan: 5.1.2.e @tudelft.nl>; 5.1.2.e @minbzk.nl' 5.1.2.e @minbzk.nl>; 5.1.2.e @politie.nl' 5.1.2.e @politie.nl>; 5.1.2.e @kpn.com' 5.1.2.e @kpn.com>; 5.1.2.e @minjenv.nl>; 5.1.2.e @minezk.nl' 5.1.2.e @minezk.nl>
CC: 5.1.2.e @cs.ru.nl' <5.1.2.e @cs.ru.nl>; 5.1.2.e @tudelft.nl>; 5.1.2.e @cybersecurityraad.nl>; 5.1.2.e @cybersecurityraad.nl>
Onderwerp: Uitnodiging startbijeenkomst technisch-inhoudelijke werkgroep Encryptie - CSR

Beste deelnemers aan de technisch-inhoudelijke werkgroep Encryptie,

Graag plan ik met jullie een moment in voor het startgesprek van de technisch-inhoudelijke werkgroep Encryptie, die onder leiding staat van prof. 5.1.2.e

Dit startgesprek zal 45 minuten duren en vindt digitaal plaats (via Webex). Het dient ter kennismaking en ter voorbereiding op een eerste fysieke, inhoudelijke bijeenkomst. Het startgesprek is bedoeld om een duidelijk beeld te krijgen van de precieze onderzoeksvragen, alsook van de te verdelen rollen en taken. Deelnemers aan deze werkgroep zijn:

- 5.1.2.e (5.1.2.e
- 5.1.2.e 5.1.2.e
- 5.1.2.e 5.1.2.e
- 5.1.2.e (Politie)
- 5.1.2.e (KPN)
- 5.1.2.e (Platform Interceptie Decryptie en Signaalanalyse - DGRR)
- 5.1.2.e (Digitale Veiligheid/ePrivacy - EZK)

Vanuit de agenda van 5.1.2.e leg ik graag de volgende momenten aan jullie voor:

- Woensdag 10 november, ergens tussen 08.30 en 14.00 uur;
- Donderdag 11 november, ergens tussen 08.30 en 16.00 uur;
- Vrijdag 12 november, ergens tussen 08.30 en 17.00 uur.

Graag verneem ik in antwoord op deze e-mail jullie beschikbaarheid voor bovengenoemde momenten. Het zou fijn zijn om **uiterlijk komende dinsdag 26 oktober vóór 12:00 uur** het moment van de startbijeenkomst vast te kunnen leggen.

Neem bij vragen of onduidelijkheden vooral even contact met mij op.

Met hartelijke groet,

5.1.2.e
.....

Ministerie van Justitie en Veiligheid
Cyber Security Raad
Turfmarkt 147 | 2511 DP | Den Haag
Postbus 16950 | 2500 BZ | Den Haag
.....
M 06 5.1.2.e
5.1.2.e@cybersecurityraad.nl
https://www.cybersecurityraad.nl/
.....

Van: 5.1.2.e
Verzonden: donderdag 18 november 2021 15:40
Aan: 5.1.2.e
CC: 5.1.2.e
Onderwerp: argumentenkaart encryptie

5.1.2.e

Zie hierbij: AMS-IX en ECP publiceren argumentenkaart om encryptiedebat te versterken - ECP | Platform voor de InformatieSamenleving.

5.1.2.e was bij de sessie van de Argumentenfabriek.

Gr

5.1 2.e

Van: 5.1.2.e
Verzonden: maandag 31 januari 2022 11:52
Aan: 5.1.2.e
CC: 5.1.2.e
Onderwerp: werkgroep sub Cie encryptie
Bijlagen: Conclusies en werkafspraken 3e bijeenkomst Technisch-inhoudelijke werkgroep Encryptie.pdf; werkgroep-encryptie-2022.docx

Bijgaand t.i. (intern)

- het verslag van het sub Cie encryptie (onder CSR) van medio januari jl. en
- een eerste concept-rapport van de sub CIe waar nu aan gewerkt wordt en straks in sub CIe besproken wordt.

Gr. 5.1.2.e

5.1.2 e

Ministerie van Economische Zaken en Klimaat
Directoraat Generaal B&I
Directie Digitale Economie

Bezuidenhoutseweg 73
2594 AC Den Haag
Postbus 20401, 2500 EK Den Haag
T : +31-70 5.1.2.e
M : +31 6 5.1 2.e

CSR Cyber Security Raad

Conclusies en werkafspraken 3e bijeenkomst Werkgroep Encryptie

Datum: Donderdag 13 januari 2022

Tijdstip: 16:00 - 17:00 uur

Locatie: Webex,

Deelnemers: 5.1.2.e

Afwezig: -

1. Opening en mededelingen

2. Takeaways tot nu toe

Tijdens de voorgaande bijeenkomsten is het volgende besproken.

Te inventariseren thema's:

1. Enhanced Access
2. (tapbaarheid van) 5G
3. Initiatieven in Europa/EU
4. Zeer beperkte inzet bestaande hackbevoegdheid
5. Aanleveren metadata Big Tech na verzoek diensten - termijn, mate van details etc.
6. Mogelijkheid verkrijgen gegevens uit onversleutelde opslag
7. Dataretentie

3. Overzicht van initiatieven op EU-niveau en in agendabepalende landen/ontwikkeling internationale discussie

- Besprekingen over deze thematiek op EU-niveau vinden plaats in de marge van overige besprekingen. Er is wel degelijk aandacht voor maar niet in speciaal daartoe ingerichte overleggen.
- De EC heeft een enquête gehouden onder de lidstaten om de standpunten te inventariseren. Deze liet verdeeldheid zien en er sprong geen bepaalde aanpak uit. Er wordt gezocht naar consensus en focuspunten, en er zijn ook wel wat initiatieven (zie link in aangeleverde documenten).
- De verwachting is niet dat er komend jaar concrete besluiten als een decryptieverplichting zullen worden genomen.
- De Encryption Declaration (rondgestuurd door 5.1.2.e geeft vooral een behoefte aan, het is niet evident tot welke conclusies deze zal leiden.
- De leden kennen desgevraagd geen analyses of onderzoeken op EU-niveau naar alternatieven, zoals het verzwakken van anonimiteit op het internet of eerst alleen weten wie met wie communiceert, zodat daarna gerichter toegang kan worden gezocht. Interceptie heeft daarbij meerdere doelen zoals identificatie, waarheidsvinding en

bewijsvoering. Naar transportencryptie en berichtenencryptie is encryptie van devices zelf van belang.
- Besproken wordt dan een volgende keer dieper ingegaan kan worden op het stuk van Europol, daar zou overlap in kunnen zitten met de activiteiten van de werkgroep.

4. Duiding van beperkte inzet bestaande hackbevoegdheden:

- Het WODC doet momenteel onderzoek naar de evaluatie van de hackbevoegdheid. Dit onderzoek wordt in februari aan een klankboardgroep gepresenteerd, kort daarna waarschijnlijk gepubliceerd. Het is niet de verwachting dat de werkgroep nog vóór de publicatie over het (concept)onderzoek zal kunnen beschikken. 5.1.2.e vraagt dit na.
- Problemen waar de politie voor de inzet van hackbevoegdheid tegenaan loopt, zitten vooral in schaal, (juridische) drempels en het specialistische karakter. Het is erg arbeidsintensief en vergt dus veel capaciteit. Juridische kaders stellen hogere eisen dan bij de aftapwetgeving, waar je bijvoorbeeld ook een betrokkene kunt aftappen. Deze mag echter niet gehackt worden, dat mag alleen bij verdachten. Bovendien kan hacken (maatwerk) niet op dezelfde schaal plaatsvinden als tappen (ingeregeld proces).
- AIVD heeft een ander wettelijk kader en kan het middel meer inzetten, maar is ook afhankelijk van het aantal mensen in dienst. Er lopen voortdurende gesprekken met toezichthouders, onder andere over het gebruik van zero days. De taakstelling is echter breder dan die van de politie.
- Als je 2x zoveel wil hacken heb je 2x zoveel hackers nodig.
- De tools die door de politie kunnen worden aangekocht moeten gekeurd worden en dat kan soms belemmerend werken. Algemeen beschikbare tools zijn niet altijd goed toepasbaar; hacken is maatwerk. De juridische werkelijkheid en de techniek van het hacken passen niet altijd bij elkaar.
- Het is maar de vraag of er voor de onderzoeks-/opsporingsvraag die voorligt een geschikte tool voorhanden is. Er is dan een wisselwerking tussen de specialiteit van het middel, de vraag en het beschikbare team.
- De zaken waar de hackbevoegdheid tot nu toe is ingezet betrekt het topsegment van de criminaliteit. Voor elk systeem dat je wil hacken is vooronderzoek nodig, toetsing, toestemming etc. Er is dus niet snel een grote klasse van vergelijkbare apparaten waar je één en dezelfde tool op kunt loslaten.
- Vanwege het wens niet herkenbaar te zijn wil men eigenlijk de inzet van tools (herhaaldelijk) vermijden. Dat leidt tot een drang naar niet-standaardisatie. Dat gaat dus in tegen de efficiëntiegedachte omdat standaardisatie tot ongewenste herkenbaarheid leidt.
- Inloggen op account van verdachten is aan extra belemmeringen onderhevig wanneer dit inloggen bij een Cloudaanbieder betekent, in plaats van op een meer lokaal systeem.

5. Vervolgaanpak en werkafspraken

- Volgende bijeenkomst eind januari
- Dan te bespreken:
    - Het doel is om een verslag van zo'n 5 pagina's aan te leveren bij de subcommissie. Ook is er de mogelijkheid om bij de subcommissie eerst een lijstje met oplossingen aan te leveren waarvan de werkgroep de moeite waard vindt om te verkennen.

Van: 5.1.2.e
Verzonden: dinsdag 8 februari 2022 13:32
Aan: 5.1.2.e
CC: 5.1.2.e
Onderwerp: FW: Concept beantwoording KV interceptie OTT VVD
Bijlagen: 220208 TK Concept beantwoording 5.1.2.e .docx

5.1.2.e

Ter info nog de aanvullingen van 5.1.2.e en mijzelf m.b.t. Kamervragen encryptie.

Gr.,

5.1.2.e

Van: 5.1.2.e
Verzonden: dinsdag 8 februari 2022 13:31
Aan: 5.1.2.e @minjenv.nl>; 5.1.2.e @minjenv.nl>; 5.1.2.e @minjenv.nl>; 5.1.2.e @nctv.minjenv.nl>; 5.1.2.e @minezk.nl>; 5.1.2.e @minbzk.nl' 5.1.2.e @minbzk.nl>; 5.1.2.e @minbuza.nl' 5.1.2.e @minbuza.nl>
Onderwerp: RE: Concept beantwoording KV interceptie OTT VVD

Hallo 5.1.2.e

Bijgaand enkele aanvullingen. Mocht je hierover willen overleggen dan hoor ik het graag.

Dank vast.

Groet,

5.1.2.e

Van: 5.1.2.e @minjenv.nl>
Verzonden: maandag 7 februari 2022 16:01
Aan: 5.1.2.e @minjenv.nl>; 5.1.2.e @minjenv.nl>; 5.1.2.e @nctv.minjenv.nl>; 5.1.2.e @minezk.nl>; 5.1.2.e @minezk.nl>; 5.1.2.e @minbzk.nl' 5.1.2.e @minbzk.nl>; 5.1.2.e @minbuza.nl' 5.1.2.e @minbuza.nl>
Onderwerp: Concept beantwoording KV interceptie OTT VVD

Beste collega's,

We hebben een set Kamervragen gekregen nav een vacaturetekst die aangeeft dat we een nieuwe medewerker die onder andere onderzoek gaat doen naar de voor- en nadelen van interceptie van OTT-communictiediensten. Hierbij een voorstel tot een conceptbeantwoording. Kan ik vragen om hier **op aanstaande donderdag** eventuele op- of aanmerkingen op te ontvangen?

Het vroeg aanbieden in de lijn is denk ik belangrijk omdat dit de eerste keer wordt dat de minister zich moet uitspreken over onze inventarisatie. Het is goed mogelijk dat we deze set retour krijgen. In de

beantwoording heb ik daarom een paar dingen benadrukt: het belang van alle betrokken belangen, de mogelijkheid dat we ook tot de conclusie komen dat we geen proportionele oplossing vinden én ik benadruk de ruimte die we in beginsel zouden moeten hebben om deze inventarisatie uit te voeren.

Naast de partners van de opsporing zet ik ook de collega's van de IenV diensten in cc. Hiernaast gaat deze set nog ter afstemming de opsporings- en IenV-partners. Houd bij de op- en aanmerkingen svp ook rekening met de grote groep met wie afstemming plaatsvindt.

Bij voorbaat dank!

Met vriendelijke groet,

5.1.2.e

.....
Ministerie van Veiligheid en Justitie
Directie Rechtshandhaving en Criminaliteitsbestrijding
Cybercrime unit
Turfmarkt 147 | 2511 DP | Den Haag |
Postbus 20301 | 2500 EH | Den Haag
.....
M 06 5.1.2.e
5.1.2.e @minvenj.nl
www.rijksoverheid.nl/venj
.....
Voor een veilige en rechtvaardige samenleving
.....

Van: 5.1.2.e
Verzonden: woensdag 9 februari 2022 17:33
Aan: 5.1.2.e
Onderwerp: FW: Definitief verslag techn. werkgroep Encryptie
Bijlagen: Verslag tecnisch-inhoudelijke werkgroep Encryptie.pdf

Zie bijgaand het def. Verslag van de technische werkgroep encryptie dat mogelijk rond 21 febr in de Subcommissie v.d. Raad besproken wordt.

Met vriendelijke groet,

5.1.2 e
Digitale Veiligheid / ePrivacy

T : +31-70 5.1.2.e
M : +31 6 - 5.1 2.e

Van: 5.1.2.e @cybersecurityraad.nl>
Aan: 5.1.2.e @cs.ru.nl' <5.1.2.e @cs.ru.nl>;5.1.2.e @tudelft.nl' 5.1.2.e @tudelft.nl>; 5.1.2.e @minbzk.nl' 5.1.2.e @minbzk.nl>; 5.1.2.e @minbzk.nl>; 5.1.2.e @kpn.com' 5.1.2.e @kpn.com>; 5.1.2.e @politie.nl>;5.1.2.e @politie.nl>; 5.1.2.e @minezk.nl>; 5.1.2.e @minjenv.nl>
Onderwerp: Definitief verslag werkgroep Encryptie

Dag allen,

Bijgaand stuur ik jullie het definitieve verslag van de werkgroep door, opgesteld door 5.1.2.e

Momenteel wordt een bijeenkomst van de subcommissie van de raad gepland, waarschijnlijk in de week van 21 februari. Dit verslag zal daar worden besproken, alsook de te nemen vervolgstappen. Mocht een aanvullende opdracht aan de werkgroep volgen, dan worden jullie daar natuurlijk van op de hoogte gebracht.

Voor nu hartelijk dank aan jullie allen!

Met hartelijke groet,

5.1.2.e

CSR Cyber Security Raad

.....
Ministerie van Justitie en Veiligheid
Cyber Security Raad
Turfmarkt 147 | 2511 DP | Den Haag
Postbus 16950 | 2500 BZ | Den Haag

.....
M 06 5.1.2.e
5.1.2.e@cybersecurityraad.nl
https://www.cybersecurityraad.nl/
.....

CSR Cyber Security Raad

Verslag bevindingen technisch-inhoudelijk werkgroep Encryptie

Inleiding

Het onderstaande is een verslag van een ad hoc werkgroep die samen met CSR-leden 5.1.2.e en 5.1.2.e in de drie maanden Nov'21 – Jan'22 een aantal maal (online) samengekomen is. Aan deze werkgroep werd (verder) deelgenomen door:

- Twee operationeel specialisten-digitaal vanuit het Team High Tech Crime van de politie;
- Een persoon vanuit de AIVD, met een technische/beleidsmatige achtergrond;
- Een senior adviseur bij het Platform Interceptie Decryptie & Signaalanalyse (PIDS) van het Ministerie van Justitie en Veiligheid;
- Een senior beleidsadviseur bij de Directie Digitale Economie / Directoraat-Generaal Bedrijfsleven en Innovatie, Ministerie van Economische Zaken en Klimaat;
- Een Adviseur Strategie en Beleid, vanuit KPN CISO Office.

De werkgroep werd begeleid door een senior adviseur bij Bureau Secretaris van de CSR.

De vraag/opdracht waarmee de werkgroep aan de slag is gegaan luidt als volgt:

> *Welke reële alternatieven zijn er om rechtmatige toegang tot end-to-end versleutelde communicatie te krijgen, anders dan verzwakking van encryptie?*

De werkgroep had dus nadrukkelijk *niet* de opdracht om te kijken naar mogelijkheden om encryptie te doorbreken, maar juist om alternatieven daarvoor te onderzoeken. De werkgroep heeft in een aantal interne expertsessies in de breedte naar de vraagstelling gekeken en is uitgekomen bij twee belangrijke onderwerpen: (1) **hacken**, door politie en inlichtingendiensten, en (2) **vordering van bedrijfslogs**, d.w.z. van gegevens die bedrijven verzamelen voor hun bedrijfsvoering. Dit verslag gaat, na een korte inleiding, nader in op deze twee onderwerpen en komt dan tot enkele aanbevelingen.

Wanneer in het onderstaande gesproken wordt over interceptie (tappen) van telefoonverkeer en van andere vormen van communicatie is de aanname steeds dat dit slechts plaatsvindt door de daartoe bevoegde instanties (met name: politie en inlichtingen & veiligheidsdiensten) binnen de daarvoor bestaande wettelijke kaders, met de juiste toestemmingen en de verschillende vormen van toezicht. Hetzelfde geldt voor inzet van de hackbevoegdheid. Onder deze bevoegdheid wordt een grote verscheidenheid aan activiteiten uitgevoerd. Deze variëren van het (forensisch) kopiëren van een USB-stick of harde schijf, tot het uitvoeren van een gecompliceerde hack-operatie op grote netwerken. Als er gesproken wordt over de handeling 'hacken' wordt eigenlijk altijd het op afstand binnendringen in computers bedoeld. Die interpretatie wordt hier ook gevolgd.

Het tappen is de afgelopen tientallen jaren internationaal uitgekristalliseerd, zowel technisch, als organisatorisch en juridisch. Deze (publieke) standaardisatie van interfaces en architectuur voor interceptie biedt veel voordelen: enerzijds rechtszekerheid voor burgers en anderzijds professionele duidelijkheid en uitvoerbaarheid voor de opdrachtgevers en uitvoerders. Commercieel beschikbare telecom infrastructuur omvat deze gestandaardiseerde tap functionaliteit.

Met de *end-to-end* (E2E) versleuteling van moderne, populaire *over-the-top* (OTT) berichtendiensten (zoals: Whatsapp, Signal, Telegram) is deze toegankelijkheid en overzichtelijkheid (voorgoed) verdwenen. Omdat een

heldere structuur zoals die voor het tappen van telefoons gefunctioneerd heeft niet bestaat voor OTT-diensten – en op korte en middellange termijn ook niet te verwachten is – is het belangrijk om zicht te hebben op het spectrum aan alternatieven dat voor handen is. Deze notitie heeft een technische focus en bespreekt bijv. niet de juridische alternatieven, zoals verruiming van de mogelijkheden voor online infiltratie. Deze notitie is in korte tijd tot stand gekomen, gebaseerd op zeer beperkt onderzoek, en heeft geen pretentie van volledigheid.

Overigens staat het tappen niet alleen door de beschikbaarheid van deze OTT-diensten onder druk. Ook bij de 5G infrastructuur die nu uitgerold wordt is er nog geen internationale helderheid. Door de versleuteling van signaleringsinformatie bij 5G kan een buitenlandse 5G telefoon in Nederland in beginsel niet getapt worden. Andersom bestaat dit probleem ook. Alleen in het land van herkomst kan de ontsleuteling van de signaleringsgegevens, en daarmee de tap, plaatsvinden. Om nationaal tappen van internationale telefoons wel mogelijk te maken moet in de (honderden) roamingsovereenkomsten tussen telecomaanbieders afgesproken worden om deze versleuteling uit te zetten. Aanbieders staan enerzijds onder druk van hun klanten (en van de AVG) om *wel* te versleutelen en anderzijds onder druk van justitiële autoriteiten om *niet* te versleutelen, om internationale taps mogelijk te maken. Deze discussie loopt nog, waarbij Nederland in Europa een actieve rol speelt. Op deze discussie zelf wordt hier niet verder ingegaan.

1. Hacken

Inlichtingen & veiligheidsdiensten hebben sinds de WiV 2002 de wettelijke basis om computers (van targets) te kunnen binnendringen, ofwel rechtstreeks, ofwel indirect. De wet CC III geeft de politie sinds 2019 een vergelijkbare bevoegdheid. Bij de inlichtingen & veiligheidsdiensten is hacken een standaard onderdeel van de werkwijze geworden. Bij de politie is het middel nog niet zo ver ingedaald en uitgekristalliseerd (zie het rapport Verslag toezicht wettelijke hackbevoegdheid politie 2020 en een nog te verschijnen rapport van het WODC). De politie heeft te maken met zwaardere beperkingen bij het uitvoeren van hacks, met name op het gebied van de tools en de kwetsbaarheden die ingezet mogen worden.

Bij hacken kan tot op zekere hoogte gebruik gemaakt worden van tools (of scripts) die ofwel aangekocht ofwel zelf opgezet zijn. De markt voor deze tools is omstreden, zie de discussie rond het Israëlische bedrijf NSO, dat nu uitgesloten is in de V.S. Zulke tools zouden hacken makkelijker kunnen maken, maar hebben als nadeel dat ze, op basis van hun uniforme werkwijze, door targets herkend kunnen worden. Ook is de effectiviteit op de langere termijn van deze tools onzeker, omdat de kwetsbaarheden waar ze nu gebruik van maken, op een goed moment onbruikbaar kunnen worden, typisch door een patch.

Hacken is voor een groot deel maatwerk en handwerk. Het middel is niet (internationaal) technisch/ organisatorisch/juridisch gestandaardiseerd. Het is bovendien niet schaalbaar: als je een twee keer zo grote hack-opbrengst wil, heb je twee keer zo veel hackers nodig.

Met hacken zijn de laatste jaren indrukwekkende resultaten behaald, zoals de ontmanteling van verschillende beveiligde communicatienetwerken van criminelen. Juist voor dit soort grote zaken, met een lange adem, is hacken een geschikt middel gebleken. Maar ook daar is de opbrengst vooraf onzeker.

Hacken kan gericht zijn op (hosting) infrastructuur en tegen de daar actieve verdachten/targets. Het hacken van mobiele telefoons is trager van de grond gekomen omdat een daarvoor geschikte uitgangspositie minder vanzelfsprekend voorhanden is. Op dit punt is verbetering voorstelbaar, via een nieuwe wettelijke en technische regeling, waarbij politie en inlichtingen & veiligheidsdiensten een betere uitgangspositie krijgen bij telecomproviders, zodat ze directe toegang hebben tot de verkeersstromen van-en-naar een specifieke telefoon. Daarbij blijft *end-2-end* versleuteling (noodzakelijkerwijs) onaangetast, maar is er wel een betere toegang om via een hackoperatie op een specifiek telefoontoestel binnen te dringen.

2. Bedrijfslogs

Omdat OTT-diensten *end-2-end* versleuteld zijn hebben de bedrijven die deze diensten aanbieden zelf geen toegang tot de inhoud van de communicatie. Wel slaan ze met betrekking tot deze communicatie allerlei bedrijfsvoeringsgegevens (logs) op, o.a. voor het kunnen uitvoeren van de dienst, voor fraude-detectie, voor profilering en marketing. Het gaat dan om de identiteit van de betrokkenen, de contacten, tijdstippen, locaties, duur, omvang en aard van de berichten, etc. Ook kunnen deze bedrijven op de toestellen zelf controles uitvoeren, in hun eigen apps, en kunnen ze daar de mogelijkheid bieden tot een (versleutelde) backup van het berichtenverkeer. Wat precies bijgehouden en opgeslagen wordt is in het algemeen niet bekend.

De Nederlandse politie en inlichtingen & veiligheidsdiensten vragen met enige regelmaat gegevens op bij (vaak Amerikaanse) aanbieders van OTT-diensten. Daarbij spelen de verschillen een rol tussen de rechtssystemen van Nederland/Europa en van de V.S., en tussen de daarin gebruikte begrippen en interpretaties. In Nederland wordt gewoonlijk een onderscheid gemaakt tussen identificerende en niet-identificerende gegevens, in lijn met de AVG. In de V.S. is het onderscheid tussen inhoud en meta-data van groter belang. Deze onderscheidingen sluiten niet op elkaar aan. Zo worden locatiegegevens in Nederland als meta-data gezien, maar in de V.S. als inhoud. In de praktijk kunnen account-gegevens (geregistreerd bij het aanmaken van het account) rechtstreeks bij het bedrijf zelf opgevraagd; ze worden dan relatief snel geleverd (in de orde van weken). Andere (gebruiks)gegevens moeten via het Amerikaanse ministerie van Justitie opgevraagd worden. Die procedure duurt langer (in de orde van maanden), waarbij niet altijd alle gegevens geleverd worden. De betrokken bedrijven houden de boot nogal eens af met als verweer dat ze niet weten waar de gevraagde gegevens staan. Het merendeel van de Nederlandse opvragingen betreft daarom accountgegevens.

Onderzoekers bij politie en inlichtingen & veiligheidsdiensten zijn vaak zaak-gedreven, zonder strategisch lange-termijn perspectief. Ze zijn gewend verschillende routes te bewandelen en schakelen makkelijk over van de ene route naar de andere wanneer bepaalde opbrengst tegenvalt. Hierdoor is van gebrekkige levering van bedrijfslogs nooit een fundamentele zaak gemaakt en is er ook nog nooit een juridische procedure gestart om (snellere, uitgebreidere) levering af te dwingen. Ook is, zover bekend, niet geprobeerd om betrokken bedrijven via hun vestigingen in Nederland aan te spreken onder Nederlands recht. Hier ligt ruimte voor verbetering. Ook zou de wettelijke basis voor (internationale) vorderingen versterkt kunnen worden. Daarnaast biedt publiek-private samenwerking bij fraude-bestrijding ruimte voor een meer effectieve aanpak, inclusief hulp aan slachtoffers.

3. Aanbevelingen

1. Probeer de verminderde opbrengst van de traditionele goedgeorganiseerde telefoontaps niet op één enkele wijze op te vangen, maar bekijk het geheel, als spectrum van mogelijke alternatieve middelen.

2. Veranker en stroomlijn het hacken als opsporingsmiddel bij de politie, in lijn met het aanstaande WODC-rapport, maar erken dat hacken slecht schaalt, maatwerk is, vooral geschikt is voor grote zaken, en geen gegarandeerde opbrengst kent.

3. Bewerkstelling in een Europees kader voor het tappen van 5G verbindingen eenzelfde transparantie, uniformiteit en rechtszekerheid als nu gangbaar is in de telecomwereld.

4. Onderzoek de mogelijkheid van een transparante wettelijke regeling voor versterkte toegang bij telecomproviders, teneinde een betere uitgangspositie te hebben om specifieke mobiele telefoons te kunnen hacken.

5. Dwing aanbieders van online diensten tot nauwere samenwerking en levering van bedrijfsvoeringsgegevens (logs). Dit kan op korte termijn via jurisprudentie en op langere termijn via (internationale) wetgeving.

6. Benader deze vordering van gegevens meer vanuit Nederlands/Europees perspectief, om interpretatiekwesties onder Amerikaans recht te vermijden. Mogelijke aanknopingspunten zijn hierbij: de Nederlandse/Europese vestigingen van de betrokken bedrijven en ook de eigen Europese kijk op gegevens, waarbij de zeggenschap bij data-subjecten ligt en niet bij verwerkende organisaties.

7. Organiseer nauwere publiek-private samenwerking met de fraude-afdelingen van deze leveranciers van diensten in de informatiesamenleving. Benadruk hierbij de maatschappelijke zorgplichten die grote ICT-partijen hebben.