Ministerie van Binnenlandse Zaken en Koninkrijksrelaties en
Ministerie van Defensie

Betreft: Internetconsultatie Wet op de inlichtingen- en veiligheidsdiensten 20XX

31 augustus 2015, Den Haag, Helsinki, Olpe

Geachte mevrouw, heer,

Wij danken u voor de gelegenheid een reactie te geven op het wetsvoorstel ter vervanging van de huidige Wet op de inlichtingen- en veiligheidsdiensten 2002 (Wiv 2002). Deze reactie is geschreven namens PowerDNS.COM BV, Dovecot Oy en Open-Xchange AG. PowerDNS is een Nederlandse leverancier van producten ten behoeve van aanbieders van telecommunicatiediensten, en is de software achter ongeveer 30% van alle domeinnamen op Internet. Dovecot levert naar schatting de technologie achter 50% van alle mailbox servers. Afsluitend, Open-Xchange onze (aanstaande) moedermaatschappij levert software die de email en overige communicatie ondersteunt van meer dan 120 miljoen gebruikers. Onze respectievelijke softwareproducten zijn in gebruik bij de grootste aanbieders van telecommunicatiediensten ter wereld.

De hoofdauteur van dit document heeft vanuit zijn vorige carriere twaalf jaar ervaring met 'Lawful Interception' (LI) in het brede & internationale spectrum van het implementeren van tap-installaties, het ontwikkelen, leveren en gebruiken van LI software tot het meeschrijven aan relevante Nederlandse wet- en regelgeving. Deze inzending is zorgvuldig opgesteld om geen blijk te geven van het kennisniveau en modus operandi van de Nederlandse inlichtingen- en veiligheidsdiensten (verder: de Diensten).

Wij vrezen dat in de huidig voorgestelde vorm de nieuwe Wet op de inlichtingen- en veiligheidsdiensten eerder een gevaar is voor "het voortbestaan van de democratische rechtsorde en de veiligheid" (artikel 8) dan dat deze daaraan bijdraagt.

Wij delen de zeer grote zorgen over de privacyschendingen en de doel- en rechtmatigheid van dit nieuwe wetsvoorstel zoals geuit door andere respondenten van deze consultatie. Onze zorg hierover kon niet groter zijn. In deze inzending echter willen wij ons concentreren op specifieke tekortkomingen en grove fouten in het voorliggend voorstel, met name aangaande de artikelen met betrekking tot de afluisterbevoegdheden.

In dit document delen wij eerst kort de problemen die wij waarnemen, gevolgd door onze aanbevelingen. Mogelijk ietwat ongebruikelijk vervolgen wij daarna met een uiteenzetting van hoe de communicatiegerelateerde artikelen van het voorstel onderling samenhangen (met diagram). Na behandeling van enige praktische punten sluiten wij ter illustratie af met een scenario hoe een nieuwe 'WIV 20XX' gevolgen zou kunnen hebben voor de Dienst Automatisering van de Tweede Kamer.

Voor wij aanvangen willen wij de vele partijen die mee hebben geholpen[1], direct of indirect, bij de totstandkoming van dit document bedanken.

In het kort zien wij in het voorliggende voorstel de volgende problemen:

- Het voorstel handhaaft het curieuze stelsel dat ambtenaren zelf toestemming mogen geven tot het grootschalig bulk afluisteren en opslaan van communicatie, maar dat de betrokken dienst daarmee nog

[1] https://twitter.com/PowerDNS_Bert/status/637904099699224576

geen ‘kennis neemt’ van deze communicatie. Deze ‘kopen maar niet kijken’ constructie bindt de kat op het spek.

- De nieuwe “medewerkingsplicht” voor tappen is in het geheel niet uitgewerkt, waardoor een hoge mate van onzekerheid (zowel in kosten als verplichtingen) voor het bedrijfsleven wordt gecreëerd. Deze onzekerheid zal voor veel bedrijven en zeker voor de onze, leiden tot het besluit servers en communicatiediensten snel buiten Nederland te plaatsen, en zeker geen nieuwe investeringen te doen die onder de reikwijdte van deze wet vallen.
    - De medewerkingsplicht kan bijvoorbeeld **ongelimiteerde** investeringen vergen die volgens het huidige voorstel niet vergoed zullen worden.
        - Er is geen enkel kader voor proportionaliteit van de inzet en ingrepen die bij aanbieders verplicht worden gesteld.
    - Het is onduidelijk wie er aansprakelijk is bij storing van de onder deze plicht geplaatste apparatuur en wie de schade bij onderbreking van de communicatiedienstverlening zou vergoeden. **Iedere toevoeging van interceptieapparatuur verlaagt per definitie de betrouwbaarheid en veiligheid van een netwerk.**
    - Er zijn geen technische standaarden vastgelegd waarmee invulling gegeven kan worden aan medewerkingslasten aangaande bulk tappen, waardoor benodigde programmatuur en apparatuur niet voorbereid of aangeschaft kan worden. Dit leidt tot hele dure ‘after sales’ gesprekken met leveranciers van netwerkapparatuur.
- De rechtspositie van aanbieders van communicatiediensten bij niet willen of kunnen voldoen aan een medewerkingslast lijkt te bestaan uit ‘strafrechtelijk vervolgd worden voor een misdrijf met een gevangenisstraf van twee jaar’[2]. Er is geen mogelijkheid tot beroep.
    - Het voorstel vordert vrijheidsstraf of een boete bij gebrek aan medewerking door aanbieders van communicatiediensten, of zelfs ‘onopzettelijk gebrek aan medewerking’. Wij vrezen dat met het dreigement van vrijheidsstraf lager technisch personeel en kleinere aanbieders zich gedwongen zullen voelen sowieso mee te werken, en niet de kans of toegang krijgen tot een adequaat verweer
    - Ook voor bedrijfsmatige aanbieders is het denkbaar dat de gevangenisstraffen en boetes op medewerkers verhaald zullen worden[3]
- Artikel 22 lid 3 maakt de levering van communicatie mogelijk die eigenlijk valt onder artikelen 30 tot en met 40, met dien verstande dat onder het regime van artikel 22 de Diensten direct zonder verdere toestemmingen of lastgevingen geheel kennis mogen nemen van de informatie.
- De sterke dwang voor ongeclausuleerde medewerking zou, bij onwil of onmacht tot medewerking, uitgeruild kunnen worden tegen het ‘vrijwillig’ leveren van andere gegevens, bijvoorbeeld klantenbestanden, overige communicatiestromen, betalingsgegevens of locatiegegevens onder artikel 22 lid 3. Er is dan sprake van *détournement de pouvoir*. Het artikel 22 regime is voor de Diensten sowieso aantrekkelijker dan de medewerkingsplicht, indien de leverancier van de informatie vrijwillig meewerkt.
- Het voorliggende voorstel definieert een klasse ambtenaren (‘supertappers’) die zelf zonder nadere toestemming volledig *kennis mogen nemen* van alle bulk getapte communicatie. Dit is ongehoord en schendt ieder principe van behoorlijk overheidshandelen. Dit is een staat in een staat.
    - Mede hierom is het verlenen van toestemming voor de bestaande en nieuwe bevoegdheden door ambtenaren en betrokken ministers zelf zeer problematisch
- Deze ‘supertapper’ ambtenaren zijn in een buitengewoon penibele positie. Bij uitsluiting van hun collega’s[4] kunnen zij kijken naar de ‘ruwe’ afgeluisterde informatie, ook uit die bronnen waar in bulk (ongericht) afgeluisterd wordt. Indien de minister (nog) geen toestemming heeft verleend om middels artikel 35 *kennis te nemen* van getapte informatie staan deze medewerkers onder grote collegiale druk van teams om een tip van de sluier op te lichten of eventueel een voorschot te nemen op te verwachten ministeriele toestemming. Wij wensen niemand deze rol toe.
- De Diensten mogen zelf, zonder toestemming van de betrokken minister[5], ‘selectiecriteria’ bepalen waarmee via artikel 35 kennis mag worden genomen van bulk afgeluisterde informatie. Specifiek bepaalde

---

[2] Uit artikel 132: “Overtreding van de in het eerste lid strafbaar gestelde feiten wordt gestraft a. in geval van een misdrijf, met gevangenisstraf van ten hoogste twee jaar of geldboete van de vierde categorie; b. in geval van een overtreding, met hechtenis van ten hoogste zes maanden of geldboete van de vierde categorie”

[3] https://nl.wikipedia.org/wiki/Strafrecht_(Nederland)#Daderschap_van_de_privaatrechtelijke_rechtspersoon

[4] Uit artikel 33: “welke ter uitvoering van het bepaalde in dit artikel bij uitsluiting van anderen kennis mogen nemen van de ingevolge artikel 33 verworven gegevens ten behoeve van de in het eerste lid, tweede volzin, bedoelde activiteiten”

[5] Uit artikel 35 “Het vaststellen van de selectiecriteria geschiedt (...) namens deze het hoofd van de dienst.”.

selectiecriteria (‘Jansen’ of ‘twitter.com’) zijn mogelijk direct gerelateerd aan een door de Minister goedgekeurde selectielast, maar kunnen ook vrijwel alle ongerelateerde communicatie selecteren.

- De definitie van aanbieder van communicatiediensten[6] omvat, voor zover wij kunnen zien, vrijwel ieder bedrijf met een telefoon, fax, mailserver of webforum, naar schatting 360000 organisaties in Nederland. De definitie omvat niet alleen daadwerkelijke aanbieders van communicatiediensten maar ook allen die **namens** een dergelijke aanbieder data opslaan of verwerken.
    - Dit maakt een eindeloze keten van leveranciers mogelijk die zo allen ‘aanbieder van een communicatiedienst’ worden!
- De diensten mogen hun bijzondere bevoegdheden inzetten voor een aantal waardige doelen zoals het voortbestaan van de democratische rechtsorde en ‘de veiligheid’. In aanvulling hierop handhaaft het huidige voorstel de mistige grondslag ‘gewichtige belangen van de staat’ (artikel 8). Dit is een gigantische ‘loophole’ waarmee allerhande (nieuwe, zware) bevoegdheden gelegitimeerd kunnen worden. Indien een bevoegdheid geen nood vindt in voortbestaan van de democratische rechtsorde of de veiligheid, wat kan het dan nog zijn?

Aanbevelingen

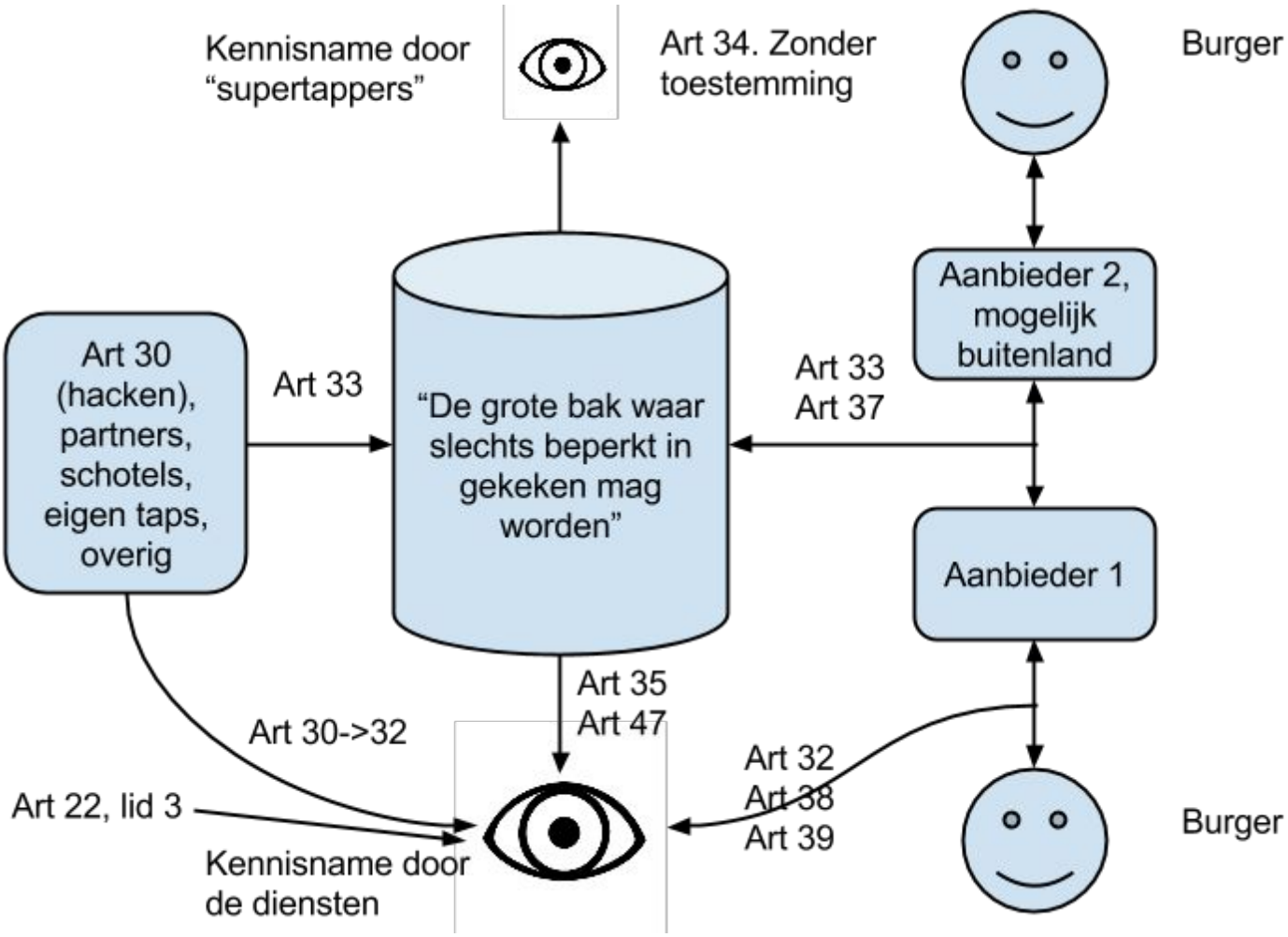
- Verhuis het door ambtenaren en minister verlenen van toestemming voor afluisteren naar de rechterlijke macht, gelijk artikel 29 nu voor het briefgeheim
- Werk de medewerkingsplicht veel verder uit, en regel daarbij minimaal:
    - Welke medewerkers binnen een organisatie aangesproken mogen worden, en dat dit een directiemedewerker met beslissingsbevoegdheid zal moeten zijn waarvan verwacht kan worden dat deze zich juridisch kan laten bijstaan in de beoordeling van het verzoek
    - Een beroepsmogelijkheid voor aanbieders van communicatiediensten anders dan afwachten van een dagvaarding voor vervolging voor een misdrijf met een gevangenisstraf van 2 jaar
        - Faciliteer tevens dat er voldoende juristen met de juiste screening beschikbaar zijn om deze aanbieders bij te staan
        - Bij deze beroepsmogelijkheid zou ook de proportionaliteit van de medewerkingslast bekeken moeten worden. Is het bijvoorbeeld legitiem om een kleine opleidingsinstelling te dwingen een gehele tapinstallatie aan te schaffen voor 1 mogelijke tap?
    - Dat de diensten ongelimiteerd aansprakelijk zijn voor schade als gevolg van storingen veroorzaakt door implementatie van het medewerkingsverzoek, met omgekeerde bewijslast
    - In welke mate communicatieaanbieders verplicht kunnen worden tot investeringen die geen ander doel dienen dan ‘meewerken’ en vanaf welk bedrag de overheid ook de investeringskosten zal dragen
    - Dat de vergoeding voor operationele kosten van hooggekwalificeerd technisch personeel meer bedraagt dan 50 euro per uur (het uit de Telecommunicatiewet overgenomen bedrag).
    - Dat verduidelijkt is of de medewerkingsplicht ook vervuld mag worden door buitenlands (ongescreened) personeel
- Aanbevelingen op technisch vlak voor de medewerkingsplicht:
    - Verplicht de Diensten zich te committeren aan het exclusieve gebruik van gepubliceerde protocollen en technieken
    - Stimuleer de ontwikkeling van een open source platform dat voor veel gebruikte communicatieplatformen ‘medewerking’ voor artikelen 32 en 38 implementeert; daarmee kan aan de bulk van de 360000 kleine aanbieders van communicatiediensten tegemoet worden gekomen,
        - Stel een testplatform beschikbaar waarop organisaties hun tapvoorziening kunnen testen
- Sluit de open deur van “andere gewichtige belangen van de staat” (artikel 8) uit als grondslag voor het inzetten van (minimaal) artikelen 30, 32, 33, 37 en 38.
- Beperk de definitie van aanbieders van communicatiediensten tot daadwerkelijke aanbieders van deze diensten, en verwijder de clausule dat eenieder die diensten levert AAN een aanbieder van communicatiediensten ook een dergelijke aanbieder is.

[6] Uit artikel 31: “aanbieder van een communicatiedienst: de natuurlijke of rechtspersoon die in de uitoefening van een beroep of bedrijf aan de gebruikers van zijn dienst de mogelijkheid biedt te communiceren met behulp van een geautomatiseerd werk, **of die gegevens verwerkt of opslaat ten behoeve van een zodanige dienst of de gebruikers van die dienst”**

- Voeg een lid toe aan artikel 22 waarbij expliciet wordt gemaakt dat gegevens die ingewonnen zouden kunnen worden via artikelen 30 tot en met 40 ook daadwerkelijk onder het regime van die artikelen verkregen moeten worden.
- Voeg een lid toe aan artikel 22 waarbij leverancier van gegevens aan AIVD verklaart dat deze gegevens daadwerkelijk vrijwillig overhandigd zijn, en niet ter compensatie voor onmacht of onwil te voldoen aan de medewerkingsplicht communicatiegegevens.
- Aangaande de 'supertappers' uit artikel 35:
    - Verschaf deze aangewezen ambtenaren een zeer heldere rechtspositie, waardoor zij nooit onder druk gezet kunnen worden door hun meerderen om de kennis die zij 'bij uitsluiting' mogen nemen binnen de dienst te delen, ook niet 'heel even'.
        - Overweeg deze ambtenaren in dienst te laten zijn van een ander ministerie
    - Als onderdeel van deze rechtspositie dient deze ambtenaren de mogelijkheid geboden te worden de vice-president van de Raad van State of de president van de Hoge Raad direct te benaderen indien zij in gewetensnood komen. Deze gesprekken dienen geprivilegieerde informatie te zijn en behandeld te worden als geheimhouderscommunicatie.
- Leg verslag van de hoeveelheid 'hits' op basis van door ambtenaren bepaalde selectiecriteria uit artikel 35, en inschatting welk percentage hits gerelateerd was aan door de minister goedgekeurde selectielasten. Dit voorkomt selectie op termen die (veel) te breed matchen.

Samenvatting relevante artikelen en hun samenhang

Het voorliggende wetsvoorstel handhaaft de internationaal gezien curieuze constructie dat de Diensten communicatie mogen afluisteren en verzamelen, zonder dat er toestemming is ook "kennis te nemen" van deze communicatie. Met andere woorden, er mag een 'bak' gevuld worden met gegevens, en die gegevens mogen drie jaar lang in de bak blijven zitten, maar men mag er niet alles mee doen. De diensten mogen volledig kennisnemen van communicatie die na toestemming (artikel 35) uit de bak 'geselecteerd' is.



In de huidige WIV mag de bak gevuld worden met 'niet-kabelgebonden communicatie met oorsprong in het buitenland'. Daarnaast kunnen specifieke individuen en organisaties afgeluisterd worden. Nieuw in het voorliggend voorstel is dat alle kabels nu ook 'ongericht' (bulk) getapt mogen worden om de bak te vullen.

In aanvulling op de huidige WIV mogen er ook automatische analyses op de gesloten bak uitgevoerd worden, waarbij slechts voor sommige analyses specifiek toestemming vereist is. Tevens creëert het voorstel een bijzondere nieuwe klasse ambtenaren ('supertappers') die ook zonder specifieke toestemming in de bak mogen kijken, met als bedoeling dat zij daarmee hun analyses vorm kunnen geven en kunnen helpen bij het bepalen van selectiecriteria waarvoor vervolgens toestemming gevraagd kan worden.

Dit wordt verantwoord met het idee dat de gegevens die in de 'verzamelen maar niet kijken'-bak zitten geen echte privacy-schending opleveren (maar zie onder).

Ook bijzonder in deze context is dat de nieuwe WIV een medewerkingsplicht voor bulk afluisteren oplegt aan aanbieders van communicatiediensten **en zelfs aanbieders van diensten aan communicatiediensten**. Tevens definieert men deze aanbieders als 'zij die onder de Telecommunicatiewet aanbieders zijn, aangevuld met zij die dat volgens deze wet niet zijn'. Met andere woorden, vrijwel iedereen.

Onderlinge samenhang artikelen

Middels **artikel 32** (stromend) en **artikel 38** (opgeslagen) moeten aanbieders als gedefinieerd in **artikel 31** communicatie van specifieke organisaties, individuen geïdentificeerd door telefoonnummers, emailadressen, facebook logins, etc, overdragen aan de diensten. Een dergelijke 'gerichte tap' kan ook gerealiseerd worden door een computer/telefoon/geautomatiseerd werk te hacken via **artikel 30**, waarbij sowieso kennis wordt genomen van alle informatie op dit geautomatiseerd werk.

Via **artikel 33** mogen de diensten bulk communicatie vergaren uit diverse bronnen om deze 3 jaar te bewaren **zonder er kennis van te nemen**. Alleen de 'supertappers' mogen de gegevens in de bulk 'bak' zonder nadere toestemming bestuderen. Via **artikel 37** worden alle aanbieders van communicatie (en ook hun onderliggende leveranciers) verplicht mee te werken aan bulk afluisteren van hun netwerken ten behoeve van **artikel 33**.

Middels **artikel 34** mogen de 'supertappers' de inhoud van de bulk bak bestuderen en analyseren (**artikel 47**), onder andere om selectiecriteria te maken die dan via **artikel 35** de rest van de diensten in staat stellen 'kennis te nemen' van geselecteerde data.

Informatie over netwerken (topologie, configuratie, geen communicatie-inhoud of metadata) kan opgevraagd worden via **artikel 36.** Informatie over gebruikers moet geleverd worden via **artikel 40**. Metadata van communicatie uit heden, verleden en toekomst kan opvraagd worden via **artikel 39**.

Tenslotte kunnen de Diensten zich middels **artikel 22** tot eenieder (overheidsonderdeel of niet) wenden om, ondanks wat overige wet- en regelgeving daarover zegt, eenmalig of permanent (online) toegang te krijgen tot "gegevens".

Enkele praktische punten

Voor gericht tappen zijn over de afgelopen jaren goede procedures uitgewerkt. Alle (grote) Nederlandse aanbieders zijn aftapbaar, en de kleinere hebben zich verenigd in een organisatie die onderling tapapparatuur uitwisselt[7]. Nederland is hiermee een voorbeeld voor de hele wereld. Via open onderhandelde standaarden worden getapte gegevens overgedragen en er is een rijk scala aan leveranciers van benodigde hard- en software.

Voor de nieuwe (bulk)tapbevoegdheden is echter in het nieuwe wetsvoorstel niets geregeld, behalve dat aanbieders 'mee moeten werken'.

Dit zou bijvoorbeeld in kunnen houden dat de provider toe moet staan dat een 'zwarte doos' in het netwerk geplaatst wordt waar aangewezen fibers doorheen moeten lopen. Deze doos zou dan met een extra verbinding

[7] Nederlandse Beheersorganisatie Internetproviders: http://www.nbip.nl/diensten/tapdiensten/

aangesloten kunnen worden op de Diensten. Tevens zal de goede werking van deze 'zwarte doos' moeten worden gewaarborgd, bijvoorbeeld dat deze op juiste wijze van voedingsspanning zal moeten worden voorzien.

In andere gevallen kan het er ook neerkomen dat de medewerking bestaat uit het extensief herconfigureren van apparatuur en het aanschaffen en installeren van nieuwe hardware- en softwaremodules om door de overheid gewenst verkeer op te sturen.

Ook ten aanzien van geheimhouding zijn er vragen te stellen. Een traditionele gerichte taplast kan zeer beperkt bekend zijn binnen een aanbieder van telecommunicatiediensten. Hoewel iedereen kan weten dat krachtens de wet de provider aftapbaar moet zijn voor specifieke gebruikers kan de identiteit van de afgeluisterde gebruikers eenvoudig afgeschermd worden.

Bij bulk afluisteren in gevolg van artikel 37 is het veel lastiger om geheim te houden welke verbindingen afgeluisterd worden, daar er apparatuur in het netwerk geplaatst wordt die gekoppeld is met specifieke netwerkelementen die niet alle klanten bedienen.

Het ligt voor de hand dat als onderdeel van de medewerkingsplicht de diensten het gebruik van Nederlands, gescreened, personeel zullen verplichten. Gegeven de grote internationalisering en vrijwel universele outsourcing zal dit een disproportionele belasting leggen op aanbieders van communicatiediensten.

Wegens het gebrek aan verdere definitie van 'medewerking' blijven wij over dit alles in onzekerheid.

Aansprakelijkheid

Uit ervaring blijkt dat interceptieapparatuur de betrouwbaarheid van netwerken verlaagt, alleen al doordat simpelweg meer handelingen verricht moeten worden en er "meer kapot kan".

Tevens kan de apparatuur zelf bijvoorbeeld kortsluiting veroorzaken, defect raken (want, wie is bevoegd hierop onderhoud op te plegen?) of het netwerk (onbedoeld) zwaarder te belasten door (te) veel gegevens naar de overheid te sturen.

De Nederlandse overheid zou voldoende vertrouwen in haar handelen moeten hebben om aanbieders middels een omgekeerde bewijslast een ruime vergoeding te garanderen voor eventuele schade naar aanleiding van onder 'verplicht meewerken' geleverde diensten.

Een mogelijk scenario

Onder het voorliggende wetsvoorstel (in tegenstelling tot de huidige WIV) kunnen de diensten de Dienst Automatisering (DA) van de Tweede Kamer verplichten om:

- Netwerkdiagrammen op te leveren, hoe de diverse fracties op het parlementaire netwerk zijn aangesloten, gegevens over hoe de draadloze (wifi) infrastructuur gekoppeld is (Art 36)
- Te vertellen wat het wachtwoord is voor het access point van de VVD fractie (indien bekend bij de DA) (Art 30)
    - En anders graag een kopie van al het netwerkverkeer naar deze fractie (Art 33/37)
- Een tap op alle telefoongesprekken van de SP fractie (over zowel de interne als de externe lijnen) (33/37)
- Een tap op alle telefoongesprekken naar Israël vanuit de Kamer (33/37)
- **Apparatuur aan te schaffen om deze telefoontaps mogelijk te maken**
- Een kopie te leveren van de data opgeslagen ten behoeve van de PvdA fractie ('de netwerkschijf') (Art 38)
- De doorgaande overdracht te verlangen van alle opgeslagen en toekomstige email en al het Microsoft Lync verkeer van de gehele D66 fractie (Art 38)
- De installatie van een "zwarte doos" op de wifiverbinding die aan journalisten beschikbaar gesteld wordt (Art 33/37)
- Een permanente kopie van al het netwerkverkeer van het gehele parlement (Art 33/37)

De vergoeding voor bovenstaande handelingen zal het salaris zijn van de betrokken medewerkers, vermeerderd met direct gerelateerde kosten (administratief, bureau, ondersteuning). Investeringen voor hardware of software gemoeid met de overdracht zal niet vergoed worden. Voordat de taps 'live' gaan zal er overleg plaatsvinden.

Indien de DA niet mee zou werken aan bovenstaande verzoeken kan men dit weigeren, waardoor de strafmaat direct overgaat van 'overtreding' naar 'misdrijf' en daarmee een boete uit de 4e categorie of een gevangenisstraf van 2 jaar, wegens 'opzettelijk niet meewerken'. Als het de DA ondanks haar beste bedoelingen niet lukt om te voldoen aan de eisen blijft de celstraf beperkt tot zes maanden (of de equivalente boete).

Onbekend is wie er precies de cel in zou moeten als de boete niet betaald wordt:

- Het hoofd van de Dienst Automatisering
- De voorzitter van het presidium, de kamervoorzitter
- De direct benaderde systeembeheerder
- De minister van Binnenlandse Zaken als budgethouder

Ook onduidelijk is of de betrokken verdachte een fatsoenlijk verweer zou kunnen voeren, daar de medewerker van de AIVD/MIVD ongetwijfeld een geheimhoudingsovereenkomst heeft afgesloten met betrokkenen, en alle details staatsgeheim zijn

Indien de 'zwarte doos' een storing in het netwerk veroorzaakt, de stoppen door laat staan, of uitbrandt, is onduidelijk of deze schade vergoed zou worden. Ook zal er geheimhouding betracht moeten worden over het incident.

Afsluitend

Het voorliggende voorstel baart ons grote zorgen. We hopen dat de bovenstaand geconstateerde problemen en de gesuggereerde oplossingen voor u stof tot nadenken zijn.

Indien het voorgaande tot vragen leidt zijn wij gaarne bereid tot een nadere toelichting. Gelieve in dat geval contact op te nemen met Bert Hubert via bert.hubert@powerdns.com of 015-7850372.

Met vriendelijke groet,

Bert Hubert
Namens PowerDNS.COM BV, Open-Xchange AG en Dovecot Oy