Programma Verbeteren Aanpak Kinderporno

Rapportage

Pilot voor de beperking van de upload van kinderporno door vergelijking met politiebestanden

120727

Rapportage over de pilot voor de beperking van de upload van kinderporno door vergelijking met politiebestanden

INHOUD

Samenstelling: PVAKP / [redacted]

Voorwoord

Het maken en verspreiden van kinderpornografie – op beeld vastgelegd misbruik van kinderen – is een vorm van ernstige criminaliteit, die met inzet bestreden moet worden. Deze opvatting leeft zowel bij de politiek en het bestuur, als bij het gezag en de politie.
Het verspreiden van beeldmateriaal via het internet is echter een zaak die de politie met haar eigen bevoegdheden en dwangmiddelen maar beperkt kan aanpakken. Daarom wordt vanuit het Programma Verbeteren Aanpak Kinderporno steeds gezocht naar mogelijkheden om kinderporno beter op te sporen en naar mogelijkheden om kinderporno of de verspreiding daarvan tegen te houden.
In het verband van het tegenhouden is in september 2011 een pilot gestart in samenwerking met de bedrijven LeaseWeb en Fox-IT, gericht op het tegenhouden van "uploads" van kinderporno naar het world wide web. In de voorliggende rapportage wordt van deze pilot verslag gedaan.
Uiteraard gaat onze dank uit naar LeaseWeb en Fox-IT voor hun inzet in deze. Daarnaast wil ik een aantal andere partners, zonder wie de pilot niet had kunnen worden uitgevoerd, hartelijk dankzeggen: het Programma Aanpak Cybercrime, het team Beeld en Internet van het Korps Landelijke Politiediensten en de Koninklijke Marechaussee.

[redacted]
Programma Verbeteren Aanpak Kinderporno
[redacted]

Samenvatting

Het Programma Verbeteren Aanpak Kinderporno is een landelijk initiatief van de politie, om te komen tot verbetering van de aanpak van kinderporno. Van meet af aan is voor deze aanpak het belang van een ketenbenadering en het gebruik van een barrièremodel onderstreept.

Een belangrijk medium voor het verspreiding van kinderporno is het internet. Een manier om verspreiding via internet te voorkomen is verhinderen dat de afbeeldingen op internet worden geplaatst. De overheid is echter niet bevoegd om het gebruik van internet te beperken. Dat kunnen alleen de leveranciers van internetdiensten (hosting) die een uploadfilter als dienst kunnen aanbieden. Voor het tegenhouden van uploads is daarom samenwerking tussen de politie en private partijen noodzakelijk.

In 2009 zijn op initiatief van het bedrijfsleven voorbereidingen gestart om het tegenhouden van uploads door middel van een pilot te onderzoeken. Dit heeft geleid tot een pilot in samenwerking met de bedrijven LeaseWeb en Fox-IT, die in 2011-2012 is uitgevoerd. LeaseWeb levert wereldwijd dedicated hosting, waarbij ze servers ter beschikking stelt aan klanten en FOX-IT ontwikkelt en levert beveiliging. Het project werd financieel gesteund door het Programma Aanpak Cybercrime en voorts door het Korps Landelijke Politiediensten en de Koninklijke Marechaussee.

De centrale vragen van de pilot waren of en hoe het benutten van politiebestanden voor het vergelijken van uploads bijdraagt aan het tegenhouden van kinderporno en onder welke condities dit proces verantwoord kan worden uitgevoerd. Een mogelijk bijproduct was het vergaren van informatie over de verspreiding van kinderporno (intelligence).

Voor de pilot werden klanten van LeaseWeb geïnteresseerd, die derden in de gelegenheid stellen plaatjes op het world wide web te brengen. Eén klant heeft hierop ingetekend.
De opzet van de pilot was dat van bestaand kinderpornografisch materiaal, waarover de politie beschikt, hashcodes werden gegenereerd, de zogenaamde "hashes". Van het materiaal dat werd aangeboden voor upload werden eveneens hashcodes gegenereerd. Alle plaatjes die voor upload werden aangeboden, zouden via de hash worden vergeleken met de kinderporno-hashes. Indien de hashes overeen zouden komen was de kans statistisch groot, dat het kinderporno betrof. Het plaatje zou dan automatisch worden tegengehouden en het systeem zou de hash van het plaatje en het IP adres (internetadres) van de uploader aan Meldpunt Cybercrime zenden.

Tijdens de pilot bleken de technische problemen bij de uitvoering groter dan verwacht. Daardoor is de daadwerkelijke uitvoering van de pilot beperkt gebleven tot enkele weken. Het systeem is getest door, gecontroleerd, een als kinderporno aangemerkt plaatje voor upload aan te bieden. Dit plaatje werd via de hash herkend en inderdaad tegengehouden. Er is bovendien een signaal afgegeven aan het Meldpunt Cybercrime, maar zonder nadere gegevens. Het vergelijkingsproces per plaatje vergde tijdelijk meer tijd dan voorzien vanwege technische problemen met de "hardware". De betreffende hardware is vervangen.

Uit de pilot mag worden geconcludeerd dat met behulp van een dergelijk systeem bedrijven hun website kunnen beschermen tegen kinderpornoplaatjes die bekend zijn bij het bestand van het Korps Landelijke Politiediensten. Het toepassingsgebied blijft beperkt tot bedrijven die intekenen. De bijdrage van een dergelijk uploadfilter aan het tegenhouden van kinderporno als fenomeen is zodoende te verwaarlozen. Voor de opsporing is het systeem in het gunstigste geval van beperkte betekenis.

Naast deze inhoudelijke resultaten heeft de pilot leerervaringen opgeleverd over het barrièremodel: de verleiding om ook reactief gericht te gaan werken blijft aanwezig, de focus verschuift bij (nieuw) betrokken politie- en justitiepersoneel steeds weer richting opsporing. Voor de bedrijven zijn er leerervaringen op het technische vlak.
Tot slot is duidelijk worden dat in dit type projecten, waar zowel politiële als technische vragen aan de orde zijn, een specifieke projectleiding vergen.

De slotconclusies zijn, dat een systeem als dit kan werken voor bedrijfsbeveiliging, dat het weinig betekenis heeft voor opsporing en tegenhouden en dat verdere ontwikkeling desgewenst aan het bedrijfsleven is, waarbij de politie medewerking zou kunnen verlenen door het beschikbaar stellen van haar database met hashcodes, afgeleid van afbeeldingen van kinderporno.

1. Inleiding

1.1. Programma Verbeteren Aanpak Kinderporno

Het Programma Verbeteren Aanpak Kinderporno (PVAKP) is een landelijk initiatief van de politie om te komen tot verbetering van de aanpak van op beeld vastgelegd seksueel misbruik van kinderen. Het programma is gestart in december 2008, mede op grond van de toenemende maatschappelijke zorg over kinderporno. Reeds bij aanvang van het PVAKP werden het belang van een goede ketenaanpak en de inzet van een barrièremodel onderstreept. De pilot "beperking upload" past in dit barrièremodel, als vorm van tegenhouden.

1.2. Tegenhouden kinderporno op internet

Een belangrijk medium voor de verspreiding van kinderporno is het internet. Een manier om verspreiding via internet te hinderen of te voorkomen is te verhinderen dat de afbeeldingen op internet worden geplaatst. De overheid is op dit moment wettelijk niet bevoegd om het gebruik van internet te beperken[1]. Het beperken is voorbehouden aan die private partijen die internet aanbieden en diensten daarbinnen ondersteunen. Daarom is de pilot uitgevoerd in samenwerking met bedrijven, te weten LeaseWeb[2] en FOX-IT, op basis van de gemeenschappelijke wil om kinderporno zoveel als mogelijk tegen te houden.
Om te onderzoeken of deze aanpak kan werken - en onder welke organisatorische, juridische, capacitaire, technische en beheersmatige condities – is een pilot uitgevoerd.

1.3. Werkwijze

LeaseWeb is een toonaangevende, wereldwijd actieve leverancier van hosting en infrastructuuroplossingen. Op sites van het World Wide Web (websites) van klanten van LeaseWeb die zich bezig houden met 'User Generated Content', zgn. 'plaatjes uploadsites' of 'uploadboeren', kunnen afbeeldingen worden geplaatst middels uploaden.
Het plan was als volgt. Klanten van LeaseWeb willen geen kinderporno op hun websites en willen dat zelf actief tegengaan door het gebruik van een hashcodefilter. In dit filter wordt van elk plaatje in de upload een unieke code berekend (een "hash"). Deze hash wordt over een beveiligde verbinding van FOX-IT getoetst aan een versleutelde database van hashes van de

[1] Zie [redacted] e.a., [redacted], Den Haag 2008, 36 en 63.
[2] LeaseWeb heeft in 2009 het idee aangereikt.

kinderpornoplaatjes waarover de politie beschikt. Indien de hashes overeenkomen worden de hash en het internetadres (IP-adres) direct naar het Meldpunt Cybercrime gezonden, die het doorstuurt naar het Team Beeld & Internet van het Korps Landelijke Politiediensten (KLPD) voor verificatie. De kans is dan immers groot, dat het kinderporno betreft. Om hierover 100% zekerheid te verkrijgen is gedetailleerde digitale inspectie of visuele verificatie nodig. Bij een overeenkomst in de hashes wordt bovendien meteen een lijst aangemaakt van alle uploads van het betreffende IP-adres, omdat het mogelijk om een pakket kinderporno kan gaan. Indien de hash niet in het hashbestand voorkomt, dan wordt de afbeelding gewoon gepubliceerd.
Tot zover het plan.

1.4. VOORBEREIDING

De voorbereiding van de pilot kende een lange doorlooptijd, omdat een aantal partijen vooraf duidelijkheid wilde hebben over voor hen belangrijke punten.
Er waren bij politie en justitie in het bijzonder de volgende zorgen:

a. dat de pilot een groot beroep zou doen op politiecapaciteit resp. opsporingscapaciteit (één "hit" zou onderdeel kunnen zijn van een heel pakket kinderporno);
b. dat de inzet van de database met hashes van kinderporno-afbeeldingen door criminelen zou kunnen worden gebruikt;
c. dat deze database ja dan neen zou vallen onder het regime van de Wet politiegegevens;
d. dat medewerkers van de bedrijven de kinderporno-afbeeldingen zou kunnen zien, hetgeen een strafbaar feit oplevert;
e. dat lopend politie-onderzoek met behulp van internettap wordt gefrustreerd;

Over deze zorgen bestonden bovendien bij betrokkenen verschillende beelden.
Bij LeaseWeb leefde de zorg dat plaatjes ten onrechte als kinderporno zouden kunnen worden aangemerkt.

2. Het verloop van de pilot

Hieronder is in vogelvlucht het verloop van de pilot weergegeven.

2008	Hostingbedrijf Leaseweb doet een voorstel aan de politie om de upload van kinderporno tegen te houden naar analogie van het Zweedse NetClean.
2009-2010	Het idee wordt uitgewerkt in een projectplan. Er worden diverse fundamentele vragen aan de orde gesteld (privacy / Wet politiegegevens, opsporing, samenwerking met private sector) en er is capaciteitsgebrek bij de politie (KLPD). Het projectplan wordt herhaaldelijk bijgesteld.
30 november 2010	Het projectplan leidt tot een fiat en tot subsidie van het Programma Aanpak Cybercrime.
December 2010 – augustus 2011	Het projectplan wordt uitgewerkt in een aanpak. Hierbij komen opnieuw de vragen over opsporing ja/neen, Wet politiegegevens, het frustreren van lopend onderzoek, betrokkenheid Landelijk Parket vs. Lokaal parket, capaciteit politie enz. aan de orde. PVAKP zorgt ervoor dat het KLPD wordt versterkt met een medewerker van de Koninklijke Marechaussee.
Mei 2011	Start van de feitelijke voorbereidingen.
September 2011	Minister Opstelten geeft het officiële startsein voor de pilot. Leaseweb en FOX-IT hebben intussen technische afspraken gemaakt over de wijze van informatie-uitwisseling. Met het Meldpunt Cyber Crime zijn afspraken gemaakt over de automatische melding van een hit door Fox-IT voor doorzending naar het Team Beeld en Internet voor verdere afhandeling.
9 november 2011	Vergadering Projectgroep. Er neemt één klant van LeaseWeb deel aan de pilot. Er vindt vanuit LeaseWeb echter geen verkeer plaats. FOX-IT heeft gemeld dat de dienst online was, het concept van de whitelist voor toegang tot de dienst uitgelegd en gevraagd om IP-adressen waar vandaan Leaseweb toegang wil. FOX-IT heeft meerdere malen gevraagd om de status omdat er geen verkeer plaatsvond.
21 december 2011	Vergadering Projectgroep. ~~Leaseweb dacht dat~~ Om onbekende reden lukt het Leaseweb niet het script te activeren. Het script wordt vanuit FOX-IT gestart en draait maar FOX-IT ziet geen verkeer. Na inzet programmeur zal opnieuw getest worden.
Januari-februari 2012	Leaseweb en Fox-It hebben contact om technische problemen op te lossen (firewall whitelist, inzet programmeur en certificaten). In februari 2012 is de filter geactiveerd en kunnen hits worden doorgegeven.

29 februari 2012	Vergadering Projectgroep. Er is nog geen hit waargenomen. KLPD zal een testplaatje uploaden om te testen of deze gezien wordt. Leaseweb dient nog aanvullende programmatuur te installeren bij de klant om aanvullende gegevens van de klant mee te kunnen leveren bij een "hit".
Maart-april 2012	Technische problemen (duurzaamheid en prestaties van de cryto-hardware) en doorlooptijden van herstelwerk zorgen ervoor dat de pilot feitelijk stil ligt. De storing heeft doorgewerkt naar de dienstverlening door de klant.
16 april 2012	Een deel van de problemen is opgelost. Een eerste proef met een als kinderporno aangemerkt plaatje uit de database van de politie wijst uit dat de hash wordt herkend en tegengehouden. Er worden echter geen metagegevens (IP-adres e.d.) naar de politie verzonden. Daarvoor zijn software-aanpassingen bij de klant noodzakelijk. De klant voelt er echter niet veel voor om nadere informatie met het KLPD te delen. Bovendien ligt het gezien de eerdere storingen niet voor de hand deze klant hiermee nu te belasten.
1 mei 2012	Einde van de pilot

3. Resultaten

3.1. Centrale vragen

De centrale vragen van de pilot waren of en hoe het benutten van politiebestanden voor het vergelijken van uploads bijdraagt aan het tegenhouden van kinderporno en onder welke condities dit verantwoord kan worden uitgevoerd. Hierbij is een veertiental deelvragen geformuleerd (zie bijlage 1).
Deze vragen zijn onder te verdelen in vijf groepen, te weten vragen over:

a) het effect, zijnde het tegenhouden;
b) de opsporingsindicaties, de intelligence (politie-informatie), het frustreren van lopende onderzoeken*
c) de capaciteit bij politie en openbaar ministerie;
d) de database, het beheer, de beveiliging, het wettelijk kader en de zekerheid van hits;
e) de (structurele) samenwerking met private partijen en de mogelijke verbreding naar andere hostingbedrijven.

* Hoewel de pilot niet was gericht op de opsporing, is toch een aantal deelvragen op dit vlak aan de pilot meegegeven, die als mogelijke "bijvangst" ook zijn opgenomen. Zie ook paragraaf 4.3.

Hieronder worden kort de resultaten benoemd.

3.2. Tegenhouden en de opsporingsindicaties

Er zijn tijdens de pilot geen hits waargenomen. Er zijn dus geen uploads van kinderporno tegengehouden. Om dezelfde reden kon er geen opsporingsindicatie of politie-informatie als bijvangst worden gemeld.
Er zijn dus ook geen IP-adressen doorgezonden van de klant naar het meldpunt Cybercrime. Indien er hits waren geweest, dan was dat ook niet gebeurd omdat dit extra technische voorzieningen vergt bij de klant, waarvan de wenselijkheid bij de klant discussie zou oproepen (zie paragraaf 3.4). Bij klanten is dit onderwerp ook niet aan de orde gesteld.
De optie om bij een hit direct een lijst te maken van andere uploads in dezelfde serie, omdat het mogelijk om een pakket zou gaan, is zodoende ook niet aan de orde geweest. Deze optie is tijdens de pilot, los van de technische vragen, overigens verlaten omdat de politie niet over de vereiste bevoegdheden beschikt.

3.3. Capaciteit bij politie en openbaar ministerie

Er is geen beroep gedaan op uitvoerend werk van politie en openbaar ministerie. Wel heeft de politie deelgenomen aan de Projectgroep en aan werkoverleg.

3.4. Database en matching

Er hebben zich geen problemen voorgedaan op het gebied van het beheer en de beveiliging van de hashcode database. Op verzoek heeft FOX-IT een beveiligingsrapport opgesteld (zie bijlage 2).
Eventuele "hits" zouden direct en zonder tussenkomst van bedrijfspersoneel naar het Meldpunt Cybercrime (MCC) worden gezonden. Er is geen aanleiding vastgesteld om het wettelijk kader aan te passen.
Voorzien was om bij een "hit" automatisch een lijst te laten generen met alle uploads vanaf het betreffende IP-adres, vanwege de mogelijkheid dat het om een pakket kinderporno zou kunnen gaan. Juridisch onderzoek in de pilot heeft uitgewezen dat een automatisme in deze niet aan de orde is. Indien de politie naar aanleiding van een melding van kinderporno via dit systeem nadere informatie wil inwinnen, dan zijn daarvoor de normale middelen van Strafvordering beschikbaar.
Gebleken is dat technische uitvoeringsproblemen om de matching tot stand te brengen aanzienlijk groter waren dan voorzien. Ook kostte de beveiligde tussenstap van de matching van de upload met de database meer tijd dan verwacht. Bovendien is bij elke klant die het filter zou willen benutten een aanpassing van de eigen software van die klant vereist, waarbij het niet gaat om standaardpakketten. Dit is voor klanten bezwaarlijk.

3.5. Publiek-private samenwerking

De verhouding tussen de publieke partij (politie) en de private partijen heeft geen bijzondere problemen opgeleverd. De private partijen worden niet betrokken bij opsporingshandelingen noch bij het beoordelen van kinderporno.
Bij een van de private partners viel de pilot samen met turbulente externe omstandigheden die veel tijd opeisten, die niet aan de pilot kon worden besteed. Daarnaast bleken er hiaten in de samenwerking tussen de private partijen onderling, waardoor de technische problemen laat werden gesignaleerd en niet snel konden worden opgelost. Sterkere procesbewaking van het project als geheel zou hebben bijgedragen tot een betere samenwerking tussen alle betrokken partijen.
Zodoende bereikte de pilot in april 2012 de status die was voorzien voor september 2011.

4. Nabeschouwing

4.1. Inleiding

De pilot heeft een aantal belangrijke ervaringen en inzichten opgeleverd. In deze nabeschouwing wordt dieper ingegaan op enkele belangrijke aspecten van de voorbereiding en de projectsturing en wordt gekomen tot een weging van de resultaten.

4.2. Voorbereiding en opzet van het project

In de voorbereiding van de pilot zijn vanuit de politie en het openbaar ministerie vele vragen en bezwaren opgeworpen. Dat duidde op zorgvuldigheid maar leidde ook tot aanzienlijke vertraging (het idee is in 2008 aangereikt en de pilot ging medio 2011 van start). Deels werden vragen mede gevoed door onvoldoende kennis van- en beeld bij het internet en de bijpassende technieken. Door de focus op politiële en juridische vraagstukken is in de voorbereiding onvoldoende aandacht gegeven aan de technische en organisatorische vraagstukken die de feitelijke uitvoering binnen de ICT-omgeving zouden oproepen. Deze werden verondersteld geregeld te zijn door LeaseWeb en FOX-IT, hetgeen tijdens de pilot anders bleek te liggen.
In 2010 is nadrukkelijk overwogen om met één private partner te werken, die verantwoordelijk zou zijn voor "daarachter" functionerende andere partners. Uiteindelijk is gekozen voor een overeenkomst met twee partners omwille van de binding en de greep op het project. In de opzet van het project had vervolgens extra aandacht moeten worden gegeven aan de projectsturing binnen de private kring.
Daarnaast bleek het gevreesde capaciteitsgebrek zich niet bij de politie, maar bij een van de private partners voor te doen. Dit was vooraf niet als risico aangeduid, wellicht omdat het initiatief vanuit het bedrijf kwam.
Advies: zorg voor een risico-inventarisatie over de volledige reikwijdte van het project.

4.3. Barrièremodel

De pilot was een invulling van het barrièremodel. Hoewel het werken met een barrièremodel al een aantal jaren binnen politie en justitie bekend is, blijkt het in de praktijk niet eenvoudig om de focus daarop te houden. De verleiding om ook reactief gericht te gaan werken blijft aanwezig. Het denken verschuift bij (nieuw) betrokken politie- en justitiepersoneel steeds weer richting opsporing (wat kunnen we ermee, wat moeten we ermee?). Dit is gedurende de gehele

voorbereiding waarneembaar geweest, reden om uiteindelijk toch een aantal aspecten van opsporing en intelligence in de vraagstelling mee te nemen. Ook tijdens het project bleef de verleiding aanwezig, wellicht gestimuleerd door de genoemde vraagstellingen. Door deze stelselmatige verschuiving of verbreding van de aandacht gingen de verwachtingen binnen de kring van projectmedewerkers vanzelf uiteen lopen. Dit vroeg om voortdurend bijsturen door de projectleider.
Advies: zie erop toe dat de verwachtingen bij het werken met een barrièremodel beperkt blijven tot de barrière die wordt beoogd.

4.4. PROJECTSTURING

De sturing op het project was opgedragen aan een projectleider van politiezijde. Dit lag voor de hand gezien de politiële en strafrechtelijke complicaties die werden voorzien. De projectleider had echter weinig zicht op de technische vraagstukken. Storingen in de voortgang werden door de projectleider pas gesignaleerd nadat de private partners zelf deze hadden gemeld. Door misverstanden tussen de private partners en gebrek aan overzicht bij de projectleider heeft het enige tijd geduurd voordat ontdekt werd dat de opzet weliswaar was gestart maar niet functioneerde. Bovendien lag de focus binnen een van de bedrijven inmiddels op andere thema's. Dit is niet onbegrijpelijk, gezien de economische ontwikkelingen sinds 2008 toen het idee voor de pilot werd aangereikt. Hoewel beide private partijen vrij heldere deelverantwoordelijkheden hadden, was een eenduidige projectleiding aan de private resp. technische kant wenselijk geweest.
De voortgang is hierdoor onvoldoende beheerst. Overigens is binnen de projectgroep collegiaal samenwerkt.
Bij het budgetbeheer hebben zich geen bijzonderheden voorgedaan.
Advies: kom bij dit type projecten tot een projectleiding die greep heeft op het geheel; te denken valt aan een algemeen projectleider vanuit de politie en een technisch projectleider vanuit het bedrijf.

4.5. BEVEILIGING TEGEN ONGEWENSTE UPLOAD

De formule is gebaseerd op de vooronderstelling dat bedrijven erin geïnteresseerd zijn om een uploadfilter tegen kinderporno aan hun uploadstroom te koppelen. Voor de pilot zijn door Leaseweb meerdere klanten benaderd. Uiteindelijk heeft één klant deelgenomen. Deze klant maakte al gebruik van een soortgelijke dienst op basis van de database van het Zweedse Netclean. Het is niet uitgesloten dat deze partij om die reden door uploaders wordt gemeden.

De vraag of er ja dan neen hits zijn is voor de klant wellicht van minder belang. Het gaat de klant immers om de inspanning upload van kinderporno op zijn sites te voorkomen en het maatschappelijk effect dat daarvan uit gaat (het tonen van maatschappelijk verantwoord ondernemen en preventie van ongewenste uploads). Indien er bij een klant hits zouden zijn, waarop actie wordt ondernomen, dan zal die klant gaandeweg geen hits meer ervaren.
Nadelig zijn de vertraging in de upload, die toeneemt naarmate de database groeit en het gegeven dat de eigen programmatuur van de klant moet worden aangepast teneinde de politie te voorzien van gegevens van de uploader (metagegevens). Dit knaagt aan de voorwaarde voor verspreiding van het filter, nl. dat de klant zo min mogelijk hinder ervaart.
Tot slot zijn er de meerkosten, die in de pilot door de overheid zijn betaald, maar die in een structurele benadering door de bedrijven zelf zullen moeten worden gedragen. Het is moeilijk te overzien hoeveel bedrijven hierop in zullen stappen.
Advies: Indien er bedrijven zijn die zich op deze wijze willen beschermen is er geen bezwaar tegen om daaraan vanuit de politie medewerking te verlenen, onder door de politie te stellen condities.

4.6. Tegenhouden of opsporen van kinderporno

Als het gaat om de bijdrage van de formule aan het tegenhouden van kinderporno in brede zin, dan moeten de beperkingen goed onder ogen worden gezien. Er zijn vele mogelijkheden om materiaal op het World Wide Web te brengen en het aantal bedrijven dat zich zal (willen) beveiligen zal niet meer zijn dan een fractie. Daarnaast is het internet een bredere infrastructuur dan alleen het World Wide Web waarop het uploadfilter betrekking heeft. Verspreiders van kinderporno maken ook gebruik van andere mogelijkheden. De bijdrage van uploadfilters aan het tegenhouden van kinderporno als fenomeen is zodoende te verwaarlozen.
De bijdrage van uploadfilters aan de opsporing of aan de politie-informatie – in het project beperkt meegenomen als mogelijke bijvangst – kan in individuele gevallen betekenis hebben. Als systeemkeuze ligt het niet voor de hand omdat andere middelen krachtiger zijn. Begrijpelijk, want een uploadfilter is ook niet voor opsporing of politie-informatie bedoeld.
Advies: het uploadfilter is niet bedoeld voor versterking van de opsporing of de intelligence en kan daarin ook geen functie van betekenis vervullen; vanuit de optiek van opsporing is verdere ontwikkeling daarom niet zinvol.

4.7. Slotconclusie

Het inzetten van een uploadfilter bij bedrijven die dat wensen is een vorm van beveiliging van de websites van die bedrijven, die daarvoor zelf organisatorisch, technisch en financieel

verantwoordelijk zijn. Binnen de pilot is een werkwijze onderzocht die, na enige doorontwikkeling, zou kunnen functioneren. Gezien de nuttige doelstelling daarvan kan de politie die beveiliging ondersteunen door, onder condities, hashdatabases in te zetten. Deze bijdrage van de politie kan worden vergeleken met de ondersteuning van andere vormen van bedrijfs(terrein)beveiliging.
Het op deze wijze filteren van uploads levert, gezien de open structuur van het internet, geen bijdrage van betekenis aan het tegenhouden van de verspreiding van kinderporno, noch aan het opsporen of aan de politie-informatie.
Vanuit de politie bezien is de pilot hiermee afgerond en is een eventueel vervolg aan het bedrijfsleven.

Bijlage 1: de vragen

a) In welke mate draagt de werkwijze bij aan het tegenhouden van kinderporno?
b) Wat levert de samenwerking op in termen van intelligence, waaronder over criminele samenwerkingsverbanden?
c) Hoe kan de politie-hashcodedatabase met optimale integriteit wordt beheerd?
d) In hoeverre is het beveiligingsniveau 'politie zeer vertrouwelijk' afdoende en in hoeverre is het nuttig of zelfs noodzakelijk om het niveau 'staatsgeheim' te bereiken?
e) Hoe kan voldoende in de vereiste beveiliging van de politie-hashcodedatabase worden voorzien?
f) In hoeverre geven de gematchte hashcodes 100% zekerheid over de aard van het materiaal, met name bij positieve herkenning?
g) Hoe kan optimaal worden omgegaan met de verificatie van 'hits'? Is verificatie door civiele personen met vrijstelling mogelijk?
h) In hoeverre levert de werkwijze opsporingsindicaties en wat kan daarmee gedaan worden (regionaal, BRT's, internationaal)?
i) Zijn er nadere wettelijke maatregelen nodig voor het delen van de informatie en zo ja welke?
j) Op welke manier is het mogelijk om private partijen binnen de (nieuwe) wetgeving bij het gebruik van een hashcodebase te betrekken?
k) Hoe ziet een werkende (bilaterale) overeenkomst er uit, die als grondslag kan dienen voor een structurele afspraak tussen een politieorganisatie en een internetbedrijf?
l) Op welke wijze zou de formule, bij succes, kunnen worden verbreed naar andere hostingbedrijven?
m) Welke structurele inspanningen voor politie en openbaar ministerie brengt de werkwijze met zich mee en wat betekent dit voor de inzet van beschikbare capaciteit op het gebied van de kinderporno?
n) Indien lopende onderzoeken worden gefrustreerd, hoe kan dat worden voorkomen?

Bijlage 2: beveiligingsrapport

Informatie van FOX-IT over de veiligheid en integriteit ten aanzien van de politie hashdatabase

Informatie betreffende de politie hashdatabase

De originele database [redacted]

Veiligheidsmaatregels in deze procedure:

- De gebruikte [redacted]
- Door over het [redacted]
- Om tijdens [redacted]

Informatie betreffende de afgeleide van de [redacted]

Wanneer er een [redacted]

De [redacted]

[redacted] Veiligheidsmaatregels in deze procedure:

- Een [redacted]
- Alle [redacted]
- [redacted]
- Op de [redacted]

0-0-0-0-0