Stichting Digitale
Infrastructuur Nederland

Tweede kamer commissie voor Veiligheid en Justitie

Betreft: rondetafelgesprek "Toename Kinderporno in Nederland" d.d. 28 juni 2017

Stichting Digitale Infrastructuur Nederland (DINL) is de spreekbuis van Nederlandse aanbieders van digitale infrastructuur. Ook DINL ziet de toename van online Kinderporno[1] in Nederland als een serieus probleem en wil haar bijdragen leveren aan de bestrijding. Daartoe moet Justitie het EOKM (Expertise centrum online kindermisbruik) ondersteunen en moet steviger ingezet worden op samenwerking met de sector.

Waarom is er zoveel KP / CSAM[2] in Nederland

De aanwezigheid van relatief veel KP in Nederland heeft te maken met de goede digitale infrastructuur.

1. Snelle en goede internationale verbindingen maken het up- en downloaden van alle soorten van beeldmateriaal mogelijk en makkelijk. Dat geldt dus ook voor KP
2. Nederland heeft een omvangrijke en wereldwijd opererende hosting sector: aanbod van webruimte voor content en toepassingen. Sommigen leveren hun diensten via wederverkopers in andere landen. Die werken vaak geautomatiseerd / met creditcards waardoor de klanten en gebruikers in die landen vaak moeilijk of niet te traceren vallen en dus gemakkelijk actief kunnen blijven.
3. Door de grote aantallen servers in Nederland zijn altijd wel ergens onbeveiligde upload mogelijkheden te vinden die buiten het zicht van de provider kunnen worden misbruikt voor KP (of andere onrechtmatige content).

Verder gaat het vaak om oude beelden die "dankzij" de goede upload mogelijkheden steeds opnieuw opduiken en meerdere keren meetellen. Ook moet worden overwogen dat verreweg de meeste meldingen leiden tot een snelle verwijdering. Maar die snel verwijderde beelden tellen wel mee in de statistieken. En verder is er ook sprake is van verspreiding van KP op het zogenaamde dark-web. Dat speelt zich grotendeels af buiten het zicht van het EOKM en justitie. Door het internationale karakter is de pakkans voor de "uploaders" gering. Maar het is de vraag wat justitie hier kan doen. Immers: het opstellen van een vordering, beoordeling door een rechter, aanschrijven van een hoster, of opstellen van internationale rechtshulpverzoeken is een traag proces. Tegen de tijd dat de vordering er is, is de KP vaak al weer weg. Zo'n aanpak is met tienduizenden meldingen jaarlijks niet werkbaar en niet effectief. DINL vindt daarom dat justitie zich zou moeten richten op opsporing van daders en dat bestrijding van online KP het beste kan worden gedaan door het EOKM en de sector.

Waarom kunnen providers KP niet voorkomen

Internet Service providers waaronder hosting bedrijven hebben een neutrale, faciliterende rol. Dat is in 2001 vastgelegd in het Europese e-commerce directive. Die neutrale rol is essentieel voor een open en vrij Internet. Het voorkomt dat providers anders continue de gangen van hun klanten na zouden moeten gaan. Dat is overigens ook fysiek onmogelijk. Want hoe ga je met de enorme data volumes om, hoe onderscheid je als provider goed van slecht, en techniek die dat betrouwbaar kan doen bestaat niet. Daarnaast kunnen providers klantdata niet zomaar bekijken,

---

[1] http://nos.nl/artikel/2163585-kinderporno-op-internet-meer-meldingen-meer-materiaal.html
[2] In de internationale context wordt gesproken over CSAM (Child Sexual Abuse Material) te hanteren.

Stichting Digitale Infrastructuur Nederland
Overgoo 13 / Postbus 262
2260 AG Leidschendam

T: +31707621070
E: info@dinl.nl

vanwege contractuele geheimhoudingsbepalingen. En in het geval van KP omdat het bekijken ervan strafbaar is.

Wat doet de sector

De sector werkt samen met partijen om het probleem aan te pakken. Er is een goede werkrelatie met het EOKM dat vertrouwd wordt door providers. Ook wordt goed samengewerkt met politie en het OM. Verder steunen enkele bedrijven en organisaties uit de sector het EOKM financieel, en helpen vrijwilligers uit de sector hen met ondersteunende software.
Voor het snel verwijderen van KP hanteren providers de gedragscode NTD, “Notice en Takedown”. De NTD voorziet in een proces waarbij providers, na een notice (melding van KP of andere onrechtmatigheid) onmiddellijk actie moet nemen: beoordeling, hoor en wederhoor en dan verwijderen. In het geval van een KP melding door het EOKM is het evident dat het onrechtmatig is en zal vrijwel iedereen het na een melding meteen verwijderen.
De NTD procedure werkt op zich goed, is snel en efficiënt. Zeker bij de hosters die aangesloten zijn bij een brancheorganisatie (DHPA en ISPConnect). De DHPA stelt de strikte naleving van de NTD verplicht voor haar deelnemers.
Als sector raden we providers die langs een andere weg KP meldingen ontvangen, aan om deze door te sturen naar het EOKM. Om te voorkomen dat hun medewerkers het beeldmateriaal moeten bekijken. En ook is dat beter voor de informatievoorziening naar justitie.

Wat vind de sector dat er moet gebeuren

De providers vinden dat het probleem moet worden aangepakt door de huidige werkwijze te versterken.

1. Ten eerste moet het EOKM financieel door de overheid worden ondersteund. Dat is de meest efficiënte manier om het probleem aan te pakken. Het EOKM doet uitstekend en belangrijk werk. En neemt feitelijk justitie werk uit handen want KP is strafbaar. Het EOKM is echter onderbemand en heeft veel te weinig financiële armslag. Het moet kunnen beschikken over meer mensen en over software die beelden kan voor-analyseren.
2. Ten tweede pleiten we voor het inrichten van een landelijk netwerk voor het versturen en ontvangen van meldingen. Ook kleine providers kunnen dan aansluiten en weten dat de bronnen en de meldingen authentiek en urgent zijn. Als justitie hier het voortouw in neemt kan politie de meldingen in de gaten houden om zo de daders op te kunnen sporen.
3. Ten derde moet justitie voor een beter inzicht niet (alleen) de aantallen, maar vooral de opvolging van de meldingen gaan meetellen in de statistieken. KP die lang blijft staan is erger dan oude beelden die direct verwijderd worden. TuDelft heeft zo’n meetmethode ontwikkeld. In combinatie met het landelijk netwerk vallen dan de providers meer op die de NTD niet (goed) hanteren, en die kunnen dan worden aangesproken of aangepakt.
4. Als laatste moet steviger worden ingezet op de Internationale samenwerking.

Samenvattend

Behoud van de neutrale rol van providers is essentieel. Maar dat ontslaat hen niet van de verantwoordelijkheid om snel te reageren als ze een NTD melding krijgen. De meesten doen dat ook. Want ze willen geen KP en cybercrime in hun netwerken of op hun servers.
Met meer middelen voor het EOKM, betere statistieken en een nationaal en internationaal netwerk voor meldingen kunnen we dit probleem samen een stuk kleiner maken.

DINL, M. Steltman, Juni 2017

Stichting Digitale Infrastructuur Nederland
Overgoo 13 / Postbus 262
2260 AG Leidschendam

T: +31707621070
E: info@dinl.nl