Stappenplan Gedragscode Abusebestrijding

versie februari 2021

Implementatie van de gedragscode abusebestrijding lijkt misschien veel werk, maar dat valt in de praktijk wel mee. Registrars, Autonomous Systems, Hosting/Cloud providers en datacenters die onderstaand stappenplan gevolgd hebben, voldoen aan de gedragscode.

Generiek
Beleid

- Maak op je site en naar je klanten duidelijk dat je deze gedragscode en de gedragscode NTD[1] hanteert.
- Maak een beleidsdocument voor je medewerkers die belast zijn met het opvolgen van abuse meldingen en incidenten.
- Besluit of je voor de implementatie de best practices van de M3AAWG[2] (vol met praktische tips) wilt gebruiken, of dat je een eigen invulling wilt geven.
- Maak een abuse policy voor je afnemers. Verbind in die policy consequenties aan herhaalde of substantiële overtredingen en geef jezelf het recht om zaken in quarantaine te plaatsen of af te sluiten.
- Verplicht je afnemers om bereikbaar te zijn voor (jouw) abuse meldingen, accepteer niet dat ze onbereikbaar zijn, of traag of niet reageren op abuse meldingen die je naar hen verstuurt.
- Verplicht je afnemers om geconstateerde kwetsbaarheden of lekken te (laten) patchen en abuse te verwijderen.

Informatie

- Je zorgt voor in ieder geval een abuse@ mailadres op je hoofddomein. Bij voorkeur kunnen abuse meldingen ook telefonisch of via chat bij jou geplaatst worden.
- Zorg dat je zelf goed bereikbaar bent voor abuse meldingen. Ook in het weekeind: veel abuse vindt juist plaats bij hosters waarvan"the bad guys" weten dat ze dan niet zo goed bereikbaar zijn.

[1] `https://noticeandtakedowncode.nl/`

[2] `https://www.m3aawg.org/sites/default/files/document/M3AAWG_Hosting_Abuse_BCPs-2015-03.pdf`

Meldingen

- Zorg dat abuse meldingen jou eenvoudig kunnen bereiken, verwijder red tape en ellenlange formulieren. Je leest en verwerkt meldingen dagelijks, en geeft altijd opvolging aan meldingen.
- Stel vast welke flaggers je als trusted beschouwt. Je kunt hierbij denken aan het Meldpunt Kinderporno (EOKM[3], SIDN[4] via Netcraft[5] en het Landelijk Meldpunt Internet Oplichting[6]. Bij meldingen van die trusted flaggers is geen interne beoordeling van de melding nodig en verwijder/blokkeer je direct de content of laat je dat doen.
- Instrueer je medewerkers dat ze meldingen over kinderporno die niet via het EOKM binnen zijn gekomen doorsturen naar het EOKM ter beoordeling. Zo voorkom je dat zij die melding moeten beoordelen en het materiaal zouden moeten bekijken, wat zelfs strafbaar is.
- Als abuse meldingen echt niet door jou kunnen worden verwerkt, scheep de melder niet af maar zet de melding door naar de juiste ontvanger als je weet of kunt weten wie het moet zijn; Of geef de verzender informatie die het voor hen makkelijk maakt de juiste target te vinden. Jij weet hoe het allemaal werkt , de verzender vaak niet.

Extra stappen Registrar

- Zorg voor publicatie van je abuse-contactgegevens in de WHOIS van de TLD's die er ondersteuning voor bieden.

Extra stappen Autonomous System

- Zorg voor publicatie van je abuse-contactgegevens in de RIPE WHOIS.
- Implementeer de maatregelen zoals beschreven in het routing security manifest MANRS[7].
- Installeer AbuseIO of vergelijkbare software voor het ontvangen en verwerken van abuse meldingen, in elk geval voor die van het EOKM en bij voorkeur voor de informatie van/via NBIP.
- Sluit je aan bij NBIP's CleanNetworks[8] portal. Via deze portal krijg je directe informatie over abuse in je netwerk. De portal toont hoe schoon

[3] `https://www.eokm.nl/`
[4] `https://www.sidn.nl/`
[5] `https://www.netcraft.com/`
[6] `https://www.politie.nl/`
[7] `https://www.manrs.org/`
[8] `https://www.cleannetworks.net/`

jouw netwerk is vergeleken met je peers en je ontvangt er abuse meldingen, waarvan sommige niet via bestaande feeds te verkrijgen zijn. Of zorg er zelf voor dat je je abbonneert op diverse abuse feeds en benchmarking van je abuse bestrijding performance.