Gedragscode abusebestrijding voor operators van digitale infrastructuur

Versie 1.1 september 2018

De samenleving moet erop kunnen vertrouwen dat operators en aanbieders van digitale infrastructuur zich inspannen om gebruik van hun faciliteiten voor onrechtmatige activiteiten te voorkomen en te bestrijden. Daartoe hanteren zulke operators en/of aanbieders deze gedragscode.

Onder digitale infrastructuur wordt verstaan: op internet aangesloten faciliteiten die digitale online diensten faciliteren, in brede zin, waaronder datacenters, hosting en cloud platforms, domeinen, netwerken (AS), internet access, platforms, file shares; en al datgene wat onder de Europese e-commerce richtlijn als een mere-conduit activiteit wordt beschouwd.

Onder abuse wordt verstaan: het misbruik van op internet aangesloten digitale infrastructuur in brede zin; zoals het versturen van spam of phishing mails, het verspreiden van malware, DDoS, runnen van een botnet, opslaan en verspreiden van CAM of ander onrechtmatig materiaal, runnen van een frauduleuze website, et cetera. Abuse omvat in elk geval onmiskenbaar onrechtmatige activiteiten en voorts datgene wat door de betreffende operator als ongewenst wordt beschouwd.

Algemeen

Operators van digitale infrastructuur:

1. Zijn in beginsel niet aansprakelijk noch verantwoordelijk voor de activiteiten van de afnemers van hun diensten.[1] Dat neemt niet weg dat zij al wat in hun mogelijkheden ligt zullen doen om abuse te bestrijden.
2. Hanteren daartoe deze gedragscode, zullen dat duidelijk kenbaar maken op hun site c.q. communiceren daarover naar hun afnemers en medewerkers.
3. Hanteren de gedragscode NTD en implementeren de bijbehorende processen in hun organisatie.
4. Hanteren een acceptable use policy voor hun afnemers en/of gebruikers, waarin wordt vastgelegd wat van hen wordt verwacht indien abuse bij hun activiteiten wordt aangetoond.
5. Verplichten zich om bij langdurig, substantieel of herhaald overtreden van de acceptable use policy door hun afnemers de dienstverlening te schorsen, diensten in quarantaine te plaatsen of de contracten met zulke klanten te beindigen.
6. Zullen bij die vormen van abuse waarbij de operator kennis heeft genomen van de aard van het abuse en het voortduren ervan ernstige schade aan individuen oplevert, direct maatregelen nemen om verdere schade te voorkomen of te beperken. CAM, phishing, malafide webshops en malware verspreiding worden in ieder geval geschaard onder deze vormen van abuse.
7. Zorgen voor correcte contactgegevens van hun klanten zodat bij abuse of het vermoeden ervan er direct contact gelegd kan worden met de afnemer.
8. Zijn pro-actief naar hun afnemers of gebruikers; dat wil zeggen ze nemen actie als zij in kennis worden gesteld van abuse of kwetsbaarheden in hun diensten.
9. Hanteren (een) industry best practice(s) voor abuse bestrijding die past bij hun activiteiten, zoals de gedragscode van de M3AAWG en maken dit (deze) kenbaar naar hun afnemers.

[1] In elk geval indien zij op grond van de Europese E-commerce directive (directive 2000/31/EC article 14) aangemerkt worden als intermediaries (mere conduit).

10. Publiceren op hun website en in de ter zake doende whois registraties contactgegevens voor het melden van abuse.

11. Accepteren in redelijkheid alle abuse meldingen die ze ontvangen via geautomatiseerde systemen en door personen opgestelde individuele meldingen.

12. Doen al wat redelijkerwijs binnen hun mogelijkheden ligt om informatie te verkrijgen over kwetsbaarheden en abuse in hun netwerken en op hun voorzieningen. Dat doen zij door zich in ieder geval te abonneren op abuse feeds of de AbuseHUB, het aansluiten op een nationale CERT en het raadplegen van- of aansluiten bij andere informatiebronnen die daarover inzicht geven.

13. Doen al wat redelijkerwijs binnen hun mogelijkheden ligt om de effecten van abuse binnen hun netwerken te verminderen voor andere gebruikers van het internet. Dat doen zij door in ieder geval het egress filteren van gespoofed verkeer en het toepassen van de maatregelen in de gedragscode MANRS.

14. Stellen zich op de hoogte van hun performance op het gebied van abuse bestrijding door raadplegen van de daartoe beschikbare bronnen.

15. Voeren beleid om hun performance op het gebied van abuse bestrijding continue te verbeteren.

Overtredingen

16. Gebruikers van deze code of conduct melden vermeend onterecht gebruik van deze gedragscode aan (en van de) brancheorganisaties die deze gedragscode onderschrijven, aan het NBIP, of aan het platform internet veiligheid (PIV) van het ECP.

17. Het NBIP, de betreffende brancheorganisatie c.q. het PIV zal de betreffende organisatie verzoeken om een toelichting. Indien naar het oordeel van bovenstaande organisatie(s) het antwoord niet volstaat, zal de betreffende partij worden verzocht zich te onthouden van het vermelden van het gebruik van de gedragscode. In dat geval zal melding worden gedaan van de situatie bij het PIV, bij de ACM en de ministeries van justitie en economische zaken.

18. Deelnemers aan deze gedragscode zullen zich indien mogelijk onthouden van zakelijke relaties met organisaties waarvan bekend is dat ze evident handelen in strijd met deze gedragscode, c.q. waarvan in redelijkheid kan worden gesteld dat ze onrechtmatigheid opzettelijk faciliteren.

Dit document

19. Deze code of conduct zal periodiek worden herzien, op basis van feedback en ervaringen van de deelnemers aan deze gedragscode.

Initiatiefnemers: DHPA, DINL, ECP, ISPConnect, Ministerie van Economische Zaken en Klimaat, NBIP, TUDelft, Vereniging van Registrars.

April 2018