

# Spam vaak verstuurd door criminelen

Sinds 2004 geldt in Nederland een verbod op spam aan particulieren. Op 1 oktober wordt dat verbod uitgebreid naar bedrijven. Helaas trekken veel grote, vaak criminele spamclubs zich er niets van aan.

Door **Ayolt de Groot**

In de redactie-inboxen van de *Volkskrant* stromen ze binnen, de e-mails waarin pr-bureaus vragen of zij de krant vanaf 1 oktober hun persberichten nog mogen toezenden. Op die datum wordt in Nederland het spamverbod uitgebreid, waarna het niet langer is toegestaan ongevraagd mails naar bedrijven te sturen. De pr-bureaus riskeren een boete van maximaal 450 duizend euro, als zij de relaties op hun mailinglijsten niet expliciet toestemming vragen.

Het is een bijeffect van de aanpassing van de Telecomwet, waarmee staatssecretaris Heemskerk van Economische Zaken nu ook bedrijven tegen spam wil beschermen.

Het ongevraagd versturen van berichten naar particulieren is al sinds 2004 verboden. In de twee jaar na de invoering van het verbod op spam naar 'natuurlijke personen' daalde de ongevraagde mail van Nederlandse komaf met 85 procent. Een indrukwekkend resultaat, waarvoor telecomautoriteit Opta een pluim kreeg van de Europese Commissie.

Toch bestond in augustus in Nederland nog steeds 86,3 procent van alle mail uit spam, aldus cijfers van internetbeveiliging Message Labs. Een maand eerder lag dat percentage zelfs op 95,7 procent.

De treurig stemmende boodschap is dat ook het algehele spamverbod dat op 1 oktober van kracht wordt, daaraan weinig zal veranderen.

'Het is een druppel op een gloeiende plaat', zegt Gruus van Woerkom van hosting- en emailprovider Byte, die aan ongeveer zeven-duizend bedrijven internetonderdak biedt. Bedrijven die massamailings de deur uit doen naar particulieren of ondernemingen vormen verreweg de kleinste categorie ongewenste mail, legt hij uit. 'Dan heb je het over ongeveer 1 en 5 procent van alle spam, waarvan met het verbod maar een fractie, namelijk het deel van Nederlandse

komaf, wordt aangepakt.'

Er zijn nog twee hardnekkiger categorieën van spam, zegt Van Woerkom. Zo is er de spam die wordt verstuurd via zogenaemde *bulletproof-hosts*: 'Dat zijn servers die doelbewust aan spammers beschikbaar worden gesteld in landen waar tegen hen niet wordt opgetreden, zoals China. Daar is eigenlijk niets tegen te doen.'

De derde en grootste categorie spam bestaat uit via zogeheten botnets verstuurd massamails: netwerken van vele duizenden thuiscomputers die zijn geïnfecteerd met kwaadaardige software, en op afstand worden bestuurd door robotcomputers. Ongeveer 85 procent van alle spam wordt verstuurd via botnets, die zo de kern van het probleem vormen.

Van Woerkom: 'Vaak wordt maar een klein beetje van de bandbreedte gebruikt voor het versturen van de spam. Op die manier hebben computergebruikers zoals jij en ik meestal niet eens in de gaten dat ze onderdeel zijn van een botnet.'

Achter de botnets, die duistere namen dragen als Cutwail en Donbot, gaan grote criminele organisaties schuil die hun netwerken verhuren aan bedrijven die spam versturen. Deze bedrijven kunnen bij de botnets 'zendtijd' inkopen, legt Paul Wood, spamanalist bij Message Labs, uit. De deals worden gemaakt in bijvoorbeeld chatrooms. 'Daarbij is het zaak eerst een vertrouwensband op te bouwen, omdat natuurlijk ook de autoriteiten die chatrooms weten te vinden.'

Voor de bedrijven is het spammen via botnets een goedkope manier van 'adverteren': volgens recent onderzoek van softwarebedrijf G Data lopen de tarieven voor een miljoen spamberichten uiteen van 250 tot 700 dollar.

Wood schat het aantal botnets dat ertoe doet op 15 à 20, waarbij de topvijf 50 tot 60 procent van de wereldwijd verstuurd spam uitmaakt. Ze zijn moeilijk te bestrijden, omdat de computers die er deel van uitmaken over de hele wereld verspreid zijn. De oorspronkelijke bron, de computer die het botnet aanstuurt, is daardoor lastig te achterhalen.

In november 2008 lukte dat wel, en werd de host achter het Srizbi-botnet afgesloten. Dit botnet met een capaciteit van 60 miljard spammails per dag was op dat moment verantwoordelijk voor ongeveer 50 procent van alle spam.

'Het spamniveau viel direct fors

terug', zegt Wood. 'Maar binnen een paar maanden had Srizbi zich weer hersteld.' De hackers hebben ervan geleerd. Wood: 'Sindsdien wedden ze niet meer op één paard,

en sturen ze de botnets aan vanaf meerdere computers.' Zo had het Cutwail-botnet, dat op 1 oktober 2009 in Letland de pas werd afgesneden, maar een paar uur nodig om zich te herstellen, in plaats van een paar maanden.

Een oplossing, voor zover die er is, ligt bij de internetaanbieder, meent Wood. Zij kunnen de 'zorkbi-computers' die onderdeel zijn van een botnet tijdelijk afsluiten, en de gebruiker informeren dat er kwaadaardige software op zijn computer is geïnstalleerd. Veertien Nederlandse internetproviders ondertekenden onlangs op initiatief van de Opta een convenant waarin zij zich aan deze aanpak committeren.

Maar hier speelt hetzelfde probleem als bij het spamverbod, zegt Niels Huijbregts van XS4ALL, een van de ondertekenaars van het convenant. De meerderheid van spam komt uit landen als Brazilië en China. Daar is vanuit Nederland niks tegen te beginnen. 'Daar zijn ze bezig iedereen op internet aan te sluiten, niet om zich zorgen te maken over ongewenste mail.'

De wetgeving over spam verschilt van land tot land, terwijl het bij uitstek een internationaal probleem is. Ook binnen de EU zijn er verschillen, omdat lidstaten vrij zijn naar eigen wensen vorm te geven aan de Europese richtlijnen.

Met het algehele spamverbod loopt Nederland voorop. Volgens Byte's Gruus van Woerkom levert dat voor Nederlandse bedrijven die niet massaal spammen, maar wel eens met legitieme bedoelingen een commerciële mailing versturen, een concurrentienadeel op. Zij verliezen een marketinginstrument dat buitenlandse bedrijven nog wel tot hun beschikking

hebben.

'Een interessant punt', meert spamanalist Wood. De Opta voorziet evenwel geen problemen: 'Het

is niet de bedoeling zakelijke mails te verbieden. We willen mails bestrijden die overlast veroorzaken. Wij meten dat af aan de hoeveel-

heid klachten die over een bepaald bedrijf binnenkomen. Op basis daarvan treden wij op', aldus een woordvoerder.



Jongeren mogen vrijblijvend gebruikmaken van MAC-computers in een grote MAC-winkel in New York.

Foto Guus Dubbelman / de Volkskrant

Bron: Groot, A. de (2009, 17 september). Spam vaak verstuurd door criminelen. *De Volkskrant*, p.8.