

Service provider worstelt met privacy e-mailgebruiker

13 december 2001

door: Hidde Koenraad

Mag van een internet-provider worden verwacht dat hij e-mail controleert op virussen? Hij is daar wel toe in staat. Volgens service providers is het filteren van e-mail echter een inbreuk op de privacy van de e-mail gebruiker. Toch is er, concludeert Hidde Koenraad, voor de provider een belangrijke rol weggelegd bij het voorkomen van grote schade.

Dat het wereldwijde web zeer kwetsbaar is en zich uitstekend leent voor allerlei onrechtmatige doeleinden is de afgelopen tijd duidelijker dan ooit. Het web blijkt bijvoorbeeld uitermate geschikt voor het verspreiden van illegale en schadelijke informatie, geheime communicatie tussen terroristen, het ongeoorloofd binnendringen in servers en databanken en het verspreiden van computervirussen. Vooral computervirussen kunnen in korte tijd zeer grote schade aanrichten bij veel internetgebruikers. Virussen als I love you, Melissa en meer recentelijk VBC/Loveletter en Sircam hebben wereldwijd samen voor miljarden guldens schade veroorzaakt. Veel van deze virussen worden tegenwoordig via [e-mail](#) verspreid door verzending tezamen met een besmet attachment. Door dit laatste document te openen wordt het virus actief. De virussen zijn vaak zo geprogrammeerd dat zij zichzelf geraffineerd kunnen reproduceren en verder verspreiden. Het anonieme karakter van het web in combinatie met slimme technische trucs maakt het traceren van de daders bovendien in veel gevallen ondoenlijk.

De vraag is nu of de internet-provider als aanbieder van een e-maildienst, voor het tegenhouden van dergelijke e-mailvirussen medeverantwoordelijk gehouden kan worden. Internet-providers zijn namelijk in staat de verspreiding van virussen te verhinderen dan wel te verminderen door de op hun servers aanwezige mailboxen en e-mails te screenen en/of te filteren op mogelijke virussen. De internet-provider kan immers, met speciale programmatuur, toegang krijgen tot de onder zijn beheer staande mailboxen. Indien een virus gevonden wordt, zou dit door de internet-provider vernietigd kunnen worden of hij zou preventieve berichten uit kunnen laten gaan naar zijn klanten.

De internet-provider is echter niet zonder meer aansprakelijkheid te houden voor de informatie die via zijn systemen loopt. Bovendien, en dit is ook een veel gehoord argument van internet-providers, is er bij het filteren van e-mailverkeer sprake van schending van de privacy van internetgebruikers. De vraag is echter of deze argumenten juridisch gezien in alle gevallen houdbaar zijn. Wellicht zou aan internet-providers een zorgplicht opgelegd kunnen worden om verdere verspreiding van 'geïnfecteerde' e-mails te voorkomen.

Artikel 13

In Nederland wordt aansprakelijkheid van de internet-provider voor de inhoud van e-mailberichten van anderen niet aanvaard, omdat het communicatiegeheim de provider verbiedt van privécommunicatie kennis te nemen. Van de verschillende typen internet-providers is de service provider, in tegenstelling tot de zogenaamde access provider, in staat de inhoud van de op zijn server aanwezige informatie in te zien, aan te passen of te vernietigen. Het filteren van e-mails zou volgens de service providers strijdig zijn met artikel 13 van de grondwet, waar naast het telefoon- en telegraafgeheim ook het briefgeheim is geregeld.

Het is echter nog onduidelijk of een e-mailbericht ook onder de bescherming van het huidige grondwetsartikel kan vallen. Ook de vraag of dit in de toekomst zal veranderen is nog onzeker, nu de aanpassing van artikel 13 aan modernere communicatiemiddelen nog op zich laat wachten. Op grond van de [telecommunicatiewet](#) is door de Tweede Kamer echter inmiddels al aanvaard dat e-mails onder de werking van deze wet te scharen zijn. In de telecommunicatiewet is onder andere bepaald dat aanbieders van openbare telecommunicatiediensten bij hun bedrijfsvoering het belang van de bescherming van het telegraaf-, telefoon- en briefgeheim in acht dienen te nemen. Service providers zijn als telecommunicatiediensten aan te merken en zodoende ook aan deze wet gebonden. Overigens dient opgemerkt te worden dat, mocht de wetgever besluiten de e-mail wél onder het communicatiegeheim van artikel 13 van de grondwet te laten vallen, dit niet per definitie betekent dat, onder bepaalde omstandigheden, van de inhoud van e-mail geen kennis genomen zou kunnen worden door de service provider.

Zo'n omstandigheid zou zich bijvoorbeeld kunnen voordoen indien de beschikbaarheid van diensten die de service provider levert, in het geding is. Een dergelijke situatie zou bij het actief zijn van een agressief computervirus zeer goed denkbaar zijn. Indien de service provider hiervan kennis draagt, dan wel goede redenen heeft om aan te nemen dat er een vernietigend virus op zijn server ronddwaalt, is hij jegens zijn klanten verplicht hier iets aan te doen.

Het screenen en/of filteren van mailboxen en e-mails is hiervoor, naast het geven van waarschuwingen, de geijkte weg. Indien de service provider immers niets zou ondernemen en hij dientengevolge zijn diensten niet meer kan leveren, kan hij hiervoor aansprakelijk zijn jegens de klanten die bijvoorbeeld geen gebruik meer kunnen maken van hun mailbox. Service providers zeggen echter, net als de overheid overigens, dat de verantwoordelijkheid voor virussen bij de individuele gebruikers dient te liggen. Het is echter de vraag of die stellingname tegenwoordig nog houdbaar is. De praktijk wijst uit dat de gemiddelde individuele gebruiker niet in staat is doeltreffende maatregelen te treffen om virussen te voorkomen. Zijn virusscanner herkent het nieuwe virus vaak niet eens.

Virussen kunnen, zoals is gebleken, dermate ingrijpende netwerkproblemen veroorzaken, waarbij dusdanig veel gebruikers betrokken zijn, dat de oplossing hiervoor op netwerkniveau dient te liggen. De service provider zou, als toegangverlener tot een netwerk, bij het tegengaan van onnodige schade een belangrijke rol kunnen vervullen.

Europese Verdrag

Een ander argument dat kan worden aangedragen tegen het filteren van e-mails kan gevonden worden in, het voor een ieder in Nederland geldende, artikel 8 van het Europese Verdrag tot Bescherming van de Rechten van de Mens. In dit artikel is de bescherming van de persoonlijke levenssfeer geregeld. Een ieder heeft recht op respect voor zijn privéleven en zijn correspondentie, zo stelt het artikel. De vraag is hoe screenen en/of filteren zich verhouden tot de in dit artikel gestelde normen. Uit de uitspraken van het Europese Hof kan worden afgeleid dat e-mail als zodanig voor bescherming in aanmerking zou kunnen komen.

Het tweede lid van dit artikel staat echter, onder omstandigheden, beperkingen van dit recht op de persoonlijke levenssfeer toe. Die omstandigheden kunnen gelegen zijn in, onder andere, de nationale veiligheid of het economisch welzijn van het land, het voorkomen van wanordelijkheden en strafbare feiten. De beperking van het privacyrecht moet, volgens dit artikel, bovendien voorzien zijn bij wet en 'noodzakelijk zijn in een democratische samenleving'. Dit laatste criterium houdt onder meer in dat er sprake moet zijn van een dringende maatschappelijke behoefte voor de beperking, en dat voldaan is aan eisen van subsidiariteit en proportionaliteit. De vraag is of de overheid op grond van dit artikel een gedragscode zou kunnen opleggen aan service providers en welke instantie vervolgens bepaalt of een virus dusdanige grote gevaren met zich meebrengt dat tot een filteractie overgegaan dient te worden. Hiertoe zou bijvoorbeeld een onafhankelijk orgaan, waarin ook alle service providers vertegenwoordigd zijn, kunnen dienen. Het hete hangijzer van het filteren, de privacy van de internetgebruiker, zou zo ook beter gewaarborgd kunnen worden doordat er op deze wijze geen sprake zal zijn van willekeurige inbreuken op het communicatiegeheim door individuele service providers.

De service provider behoeft op deze manier ook niet de dure en tijdrovende plicht opgelegd te krijgen om voortdurend actief zijn servers te doorzoeken naar mogelijke virussen. Dit zou overigens met het in omloop zijn van veel zogenaamde 'hoaxen' (valse viruswaarschuwingen) ook een ondoenlijke opgave zijn.

Bovendien is in de e-commerce-richtlijn bepaald dat service providers geen algemene verplichting hebben om toezicht te houden op de informatie die zij doorgeven of opslaan, noch om actief naar feiten of omstandigheden die op onwettelijke activiteiten duiden, te gaan zoeken. Het doorzoeken van de servers zou overigens, als bijkomende maatregelen, ook nog naar tijd gelimiteerd kunnen worden.

Het steeds frequenter voorkomen van virussen vraagt aldus om een serieuze afweging tussen het recht op privacy enerzijds en de noodzaak tot het efficiënt tegengaan en bestrijden van hardnekkige computervirussen anderzijds. Mits met duidelijke, wettelijke waarborgen omkleed, kan voor de service providers, in geval van een grootschalige virusdreiging, een belangrijke rol zijn weggelegd bij het voorkomen van onnodig hoge schade. De service provider zou hiertoe een bepaalde (juridische) verantwoordelijkheid dienen te krijgen. De vraag blijft vooralsnog hoever deze verantwoordelijkheid dient te reiken.

Mr. H.J. Koenraad is advocaat bij SchutGrosheide Advocaten en Notarissen te Amsterdam en aldaar werkzaam in de praktijkgroep Technology, Media & Communications.