

## EEN SCHONE INBOX MET HET JUISTE SPAMFILTER

# Spamzuigers

De strijd tegen ongewenste e-mail woedt onverminderd voort. Voor het bedrijfsleven zijn er verschillende anti-spamoplossingen beschikbaar. Welke oplossing het meest geschikt is, is sterk afhankelijk van de e-mailinfrastructuur binnen je bedrijf. 'Voor elk wat wils' lijkt hier sterker dan ooit te gelden.



'Spam op recordhoogte' meldt een artikel op WINMAGPro.nl. Beveiligingsbedrijf Cleanport rapporteerde begin 2008 dat in het jaar 2007 gemiddeld negen van de tien e-mails spam betrof. Een samenvatting van dit rapport, met meer details, lees je op [winmagpro.nl/spamrapport](http://winmagpro.nl/spamrapport)

Op het gebied van anti-spambescherming heb je als ondernemer anno 2008 een drietal opties. Voor welke optie je uiteindelijk kiest, wordt sterk bepaald door het type organisatie en de gebruikte infrastructuur. Een organisatie die intensief gebruik maakt van mobiele apparaten of thuiswerkers, heeft andere beveiligingsbehoeften dan een bedrijf dat overwegend uit vaste werkstations bestaat. Er zijn primair drie opties te onderscheiden: bescherming van de lokale e-mailserver, hosted bescherming en lokale bescherming van de individuele werkstations. Steeds meer bedrijven maken gebruik van Microsoft Exchange Server, voor de afhandeling van hun e-mail. Fabrikanten van anti-spamoplossingen spelen slim op deze trend in en bieden steeds vaker oplossingen aan die specifiek zijn bedoeld voor een Windows Server-omgeving in combinatie met Microsoft Exchange Server. De door ons bekeken oplossingen zijn geschikt voor installatie op de meest gangbare server-versies (2000 en 2003), maar ook voor het relatief recente Windows Server 2008. In deze situatie wordt de anti-spamoplossing geïnstalleerd op de server waarop Exchange draait.

## Hosted

Een andere manier om de organisatie te beschermen, is door gebruik te maken van een zogeheten 'hosted' dienst. Hosted anti-spamoplossingen hebben in korte tijd aan populariteit gewonnen. Niet zo vreemd, wanneer we een blik werpen op de kenmerken van een dergelijke oplossing. Bij een hosted oplossing neemt de aanbieder van de hosted dienst een groot deel van het onderhoud en de configuratie van je over. Door de MX-records van het e-maildomein aan te passen, zorgt je ervoor dat de mail niet meer direct naar de e-mailserver wordt gestuurd, maar eerst naar de service van de hosted anti-spam-aanbieder. Je hebt hiervoor de medewerking van de provider van het domein nodig, of de mogelijkheid om de instelling via een self-service omgeving zelf aan te passen. De wijziging is meestal niet direct van kracht: reken op 24 tot 48 uur voordat de wijziging actief is. Het is dan ook aan te raden om de wijziging in het weekend of in de avonden uit te voeren. Op de servers



van deze aanbieder vindt vervolgens de controle van de berichten plaats. Goedgekeurde berichten worden doorgezet naar de mailbox van de gebruiker. Via een beveiligde webomgeving kun je de geblokkeerde e-mail opvragen en controleren of er geen legitieme mail is achtergehouden.

## Lokaal

Tot slot is er de lokale bescherming. Het gaat hier om oplossingen die op de lokale werkstations worden uitgevoerd. E-mail wordt hierbij direct na ontvangst onderzocht op spam en in een aparte map ondergebracht. Dit type oplossing leent zich bijvoorbeeld goed voor mobiele gebruikers met een laptop, die niet altijd met internet is verbonden. Met een lokale anti-spamoplossing ben je immers continu beschermd, zonder de afhankelijkheid van een online dienst.

Dennis Gandasoebata

## "Express herbals: gain an amazing 1 to 3 full inches!"

Spam is een verzamelnaam voor ongewenste berichten. Spam is ook bekend als Unsolicited Commercial E-mail en Unsolicited Bulk E-mail. Meestal wordt met de term ongewenste mail bedoeld, maar ook ongewenste reclameboodschappen op websites (onder andere fora) vallen onder spam. Spam is moeilijk te definiëren. Niet ieder initiatief van mensen of organisaties om contact te leggen is spam. Spam onderscheidt zich van andere

vormen van commerciële communicatie doordat een bericht wordt gestuurd aan een groep die zeer veel groter is dan de potentiële doelgroep. Omdat deze afbakening te maken heeft met de properties, zou je verwachten dat het moeilijk is om te bepalen of een bericht spam is of niet. Vanwege de enorme schaal waarop spammers opereren is het in de meeste gevallen echter zeer duidelijk.

## Kenmerken van spamberichten:

- berichten worden in grote hoeveelheden verstuurd, naar duizenden mensen tegelijkertijd.
- het spammen heeft een commercieel doel. Meestal bevatten de berichten daarom een verwijzing naar een product of website. Dit is niet altijd het geval.
- de berichten worden verstuurd of geplaatst zonder toestemming of medeweten van de website, of

de ontvanger. De economische bestaansreden van spam is gelegen in de zeer lage kosten van het versturen van e-mail of het plaatsen van een ongewenste reactie op een website. Een spammer kan rendabel miljoenen spamberichten versturen om slechts één product te verkopen. Er is wereldwijd een levendige handel in bestanden met vele miljoenen e-mailadressen.

## SPECS

**Prijs:** € 21,00 (excl. btw) per licentie (verkocht per 5 gebruikers)  
**Toepassing:** Antispam, antivirus, antiphishing  
**Systeemeisen:** Windows 2000 Server of nieuwer, Internet Information Services, .NET Framework, Microsoft Data Access Components  
**Info:** [www.spamfighter.com/Lang\\_NL/product\\_sem.asp](http://www.spamfighter.com/Lang_NL/product_sem.asp)

## VOOR EN TEGEN

- webgebaseerde controleomgeving
- nederlandsstalige gebruikersomgeving
- verschillende filters, per stuk configureerbaar
- Outlook Web Access uitbreidbaar met eigen SPAMfighter-werkbalk
- gebrekkige vertalingen

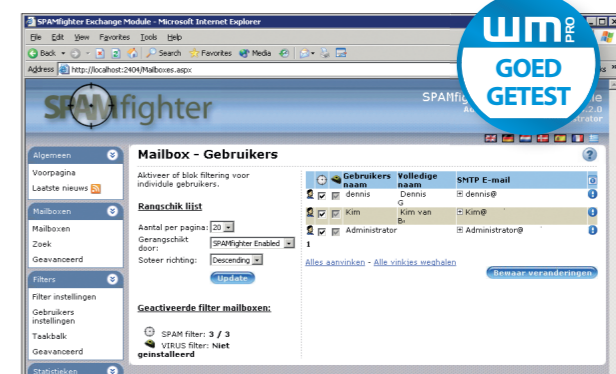
## OORDEEL

★★★★★  
 "SPAMfighter is een uitgebreide oplossing, die gebruiksgemak en functionaliteit op een slimme manier combineert."

## VAN ALLE GEMAKKEN VOORZIEN

# SPAMfighter

SPAMfighter beschikt over een overzichtelijk ingedeeld controlevenster, dat toegankelijk is via de browser. Na de installatie wordt het overzicht met beschikbare Exchange-postbussen direct gevuld. Via hetzelfde scherm kun je de anti-spambeveiliging per account in- en uitschakelen. Voor grotere organisaties is de zoekfunctie nuttig; hiermee kun je binnen de accounts op zoek gaan naar specifieke accounts. Vooral de statistieken vallen in positieve zin op. Je kunt hierbij filteren op dag, week, maand en mailbox. Bij de binnenkomst van een e-mailbericht gaat het bericht in kwestie door een vier- of vijftal individuele filters (afhankelijk van de licentie). De filters werken onder meer op basis



## "SPAMfighter maakt slim gebruik van haar gebruikers"

van whitelists en blacklists, taal en gegevens van de gebruikerscommunity. Voor dat laatste maakt SPAMfighter slim gebruik van haar gebruikers. Zij kunnen een bericht of afzender

aanmerken als spam en dit bij de makers opgeven. Vervolgens wordt de afzender op een zwarte lijst geplaatst en direct geweerd. Op het moment van schrijven bestaat deze groep

[EXCHANGE BESCHERMING]

uit 5 miljoen gebruikers, die over ruim 220 landen zijn verspreid. De filters kunnen per stuk worden in- en uitgeschakeld. Bij het bijwerken van de software maakt SPAMfighter onderscheid tussen twee modi: bij de eerste wordt het programma zelf bijgewerkt (de engine), terwijl de tweede updatesoort zich richt op het bijwerken van de Exchange-module. Systeembeheerders kunnen zelf opgeven op welke momenten welke update moet plaatsvinden. Bij de aanschaf van licenties kun je ervoor kiezen ook anti-virusbeveiliging aan de module toe te voegen. Voor deze functionaliteit verdubbelt de prijs per gebruiker.

## NAUWE INTEGRATIE MET WINDOWS-BEHEERCONSOLE

# GFiMailEssentials

## SPECS

**Prijs:** € 186,- (vanaf 10 gebruikers)  
**Toepassing:** Antispam, antivirus, antiphishing  
**Systeemeisen:** Windows 2000 Server of nieuwer, Internet Information Services, .NET Framework 2.0, Microsoft Data Access Components  
**Info:** [www.gfi.nl](http://www.gfi.nl)

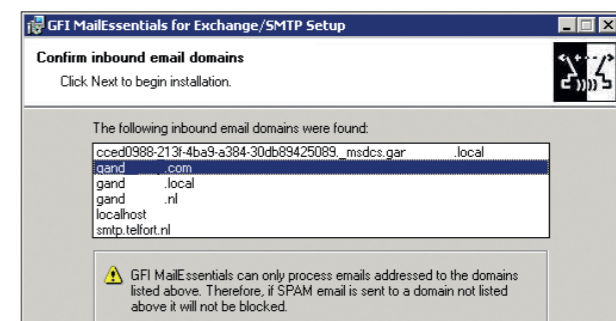
## VOOR EN TEGEN

- herkenbare Windows-gebruikersomgeving
- intelligente filtering
- uitgebreide handleiding en productondersteuning
- geen webomgeving
- Bayesian Filtering niet standaard ingeschakeld

## OORDEEL

★★★★★  
 "Een complete oplossing voor de gevorderde gebruiker, met een flinke no-nonsense uitstraling."

De gebruikersomgeving van GFiMailEssentials vertoont grote gelijkenis met de beheervensters van Microsoft Windows Server en is overzichtelijk opgebouwd. Links vindt u de onderdelen, terwijl rechts de bijbehorende instellingen worden getoond. Door op een instelling te dubbelklikken, wordt het eigenschappenvenster geopend. Nadeel van deze aanpak – ten opzichte van een webomgeving – is dat je voor het aanpassen van de instellingen bent aangewezen op de server waarop GFiMailEssentials is geïnstalleerd. GFiMailEssentials maakt intensief gebruik van 'Bayesian Filtering'. Hierbij vindt de filtering plaats op basis van wiskundige formules. In de praktijk wordt gebruik gemaakt



van een dataset die specifiek wordt samengesteld op basis van de installatie en de ontvangen én verzonden berichten. Hierdoor beschik je dus over een intelligent afweermechanisme. Het principe is relatief eenvoudig: de eerste weken wordt een database samengesteld met woorden afkomstig uit zowel legitieme als malafide e-mail. Vervolgens wordt een

'waarschijnlijkheidswaarde' toegekend aan elk woord. Als een specifiek woord in 50 van de 200 spamberichten voorkomt en slechts in 5 van de 500 goede e-mailberichten, wordt deze waarde 0,96 (50/200 / (5/500+50/200)). Hoewel GFiMailEssentials veel vertrouwen heeft in Bayesian Filtering, is het filter bij een standaardinstallatie niet ingeschakeld, en

[EXCHANGE BESCHERMING]

ben je gedwongen het zelf in te schakelen. Exchange Server beschikt zelf al over een anti-spamfilter, het Internet Message Filter (IMF). Hoewel dit niet wordt aangeerd, kun je zowel GFiMailEssentials als IMF tegelijkertijd inschakelen. Naast spam wordt ook phishing-e-mail geblokkeerd. Daarvoor maakt de oplossing gebruik van een Realtime Blocklist. Bij binnenkomst van een phishing-bericht wordt het IP-adres van de afzender direct vergeken met een database van beruchte IP-adressen. Hoewel steeds minder oplossingen nog ondersteuning bieden voor het gedateerde Exchange Server 5.5, doet GFiMailEssentials dit nog wel.