WHIRLWIND INTERNET

NIEUWS

Whirlwind Nieuws ▪ Nummer 5 ▪ December 2006

Bestrijd ongewenste e-mail met CleanPort

E-mail is als medium voor communicatie niet meer weg te denken uit onze maatschappij. De snelheid en laagdrempeligheid van het gebruik van e-mail brengen enorme voordelen met zich mee, maar helaas vormt spam een grote bedreiging.

Meer dan 70% van alle e-mailberichten is spam. De kans is groot dat u dagelijks geconfronteerd wordt met vele ongewenste berichten. Afgezien van de ergernis kost het afhandelen van spamberichten tijd waardoor de productiviteit afneemt. Daarnaast vormen virussen in e-mailberichten een bedreiging.

Samenwerking
Deze ontwikkeling is ons uiteraard niet ontgaan, vandaar dat we een samenwerking aangegaan zijn met het Nederlandse bedrijf CleanPort om een geavanceerde oplossing voor spam en virussen te introduceren.

Geen spam en virussen meer
De afhandeling van spam en virussen kunt u volledig overlaten aan CleanPort. Alle e-mail wordt via gecombineerde technieken real-time gescand. Op basis daarvan bepaalt CleanPort of een e-mailbericht spam is of een virus bevat.

Onderscheidende aanpak
Pas als van een bericht vastgesteld is dat het geen spam betreft of geen virus bevat, wordt de mail in uw mailbox geplaatst. Dat is het punt waarmee CleanPort zich onderscheidt van spamfilters die momenteel veel gebruikt worden. Bij dergelijke spamfilters wordt de spam weliswaar gefilterd, maar u blijft de berichten ontvangen waardoor u tijdens het werk mogelijk afgeleid wordt door de spam die regelmatig binnenkomt. Daarnaast nemen de mailboxen onnodig veel opslagruimte in. Met CleanPort ontvangt u 's morgens één overzichtelijke e-mail waarin staat welke berichten de afgelopen dag als spam herkend zijn. Zo hoeft u niet meer alle spamberichten door te kijken en ontvangt u alleen de berichten die van belang zijn.

Mocht in het onwaarschijnlijke geval een e-mail onterecht als spam herkend zijn (geen enkel spamfilter is immers perfect), dan kunt u dat met één druk op de knop in de dagelijkse e-mail herstellen. Alle gefilterde berichten worden 30 dagen bewaard in de quarantaine. Zo weet u zeker dat u geen mail mist en toch blijft uw mailbox vrij van spam en virussen.

Moderne techniek
Voor het scannen van de e-mailberichten maakt CleanPort gebruik van een in eigen beheer ontwikkelde spam- en virusscanner. De scanner is ook in staat spam die volgens de nieuwste trend gemaakt is, namelijk in de vorm van afbeeldingen, te onderscheppen. Verder is de zelflerende scanner in staat om nieuwe virussen te herkennen.

Online beheer

Via internet kunt u CleanPort aanpassen aan uw wensen. Zo kunt u bijvoorbeeld zelf nieuwe e-mailadressen toevoegen, instellen hoe streng berichten gescand moeten worden, bepaalde afzenders blokkeren en de quarantaine en statistieken bekijken. Een demonstratie van CleanPort vindt u op http://cleanport.whirlwind.nl

Kosten
CleanPort kunt u als abonnement bij ons bestellen. Een abonnement kost maandelijks € 2 per gebruiker. Er geldt een minimum afname van 5 gebruikers, ook als u CleanPort bestelt voor minder werknemers. Bij grotere aantallen sturen we u graag een offerte.

Kosteloos 30 dagen testen
We bieden u de mogelijkheid om CleanPort gratis 30 dagen te proberen zodat u de voordelen van een overzichtelijke Postvak IN zonder spam en virussen kunt ervaren. U kunt zich telefonisch of per e-mail aanmelden: cleanport@whirlwind.nl.

Gemak
U hoeft geen software te installeren; we schakelen CleanPort voor u in zodat u daar geen omkijken naar heeft.

Voordat de proefperiode afloopt nemen we contact met u op om te vragen hoe de dienst bevallen is. Als het product aan de verwachtingen voldaan heeft, kan het proefabonnement omgezet worden in een blijvend abonnement.

Anti-spam

Deze laatste nieuwsbrief van 2006 staat in het teken van spam. Iedereen lijkt er inmiddels last van te hebben: overvolle e-mailprogramma's die uitpuilen van ongewenste berichten. We bekijken een aantal mogelijkheden om spam tegen te gaan, waaronder CleanPort waarover u meer leest in deze nieuwsbrief.

Voordelen CleanPort
- Geen investeringen nodig in hardware en software
- Controle over instellingen, rapportage, quarantaine en black / whitelist via handig online controlpanel
- Elke gebruiker kan persoonlijke voorkeuren instellen, zoals het filterniveau van de spamscanner: voorzichtig, normaal of streng
- Onderwerp uitbreiden met **SPAM** is ook mogelijk
- Updates zijn inbegrepen
- E-mails met ongewenste bijlagen kunnen tegengehouden worden
- CleanPort is ook geschikt indien u een eigen mailserver heeft (via MX-record)
- De mail wordt bewaard indien uw mailserver tijdelijk onbereikbaar is
- Eventueel kan ook uitgaande mail gescand worden op spam en virussen

Postbus 477

5460 AL Veghel

T 0413 352632

F 0413 784584

E info@whirlwind.nl

▶

Op de achterzijde
vindt u tips om spam te voorkomen

Hoe om te gaan met spam en tips om spam te voorkomen

- **Voer uw e-mailadres niet zomaar in**
  Afzenders van spam maken gebruik van software die op het web zoekt naar e-mail-adressen. Onder andere gastenboeken en forums zijn doelwit van dergelijke spambots aangezien daar vaak veel e-mailadressen in vermeld worden. Als u toch een e-mailadres wilt invoeren op websites, kunt u gebruikmaken van een apart e-mailadres, bijvoorbeeld van MSN Hotmail. Mocht op dat e-mailadres later veel spam komen, dan kunt u het adres eenvoudig afsluiten. Het voorgaande geldt niet alleen voor websites, maar ook in het algemeen. U weet immers niet wat de ontvanger met uw e-mailadres doet.

- **Scherm uw e-mailadres op de website af**
  Op uw website is mogelijk uw e-mailadres vermeld. Zo ja, dan is de kans groot dat spambots op deze manier het e-mailadres ontdekken, tenzij uw e-mailadres afgeschermd is. Er zijn diverse manieren om e-mailadressen af te schermen. Het is onder andere mogelijk om e-mailadressen te versleutelen zodat spambots het e-mailadres niet opmerken. Een andere manier is het e-mailadres als een afbeelding op te nemen in de website. Een afbeelding kan in principe alleen door mensen gelezen worden, vandaar dat een spambot dan achter het net vist. Verder kunt u de bezoeker alleen de mogelijkheid bieden om een e-mailformulier in te vullen. U weet dan zeker dat spambots het adres niet kunnen vinden, maar helaas bestaan er ook spambots die het formulier invullen zodat u de spam alsnog ontvangt. Hoe dan ook, geen enkele methode is 100% waterdicht. Desondanks is het de moeite waard om e-mailadressen af te schermen aangezien het voor de spambots lastig is om de adressen te achterhalen.

- **Reageer niet op ongevraagde berichten**
  Als u antwoordt op spamberichten weet de afzender dat uw e-mailadres bestaat en gebruikt wordt. U ontvangt dan waarschijnlijk nog meer spam. Bovendien bevatten de berichten soms verborgen links die geactiveerd worden zodra u de berichten opent of beantwoordt. Het beste is om nergens op te klikken en het bericht te verwijderen. Klik ook niet op *unsubscribe* of een vergelijkbare mogelijkheid om u af te melden, tenzij u de afzender vertrouwt.

- **Gebruik BCC in plaats van CC**
  Gebruik het BCC-veld (blind carbon copy) in plaats van het CC-veld (carbon copy) als u een bericht naar meerdere mensen tegelijk stuurt. Het voordeel van BCC is dat de ontvangers niet kunnen zien naar welke andere ontvangers het bericht gestuurd is. Zo beschermt u de adressen van anderen.

- **Reageer niet op kettingbrieven**
  Negeer e-mails waarin u gevraagd wordt om het bericht naar zoveel mogelijk mensen door te sturen. Deze e-mails bevatten bijna altijd een *hoax*: een vorm van bedrog. Door niet te reageren zorgt u ervoor dat uw adres niet bevestigd wordt bij de afzender en geeft u geen adressen van anderen door.

- **Let op voor oplichting via e-mail**
  Oplichting via e-mail wordt *phishing* genoemd, een verbastering van het Engelse woord *fishing*, aangezien de oplichters hengelen naar persoonlijke informatie van de ontvanger; ze vissen naar creditcardnummers, bankgegevens en wachtwoorden. Bekende voorbeelden zijn officieel ogende e-mails die afkomstig lijken te zijn van eBay, PayPal en Postbank. De ontvanger wordt gevraagd op een website de gegevens bij te werken of een nieuw wachtwoord in te stellen waarna deze in handen komt van de oplichter. Bij phishing wordt een vertrouwde website vaak gekopieerd zodat nietsvermoedende personen de gegevens invoeren. Soms wordt bovendien gebruikgemaakt van lekken in Internet Explorer en andere browsers zodat het lijkt alsof de bezoeker zijn gegevens op de echte site van het bedrijf invoert.

- **Koop niet via ongevraagde berichten**
  Als u van spammers koopt, zorgt u ervoor dat het loont om te spammen. De spamberichten verdwijnen alleen als de verzending niet meer rendabel is.

- **Voorkom dat uw computer ongemerkt spam en/of virussen verstuurt**
  Er zijn virussen en spyware in omloop die ervoor zorgen dat uw computer ongemerkt spam verstuurt. Dit kunt u voorkomen door gebruik te maken van een firewall. Een firewall beveiligt uw computer tegen ongewenste toegang van en naar internet. Zo voorkomt u dat een bepaald programma zonder toestemming contact maakt met internet. Ook andersom biedt een firewall uitkomst, namelijk als vanaf een andere computer verbinding met uw computer gemaakt wordt om bijvoorbeeld een softwarelek te benutten. Bekende firewalls zijn ZoneAlarm en Norton Internet Security.
  Naast een firewall is het van belang dat uw computer over de nieuwste updates van het besturingssysteem beschikt. Daarmee voorkomt u dat bekende veiligheidslekken gebruikt worden door onder andere virussen. In het geval van Windows kunt u updates downloaden via Windows Update: http://windowsupdate.microsoft.com. Verder is een virusscanner van groot belang. Er bestaan namelijk virussen die uw adressenboek naar spammers sturen. Veel virusscanners zijn ook in staat om spyware te vinden en te verwijderen. Mocht uw virusscanner geen spyware kunnen detecteren, dan kunt u ook een afzonderlijk programma installeren, bijvoorbeeld Spyware Doctor.

- **Negeer e-mails waarin staat dat u een virus verzonden zou hebben**
  Zolang u over een recente virusscanner beschikt en uw computer dus in principe niet besmet kan zijn, kunt u e-mails negeren waarin beweerd wordt dat u een virus verzonden zou hebben. Deze e-mails zijn het gevolg van virussen die zichzelf versturen met als afzender een fictief adres of een adres dat uit adresboeken van besmette computers gehaald is (*spoofing*).

- **Maak geen gebruik van catch-all**
  Spam wordt vaak naar niet bestaande e-mailadressen gestuurd. Als u gebruik maakt van een catch-all, dan ontvangt u dergelijke berichten toch. Een catch-all zorgt er namelijk voor dat alle mail gericht aan uwnaam.nl wordt ontvangen. Mocht u veel spam ontvangen, dan is het de moeite waard om te kijken naar welke adressen de spam gestuurd wordt. Dat kunt u zien in uw e-mailprogramma als u de broncode van een spambericht bekijkt. Mocht blijken dat de mails naar niet bestaande adressen gestuurd worden, dan kunt u de catch-all uitschakelen om spam te voorkomen.

- **Maak gebruik van een spamfilter**
  Microsoft Outlook 2003 beschikt standaard over een goed functionerend spamfilter, mits deze voorzien is van updates. De updates van het spamfilter en de andere Office-programma's vindt u op http://office.microsoft.com. Mocht u een ander e-mailprogramma gebruiken, dan kunt u ook een afzonderlijk spamfilter gebruiken. Bijvoorbeeld Internet Security van Norton biedt onder andere een spamfilter dat geïntegreerd kan worden in Outlook Express en Outlook. Ook bij dit programma is het noodzakelijk om het filter van updates te voorzien.