

## MicroWorld MailScan

### Revolutionaire poortwachter

Ieder zichzelf respecterend bedrijf heeft tegenwoordig wel een of andere vorm van een firewall geïnstalleerd. En natuurlijk draait er op regelmatige tijden, veelal eenmaal per week, een virusscan over alle systemen. Op deze manier is men veilig. Tenminste dat wordt gedacht. Het product MailScan laat echter zien dat er nog veel meer gaten te dichten zijn. En het helpt daarbij.

MailScan is een product van het van oorsprong Indiase bedrijf MicroWorld. Zoals de naam al doet vermoeden is de kern-taak van het pakket het in de gaten houden van in- en uitgaande mailberichten. Dit is niet zo'n gekke benadering want helaas laat de praktijk zien dat ruim 95% van alle virussen en andere enge zaken als trojaanse paarden via e-mail onze bedrijven binnenkomen.

Maar we hebben toch een anti-virus product op onze machine draaien? En één keer per week kijken we of er nieuwe stuurbestanden zijn om ook de allernieuwste aanvallen te kunnen weerstaan? Ja, dat kan wel waar zijn, maar dat is echt niet voldoende. Ten eerste draait de anti-virus-software nooit vaak genoeg en ten tweede is een updatefrequentie van eenmaal per week lang niet hoog genoeg. Verder draait op de firewallmachine dan wel de viruschecker, om in ieder geval ingaande berichten tegen het licht te houden, maar mail die intern wordt verzonden - via het intranet - valt daar dus buiten. Aanvallen met - wellicht onbedoelde - virussen kunnen dus makkelijk door de mazen van het security-net glijpen.

MailScan biedt deze problemen het hoofd door te kiezen voor een realtime strategie. Alle, maar dan ook echt alle e-mail berichten die door de mailserver worden verwerkt, worden direct gecontroleerd. Wordt er iets gevonden en is er reden om een bericht als verdacht te bestempelen, dan neemt het pakket ook de bijbehorende maatregelen.

#### MWL

De geheime kracht achter MailScan heet MWL. Deze afkorting staat voor MicroWorld WinSock Layer. Ook hier doet de naam al vermoeden in welke richting moet worden gekeken. Inderdaad WinSock. Vrijwel alle mail wordt via WinSock verstuurd en ontvangen. MailScan's MWL is nu een laag bovenop WinSock en kan dus alle verkeer doorlichten. Van boven naar beneden bekeken zijn een aantal lagen te onderscheiden. Allereerst WinSock zelf. Direct hieronder bevindt zich de MWL-laag die met behulp van de Content Parser het bericht disassembled - uiteen haalt. Zijn er .zip-bestanden dan komt een volgend filter in actie om ook deze bestanden te ontrafelen. Nu volgt de zogenaamde e-Scan Content Analyser. Deze module heeft op de achtergrond alle up-to-date virusinformatie beschikbaar. Deze is up-to-date omdat MailScan automatisch iedere N minuten van een van de wereldwijde MicroWorld websites de meest recente informatie kan ophalen. De waarde van N is uiteraard zelf in te stellen. En als laatste onderdeel van de MailScan MWL-laag is er de Object Assembler die het ontrafelde bericht weer keurig in de originele vorm terugbrengt. Nu kan het bericht, als het tenminste 'schoon' is, verder worden doorgegeven aan de mailclient.

Ter verduidelijking: WinSock is een DLL, die start voordat er een netwerkprogramma gaat draaien dat gebaseerd is op TCP/IP.

#### Productinformatie

##### MicroWorld MailScan

##### Fabrikant

MicroWorld

<http://www.raxco.nl/mapl/>

##### Prijs

Neem voor actuele prijsinformatie contact op met de distributeur

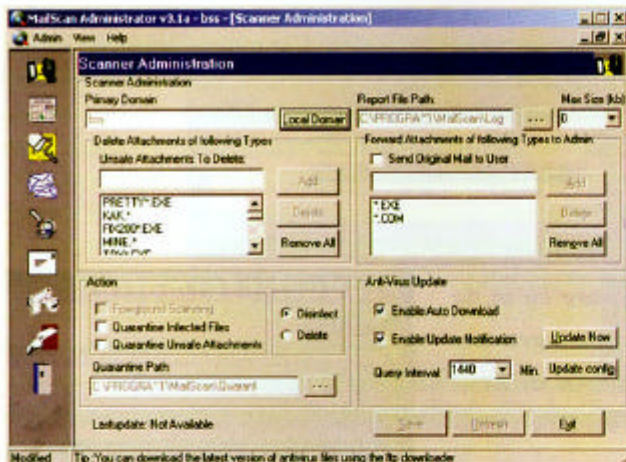
##### Beoordeling

- + Eenvoudig beheer; Real-time; Snelle virusupdates; MailScan start voordat de allereerste TCP/IP applicatie start; Geen extra machine nodig als gateway - geen routering dus; Brede scan mogelijkheid o.a. POP3; Kan overweg met vele type archives zoals ZIP, Tar, ARJ enzovoorts.
- Nog geen support voor HTTP en FTP; Enige kennis van protocollen nodig.

#### Installatie en configuratie

Het installeren van MailScan verloopt als verwacht. Er zijn keuzemogelijkheden om MailScan te installeren voor onder meer mailservers als Lotus Notes, Mdaemon, Exchange en VPOP3. Helaas moet wel de computer een herstart ondergaan. Waarschijnlijk is dat in de versie voor Windows XP binnenkort niet meer nodig. En daarna is MailScan klaar om verder geconfigureerd te worden.

De configuratie is nodig omdat MailScan nogal wat eigenschappen heeft die wat aandacht nodig hebben voordat het pakket zelfstandig - realtime - zijn werk kan doen. Die eigenschappen zijn onder andere het scannen van bijna alle mailberichten voordat ze de mailserver zelf bereiken. Maar ook spam-controle is mogelijk. Hiervoor moet wel een adres(sen) lijst worden samengesteld van ongewenste afzenders. In veel gevallen zullen dit dus adressen zijn van zogenaamde Free Mail Providers als Hotmail. Een ander in te stellen stuk van MailScan is de compressie van bestanden. Zijn



▲ Afbeelding 1:  
Administrator menu

bestanden groter dan de ingestelde waarde, dan zal met behulp van de standaard compressiesoftware - zeg maar WinZip - het bestand worden gecomprimeerd tot een zelf-uitpakkend bestand. Zodoende gaat er veel minder verkeer over het net. En aan de andere kant zal een binnenkomend gecomprimeerd bestand worden uitgepakt, worden bekeken op viri en dan naar de eindgebruiker worden verstuurd. Dit geldt natuurlijk ook voor alle aanhangsels, de attachments en HTML-mails. Is het aanhangsel een script in bijvoorbeeld Visual Basic, dan zal dit eveneens onder de loep worden genomen voordat het verder door mag. En om de ethiek van het bedrijf hoog te houden kan de verantwoordelijke ook een lijst samstellen van woorden die noch in het subject, noch in de mail zelf mogen voorkomen. Het mag duidelijk zijn wat voor soort lijst dit is.

Op het moment dat een mail het bedrijf wil verlaten en MailScan vindt een verdacht deel, dan zal er een bericht naar de geadresseerde uitgaan met daarin de opmerking dat de bedoelde mail door MailScan is tegengehouden. Tevens wordt naar de MailScan-beheerder een mail gestuurd met daarin de melding van wat er is voorgevallen. Alle uitgaande mail krijgt van MailScan een onderschrift mee dat het bericht plus aanhangsel(s) is gecontroleerd.

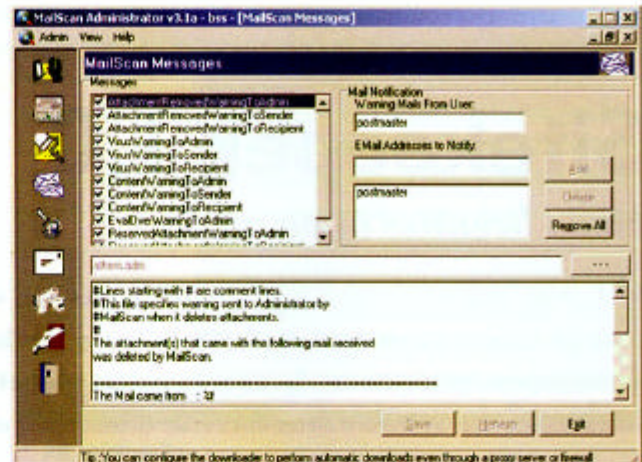
Voor binnenkomende mail geldt in feite hetzelfde, met dien verstande dat verdachte of niet te analyseren bestanden in

een speciale quarantaine directory een plaatsje vinden. Ook nu krijgt de MailScan beheerder, de Postmaster, een bericht dat er iets niet in de haak is. Deze postmaster heeft binen MailScan een menustructuur ter beschikking om het onderhoud uit te voeren. Deze structuur is simpel en eenvoudig te doorgronden. Onderwerpen als Administration, Content Control, Compression Control en Scan Control laten zich goed instellen en monitoren. Voor de instellingen in het Domain Control is kennis nodig van



welke TCP/IP poorten de diverse protocollen gebruiken, maar de standaard waarden zijn voor de meeste implementaties accuraat. De Postmaster heeft ook de mogelijkheid in te stellen om de hoeveelheid tijd er een download moet plaatsvinden van de nieuwste virusinformatie. Standaard is dit 1440 minuten, inderdaad 24 uur. Ook kan een keuze worden gemaakt tussen FTP of HTTP downloads voor de virusinformatie.

In het menu onderdeel Content Control staat de al genoemde lijst met 'verboden woorden'. Als zo'n woord door MailScan is ontdekt, dan kan of de betreffende mail permanent worden verwijderd, in quarantaine worden geplaatst of naar de



▲ Afbeelding 2:  
Meldingen optie in menu

Postmaster worden verzonden. Uitgaande mail kan tevens worden voorzien van een standaard disclaimer zodat bedrijf X niet aansprakelijk kan worden gesteld voor de verzonden mail. Ook kan enkel alle mail van of naar een bepaalde gebruiker worden behandeld door MailScan. Post voor andere gebruikers valt dan buiten de scanner. Zo kun je een verdachte medewerker - en hier moet uiteraard de grootst mogelijke omzichtigheid worden betracht - in de gaten houden. Omgekeerd kan er juist een uitzondering worden gemaakt voor een bepaalde gebruiker terwijl alle anderen wel onder de controle vallen. Ook hier is het ijs glad. Maar de mogelijkheden zijn beschikbaar.

### Conclusie

Al met al is MailScan een product dat veel ellende kan voorkomen en dat doet op plekken waar geen ander pakket dat doet. Voor de mailserver en in realtime. Gecombineerd met de hoge frequentie van virus update-informatie maakt het het leven van virussen, trojaanse paarden en verdachte scripts behoorlijk moeilijk. Zijn er ook negatievere kanten? Ja natuurlijk. FTP- en HTTP-verkeer is nog vogelvrij in deze versie, al heeft MicroWorld aangekondigd hier snel verandering in te zullen brengen. Dus mail van Hotmail-accounts - sowieso twijfelachtig - wordt ongestoord doorgelaten, mits de beheerder er een stokje voor steekt via zijn menu. ▲