

Controllo dello spam basato su server

Un test pratico di 5 noti prodotti software antispam per Microsoft Exchange Server

Non c'è bisogno di discutere a lungo su quanto lo spam possa costare alle organizzazioni. Siete in difficoltà? Lottate ogni giorno con questo problema. Sebbene gli utenti domestici non abbiano molta scelta nell'installare prodotti antispam nei loro computer, comprendete certo che un approccio basato su server fornisca vantaggi significativi alle imprese, come ad esempio un minor tempo di implementazione e amministrazione, e un minor costo per utente.

Ho provato 5 soluzioni software antispam basate su server progettate specificatamente per integrarsi con Microsoft Exchange Server e trarre vantaggi dalle caratteristiche di Exchange che Microsoft ha messo a disposizione per gli sviluppatori: iHateSpam for Exchange di Sunbelt Software, Server Edition; GFI Mail Essentials for ExchangeSMTP di GFI Software; Policy Patrol Enterprise di Red Earth Software; Xwall for Microsoft Exchange con XWALLFilter di DataEnter; e Power Tools for Exchange-Internet di Nemx Software. Ho installato ognuno di questi prodotti su Windows Server 2003 con Exchange Server 2003 e li ho eseguiti per un certo periodo.

Metodi di filtro e criteri di test

Ognuno di questi pacchetti software offre diverse tecnologie di filtraggio che consentono di personalizzare come le email vengano analizzate per determinare la probabilità che il messaggio sia uno spam (mail non richiesta) o un ham (mail legittima). Alcune di queste tecnologie utilizzano informazioni basate su server per analizzare il contenuto dei messaggi, mentre altre confrontano le proprietà dei messaggi con una blacklist (cioè una lista di spammer conosciuti) che viene gestita da organizzazioni di terze parti su server remoti, e whitelist (cioè liste di indirizzi email riconosciuti come validi). Sebbene il metodo del confronto con le blacklist possa incrementare il rilevamento dello spam rispetto agli algoritmi basati su server, questo può produrre una certa latenza nel processo in quanto ha bisogno di eseguire query su reti remote. Gli amministratori dei sistemi di messaggistica devono valutare la necessità e il valore di queste interrogazioni remote e degli algoritmi nel loro particolare ambiente.

Il filtraggio semantico, nel quale la presenza di specifiche parole o frasi è un indicatore che il messaggio è uno spam, è una tecnica comune supportata da ogni prodotto presentato in questa analisi. I filtri bayesiani usano algoritmi matematici per analizzare il contenuto di spam e ham, quindi utilizzano l'analisi dei risultati per predire la proba-

bilità che un messaggio in entrata sia uno spam. I filtri bayesiani sono stati provati essere una delle tecniche di filtraggio maggiormente valide ma, come per il software di riconoscimento vocale, dipendono da quello che possono apprendere nei riguardi dello spam e dell'ham di una organizzazione. In un tipico ambiente aziendale, questo processo di apprendimento può durare una settimana o più.

Per valutare questi prodotti, ho esaminato la varietà di tecnologie di filtro che supportano, come la flessibilità che il prodotto offre in fase di personalizzazione. Ho analizzato le capacità di reporting, la facilità di implementazione, l'usabilità e l'efficienza di ogni strumento amministrativo disponibile. Lo scopo del mio test è stato quello di misurare l'efficienza delle capacità di filtraggio di ogni prodotto.

iHateSpam for Exchange, Server Edition

iHate Spam for Exchange, Server Edition di Sunbelt Software si installa su server Exchange 2000 o Exchange 2003. Il software adopera un filtraggio semantico, basato su regole o su blacklist per eliminare le mail non richieste o posizionarle in una cartella di quarantena.

Secondo la documentazione del prodotto, con l'installazione di iHateSpam è possibile riconoscere il 90 per cento dello spam. È possibile incrementare la capacità di rilevamento del prodotto personalizzando le sue caratteristiche. Per esempio, iHateSpam consente di definire filtri globali da applicare a tutti gli utenti. Utilizzando questi filtri globali, è possibile creare una lista di indirizzi email, domini e nomi che devono essere sempre accettati o rifiutati. La personalizzazione delle regole consente di creare i propri criteri per l'identificazione dei messaggi. Quando un messaggio corrisponde ai criteri impostati, il suo peso come spam viene incrementato di un fattore associato con la regola. Il peso finale del messaggio dopo che tutti i criteri sono stati applicati determina se il messaggio deve essere eliminato, posto in quarantena o inoltrato. Finalmente, è possibile definire in un criterio personalizzato un insieme di criteri di filtro che vengono applicati a ogni mailbox che viene assegnata al criterio. Al criterio predefinito di iHateSpam vengono assegnate tutte le mailbox.

iHateSpam inoltre fornisce diversi report statistici se viene installato il componente opzionale di reporting. I report sono disponibili sia in formato grafico che testuale. Alcuni tra quelli disponibili sono: messaggi spam identificati dall'utente, i 50 utenti che hanno ricevuto la maggior parte di spam, il numero di messaggi spam identificati in un dato periodo di tempo, il numero di spam e ham rice-

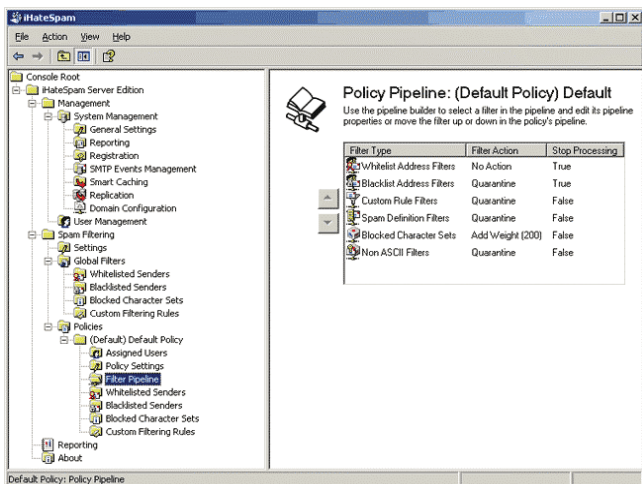


Figura 1

vuti, i messaggi catturati da ogni filtro, i messaggi gestiti dal motore di filtraggio.

L'interfaccia amministrativa di iHateSpam è uno snap-in della Microsoft Management Console (MMC) che viene eseguito da Exchange Server. L'interfaccia gerarchica simile a Windows Explorer permette un rapido accesso a tutte le funzioni, incluse le policy, i filtri globali e l'assegnazione delle policy agli utenti.

Per incrementare le prestazioni del sistema, iHateSpam utilizza lo smart caching per le informazioni di configurazione. Le regole di definizione, l'assegnazione dei criteri agli utenti, le whitelist e le blacklist memorizzate nella cache vengono automaticamente aggiornate ogni 6 ore. Per forzare le modifiche ad avere effetto in modo immediato, è possibile utilizzare la console amministrativa e ricaricare manualmente la cache. I siti con più di una macchina Exchange Server che ospita mailbox apprezzeranno la capacità di iHateSpam di replicare le informazioni di configurazione da un server all'altro.

Il software si è installato con facilità sul mio server di test, legandosi all'archivio SMTP OnPostCategorize. Ho installato nello stesso tempo anche il componente di reporting opzionale.

Per il mio test, ho creato una policy personalizzata, mostrata nella Figura 1, con una regola di filtro personalizzata che incrementasse il peso del messaggio di 200 unità quando il filtro identificava un messaggio con una stringa di caratteri inusuale. Dopo aver ricaricato la cache, iHateSpam ha messo in quarantena i messaggi contenenti la stringa impostata per gli utenti configurati per l'utilizzo del criterio.

Sebbene il software manchi di supporto per alcuni dei più sofisticati algoritmi di filtro, iHateSpam fornisce un filtro antispam basato su server di base a un prezzo ragionevole.

iHateSpam for Exchange, Server Edition

Contatto: Sunbelt Software

Web: <http://www.sunbeltsoftware.com>

Prezzo: Iniziale pari a \$395 per 25 mailbox

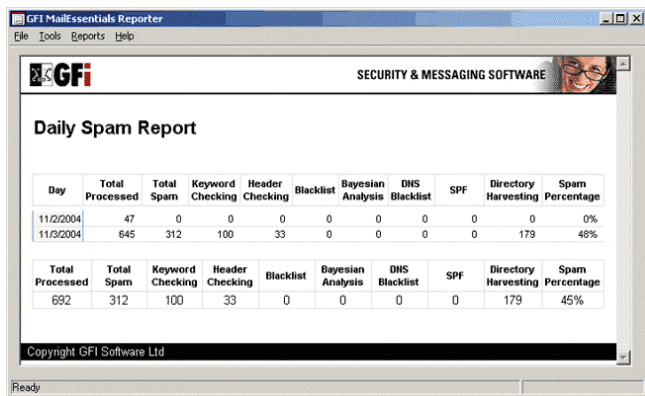


Figura 2

Riepilogo

Pro: Un filtro antispam basato su server di buon valore: interfaccia amministrativa semplice da utilizzare

Contro: Richiede un certo sforzo amministrativo per la personalizzazione del rilevamento dello spam in maniera efficiente: non consente l'amministrazione remota

Commento:

iHateSpam for Exchange, Server Edition fornisce un filtro antispam basato su server di base a un prezzo ragionevole

GFI Mail Essentials for Exchange/SMTP

GFI MailEssentials for Exchange/SMTP di GFI Software aggiunge un controllo antispam basato su server, monitoraggio ed archiviazione dei messaggi, e download POP3 a Exchange Server, e possiede una lista di componenti server opzionali. È possibile implementare MailEssentials come gateway di posta su un sistema che non esegue Exchange Server, ma alcune caratteristiche come l'inoltro dei messaggi verso la cartella di posta indesiderata dell'utente non sono disponibili nella configurazione.

In aggiunta ai filtri bayesiani, MailEssentials supporta Sender Policy Framework (SPF) e la caratteristica DNS Blacklist. SPF identifica lo spam confrontando gli indirizzi IP del server di posta che ha inviato il messaggio con una lista di indirizzi di server di posta che sono registrati come domini di invio. Se il messaggio sembra provenire da un utente di xyz.com ma non proviene da un server di posta che l'amministratore ha registrato in SPF, il messaggio viene considerato spam.

I filtri e le regole di MailEssential offrono una serie di opzioni per la gestione dei messaggi di posta. È possibile specificare che lo spam venga inviato direttamente a una cartella nella mailbox dell'utente quando si installa il software su Exchange Server 2000 o Exchange Server 2003. Opzionalmente, MailEssentials può marcare lo spam con una stringa, in modo da consentire alle regole di Outlook di determinare la disposizione finale del messaggio. Questo è utile per gli utenti di Exchange 5.5 e a chi vuole installare MailEssentials come gateway di posta.

MailEssentials include report standard che è possibile personalizzare a seconda dei dati o altre rilevanti opzioni in report specifici. È possibile visualizzare le informazioni per utente o per dominio di posta di ricezione o invio, ricevere un riepilogo dei messaggi divisi per data, e ricevere

Controllo dello spam basato su server

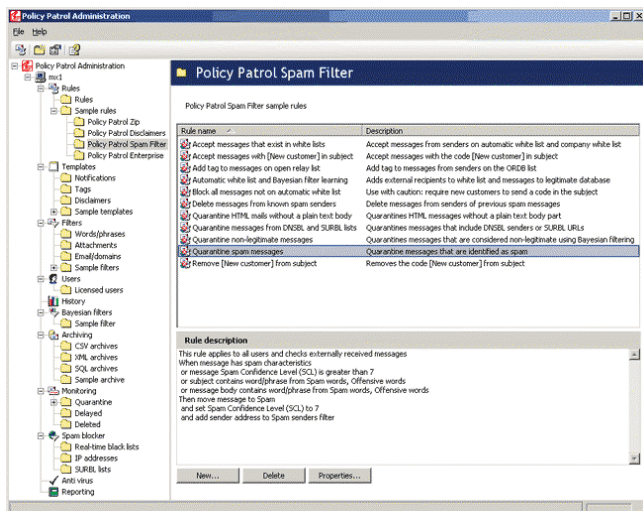


Figura 3

un riepilogo giornaliero riguardo allo spam rilevato. La Figura 2 mostra un semplice Daily Spam Report.

Io ho installato MailEssentials in pochi minuti senza problemi. Durante l'installazione mi è stata data l'opportunità di installare MailEssentials in Active Directory (AD) mode o in SMTP mode. L'AD mode consente di impostare regole personalizzate per gli utenti AD. In modalità SMTP invece si impostano le regole secondo gli indirizzi di posta.

Dopo aver completato l'installazione, ho provato ad utilizzare lo strumento di configurazione di MailEssentials. Per default, i filtri bayesiani non sono abilitati; altre opzioni di filtraggio sono configurate per marcare i messaggi filtrati con "SPAM", un default che gli utenti Exchange 2003 possono modificare. MailEssentials rileva gli attacchi Directory Harvesting, dove uno spammer ottiene un indirizzo email, attraverso messaggi inviati a una combinazione di indirizzi email validi e non validi. La visualizzazione dei file di log di MailEssentials rivela che la caratteristica Directory Harvesting è in funzione, filtrando i messaggi che vengono inviati a mailbox esistenti e non esistenti.

GFI Mail Essentials è un buon prodotto anti-spam. Le caratteristiche aggiuntive di archiviazione e monitoraggio, del downloading POP3 e della lista di server rendono il pacchetto una scelta interessante per molte imprese.

GFI MailEssentials for Exchange/SMTP

Contatto: GFI Software

Web: <http://www.gfi.com>

Prezzo: Iniziale fissato a \$295 per 10 mailbox, \$315 per 25 mailbox. Include supporto per 3 mesi e l'aggiornamento anti-spam per 1 anno.

Riepilogo

Pro: Supporto dei filtri bayesiani, del directory harvesting e dei filtri Sender Policy Framework (SPF)

Contro: Usa un insieme di comandi basati sulla posta per l'amministrazione remota

Commento:

Buon prodotto, soprattutto come filtro antispam. Le caratteristiche aggiuntive lo rendono una scelta interessante.

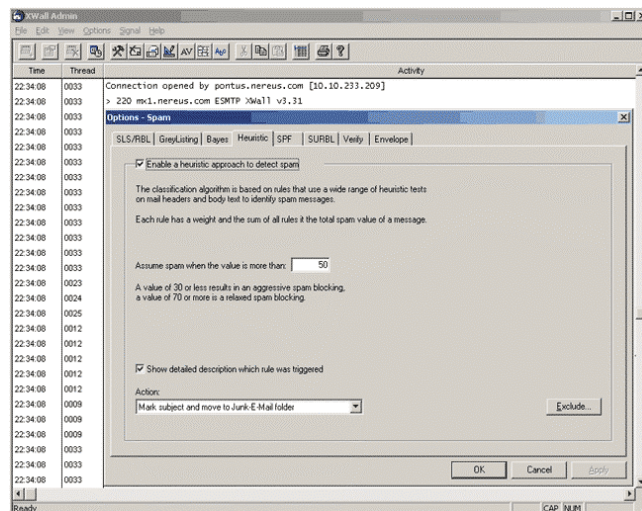


Figura 4

Policy Patrol Enterprise

Policy Patrol Enterprise di Red Hearst Software offre il filtraggio dello spam basato su server con la compressione e decompressione automatica degli allegati e altre caratteristiche relative alla posta elettronica.

Policy Patrol supporta i filtri bayesiani, lo Spam URL Realtime Block List (SURBL), e altre tecniche standard di filtraggio, incluso il filtro semantico, le blacklist, e le whitelist. Policy Patrol è estremamente flessibile nella definizione delle regole e questo rende semplice creare regole personalizzate per specifici utenti, sottoposte ad una varietà di condizioni ed eccezioni. La capacità di utilizzare espressioni regolari simili a UNIX quando confronta le stringhe di caratteri aggiunge a Policy Patrol potere e flessibilità. Policy Patrol è in grado di rimuovere tag HTML incorporati, che molti spammer utilizzano per distinguere parole e frasi che possono identificare un messaggio come spam.

La regola di default di Policy Patrol per la gestione dello spam posiziona i messaggi filtrati in una speciale cartella spam per il controllo e l'inoltro o la cancellazione da parte di un amministratore. Ad ogni modo, è possibile configurare Policy Patrol affinché aggiunga un x_header al messaggio, che consentirà ad Outlook di spostare il messaggio in una cartella spam. Policy Patrol consente agli utenti di aggiungere nuovi indirizzi email alla whitelist globale codificando ["New Customer"] nella linea dell'oggetto del messaggio che viene inviato. Policy Patrol rimuove il codice prima di inviare il messaggio. Quando gli utenti utilizzano una blacklist in tempo reale e Policy Patrol identifica la sorgente del messaggio come spammer, si ha l'opzione di rifiutare il messaggio prima di scaricarlo, in questo modo risparmiando tempo e risorse. Il software supporta le regole che impostano lo Spam Confidence Level (SCL) che Exchange 2003 utilizza per inoltrare lo spam alla cartella Posta Indesiderata dell'utente.

Policy Patrol è in grado di archiviare i messaggi in formato XML, comma-separated value (CSV), o SQL database. È possibile abilitare l'archiviazione creando una regola che consenta il deposito di tutti i messaggi selezionati. Il software inoltre include 21 definizioni di report che posso-

no essere generati dagli archivi basati su SQL, necessitando dunque di una implementazione di database SQL per poter utilizzare le capacità di reporting di Policy Patrol.

Sebbene l'installazione di Policy Patrol non sia difficile, ha occupato più tempo degli altri prodotti. La guida online Quick Start del software guida il processo di installazione. Questo consente di installare l'interfaccia amministrativa del prodotto in workstation multiple per l'amministrazione remota. Nessuna delle caratteristiche di Policy Patrol è abilitata per default. Un'altra guida scaricabile, How to Filter Spam with Policy Patrol, mi ha aiutato a configurare il prodotto. Ho esaminato le semplici regole disponibili, mostrate dalla Figura 3, e abilitato la regola che consente il filtraggio semantico.

Complessivamente, Policy Patrol è significativamente più configurabile degli altri prodotti. Ad ogni modo, il lato negativo di questa flessibilità è una curva di apprendimento meno dolce durante la fase di implementazione del software, e richiede uno sforzo amministrativo maggiore per la gestione del suo uso.

Policy Patrol Enterprise

Contatto: Red Earth Software

Web: <http://www.redearthsoftware.com>

Prezzo: Iniziale fissato a \$395 per 10 utenti, più \$79 per il mantenimento annuale seguente al periodo di garanzia di 30 giorni. Policy Patrol Spam Filter costa inizialmente \$325 per 10 utenti, più \$65 per il mantenimento annuale.

Riepilogo

Pro: Capacità di definizione delle regole flessibile; interfaccia amministrativa che può essere eseguita dalle workstation

Contro: La flessibilità del prodotto produce una maggior complessità e una curva di apprendimento più dura: tutti i report sono generati da archivi di messaggi SQL, richiedendo l'abilitazione della archiviazione SQL.

Commento:

Complessivamente, Policy Patrol è significativamente più configurabile degli altri prodotti. Ad ogni modo, il lato negativo di questa flessibilità è una curva di apprendimento meno dolce durante la fase di implementazione del prodotto, e richiede uno sforzo amministrativo maggiore per la sua gestione.

XWall for Microsoft Exchange with XWALLFilter

XWall for Microsoft Exchange with XWALLFilter di DataEnter è un firewall di posta SMTP che è possibile installare sia su Exchange Server che su un server diverso in una configurazione gateway. Un componente opzionale, XWALLFilter, si può inserire in Exchange 2003 per inviare lo spam direttamente nella cartella Posta Indesiderata dell'utente. XWall include caratteristiche non legate al controllo dello spam, come la compressione e la cifratura dei messaggi e la scansione antivirus in associazione al programma antivirus di terze parti implementato.

XWall viene eseguito come servizio o in modalità console. In ogni caso, l'interfaccia amministrativa, mostrata nella Figura 4, registra l'attività di XWall in una finestra di console e fornisce un menu di accesso alle caratteristiche configurabili.

XWall include un completo insieme di caratteristiche di filtraggio e supporta lo Spam Lookup Service (SLS), l'SPF, il

SURBL, e altre liste di blocco. Il software inoltre supporta il greylisting, un metodo che rifiuta temporaneamente i messaggi con una combinazione di indirizzi email e indirizzi IP di server di invio sconosciuti. Il greylisting dipende dalla caratteristica di reinoltro automatico dei server SMTP standard per il rinvio dei messaggi legittimi; solitamente gli spammer non utilizzano questa caratteristica e non rinviando un messaggio quando è stato rifiutato una prima volta.

XWall utilizza un approccio euristico per il filtraggio semantico, applicando una varietà di controlli sia sulle intestazioni (header) del messaggio che sul testo del messaggio stesso. Questo metodo calcola un valore di spam per ogni messaggio. Su una scala di 100, il valore di default assegnato da XWall è 50: un valore di 30 classifica più messaggi come spam; un valore di 70 ne classifica di meno.

XWall supporta una varietà di azioni dopo aver determinato che il messaggio è uno spam, incluso l'inoltro del messaggio al postmaster e l'utilizzo di diversi metodi per marcare il messaggio prima che venga depositato. Gli utenti di Outlook possono scegliere un metodo che possa inviare i messaggi rilevati come spam alla propria cartella di Posta Indesiderata.

XWall può salvare una copia di tutti i messaggi processati in una cartella storica, ed è in grado di analizzare e bloccare sia gli allegati in entrata che quelli in uscita aventi contenuto sospetto, incluso gli exploit conosciuti e i file con doppia estensione (ad esempio .exe.jpg). Quando si abilita questa caratteristica, il software registra l'attività in file di formato CSV per l'analisi e i riepiloghi statistici nella finestra di console. XWall non include un modulo di reportistica.

Io ho installato e configurato XWall sul mio Exchange Server 2003 di test in pochi minuti, utilizzando le istruzioni disponibili presso il sito Web di XWall. Come indicato, ho configurato XWall per inoltrare il traffico di mail verso Exchange Server sulla porta 24 e ho utilizzato Exchange System manager per configurare Exchange Server per ricevere la posta sulla porta 24, seguendo l'architettura del gateway XWall.

Complessivamente, XWall è semplice da installare e flessibile, con una varietà di utili caratteristiche non direttamente legate alle operazioni antispyam.

XWall for Microsoft Exchange with XWALLFilter

Contatto: DataEnter (Austria)

Web: <http://www.dataenter.com>

Prezzo: \$679 per il bundle XWall/XWALLFilter; \$398 per XWall; \$299 per XWALLFilter

Riepilogo

Pro: Configurazione flessibile, supporto per una varietà di filtri antispyam

Contro: Nessun componente di reportistica

Commento:

Complessivamente, XWall è semplice da installare e flessibile, con una varietà di utili caratteristiche non direttamente legate alle operazioni antispyam.

Power Tools for Exchange-Internet Edition

Power Tools for Exchange di Nemx Software è un prodotto multifunzionale che include alcune caratteristiche antispyam non trovate in altri prodotti. In aggiunta alle caratteristiche

Controllo dello spam basato su server

di cui si è discusso, Power Tools esegue una scansione anti-virus e adopera il rilevamento malware Norman SandBox Technology. Power Tools è disponibile in due edizioni. L'Internet Edition, che ho provato, analizza i messaggi che passano attraverso il connettore SMTP internet. L'Advanced Edition aggiunge funzionalità di monitoraggio e analisi dei contenuti delle mailbox e delle cartelle pubbliche.

In aggiunta alla lista di indirizzi e al rilevamento dello spam basato su regole, Power Tools include un approccio proprietario che Nemx Software definisce Concept Manager.

Concept Manager è una logica variabile per localizzare parole e frasi comunemente utilizzate nello spam ed utilizza tecniche di riconoscimento del linguaggio naturale per identificare il contesto del messaggio. Nemx Software descrive questo tipo di approccio come superiore a quello bayesiano; tra le altre cose, non viene ingannato dalle presenza di parole generiche. Nemx Software aggiorna mensilmente le definizioni delle Concept Manager Policy. La versione che ho provato include 64 livelli di spam, 14 dei quali relativi alla pornografia. È possibile abilitare i livelli selettivamente.

Power Tools include le estensioni Microsoft Intelligent Message Filter (IMF), un filtro antispam disponibile per Exchange Server 2003. IMF consente di personalizzare le azioni a seconda del server, del gruppo, o della mailbox. L'IMF Manager di Nemx Software è disponibile come componente standalone.

Power Tools consente di configurare un insieme personalizzato di azioni, in aggiunta alle azioni standard Delete e Quarantine. È possibile configurare regole personalizzate che avviano azioni personalizzate ed applicare queste regole sia al traffico in entrata che a quello in uscita. È possibile anche registrare questa attività in file CSV per eseguirne una analisi.

Come gli altri prodotti, anche Power Tools è semplice da installare. Viene distribuito come un singolo file eseguibile che viene posto ed eseguito all'interno della directory BIN di un server Exchange. L'interfaccia amministrativa di Power Tools si inserisce in Exchange Administrator o in System manager aggiungendovi il proprio relativo collegamento.

Power Tools è leggermente più costoso degli altri prodotti ma offre alcune caratteristiche uniche, può includere una grande varietà di funzionalità, ed è legato ad una flessibile e semplice interfaccia amministrativa.

Power Tools for Exchange-Internet Edition

Contatto: Nemx Software

Web: <http://www.nemx.com>

Prezzo: \$795 per i moduli e il connettore Spam and Content ; \$795 per la sottoscrizione antivirus per 1 anno, \$1095 per 2 anni

Riepilogo

Pro: Caratteristiche uniche; design modulare che consente di acquistare le sole caratteristiche di cui si ha bisogno; una certa flessibilità nella configurazione che non ne rende difficile l'uso

Contro: Nessun sistema di reportistica incluso

Commento:

Power Tools è leggermente più costoso degli altri prodotti ma offre alcune caratteristiche uniche.

Microsoft Intelligent Message Filter

Microsoft Intelligent Message Filter è un add-in liberamente scaricabile per i server Exchange 2003 non in cluster. Usa un algoritmo adattivo simile ai filtri Bayesiani per distinguere lo spam dai messaggi legittimi. Quando ha sviluppato IMF, Microsoft ha utilizzato messaggi di email che i suoi business partner avevano classificato come spam per creare una base di dati che consentisse a IMF di effettuare la distinzione.

IMF esamina i messaggi appena vengono inseriti nei server Exchange, ma solo se il messaggio non viene filtrato da altri filtri sulla connessione, sulle cartelle o sul mittente. IMF non analizza gli archivi di messaggi esistenti. IMF assegna ad ogni messaggio un numero indicante la probabilità che il messaggio sia uno spam - questo sistema costituisce uno Spam Confident Level (SCL).

Quando si implementa IMF, gli amministratori specificano un valore di soglia Gateway Threshold SCL, che viene usato da IMF per determinare se i messaggi devono essere cancellati, rifiutati, archiviati o inoltrati. È possibile impostare un valore di questo tipo che può essere utilizzato da Outlook Web Access per Exchange Server 2003 e Outlook 2003 per determinare se un messaggio deve essere inviato alla cartella Posta Indesiderata o alla cartella Posta in arrivo dell'utente. Le azioni impostate per Outlook 2003 sovrascrivono l'SCL.

Gli amministratori possono configurare IMF utilizzando la pagina Properties in Exchange System Manager. È possibile installare questi componenti in una workstation per l'amministrazione remota.

Per default, IMF non analizza i messaggi provenienti da mittenti autenticati o archivia messaggi che non vengono inviati da utenti ma piuttosto li salva per una analisi da parte degli amministratori. È possibile sovrascrivere le impostazioni di default modificando il registro.

IMF registra gli eventi sull'event log Application di Windows Server e rende disponibili dei contatori per le prestazioni con il System Monitor. Gli utilizzatori di Microsoft Operations Manager (MOM) possono scaricare il Exchange Intelligent Message Filter Management Pack e aggiungere il monitoraggio IMF al MOM. Per la maggior parte dell'utilizzo effettivo di IMF, Microsoft suggerisce di controllare la distribuzione dei SCL assegnati ai messaggi per determinare i propri valori di soglia.

Commento finale

Personalmente ho selezionato sia GFI Mail Essential per Microsoft Exchange sia Nemx Power Tools come scelta dell'editore.

Entrambi offrono una gran varietà di tecnologie di filtraggio. Entrambi possiedono notevoli opzioni che consentono di personalizzare il prodotto a seconda delle proprie necessità, e tutte queste opzioni sono sempre semplici da configurare. Ogni prodotto ha le sue qualità. MailEssentials supporta i filtri bayesiani e include un componente di reportistica. Power Tools include la tecnologia di rilevamento proprietaria Concept Filtering e una interfaccia di gestione raggiungibile attraverso Exchange System Manager.

Entrambi i prodotti offrono caratteristiche aggiuntive che non si riferiscono al filtro antispam, che aggiungono valore al prodotto sotto lo stesso ombrello amministrativo. ▲

John Green