WHITE PAPER

Come tenere lontano lo spam dalla rete

Quali funzionalità richiedere ad una tecnologia anti-spam

Questa white paper, una guida per il cliente di software anti-spam, evidenzia le caratteristiche principali da cercare in un software anti-spam e perché.

Introduzione

La presente white paper aiuta ad identificare le caratteristiche principali necessarie per gestire lo spam.

La crescita e il costo dello spam

Radicati Group, una società di ricerche americana, stima che il 52% del traffico di email complessivo attuale sia costituito da posta spam e prevede che tale percentuale raggiungerà il 70% entro il 2007. Analogamente, l'Unione Europea stima che il 50% di tutti i messaggi di posta elettronica sia costituito da spam.

Ciò significa che i dipendenti devono dedicare parte del loro orario di lavoro alla gestione dello spam, il che determina una riduzione della produttività (ed un contestuale aumento della frustrazione!). La perdita di produttività rappresenta il costo principale dello spam, soprattutto perché, quotidianamente, si ricevono così tante email di spam. Bisogna inoltre considerare il costo relativo alla larghezza di banda sprecata dallo spam e gli ulteriori costi di archiviazione e infrastruttura della rete. Inoltre, considerando il flusso di spam e la sua rimozione, nella fretta di cancellare il contenuto della propria cartella di posta indesiderata, può accadere di eliminare un messaggio importante finito accidentalmente nella posta indesiderata.

Ferris Research ha calcolato che se un dipendente ricevesse soltanto 5 email di spam al giorno e dedicasse 30 secondi ad ognuna, sprecherebbe 15 ore all'anno a causa della posta indesiderata; moltiplicando tale valore per la paga oraria di ciascun dipendente dell'azienda, si avrà un'idea molto contenuta del costo dello spam per la vostra organizzazione. Radicati Group ha riportato che, nel 2003, lo spam è costato al settore informatico circa 49 dollari USA per casella postale e prevede che raggiungerà la considerevole somma di 257 dollari USA per casella postale nel 2007.

È indispensabile porre fine allo spam, in modo da risparmiare tempo, denaro e larghezza di banda. Un passo in questa direzione consiste nel consigliare agli utenti della propria rete di non divulgare il proprio indirizzo email (per esempio non inviare posta ad una message board, ecc.) Tuttavia, oltre al buon senso, è possibile utilizzare un efficace strumento anti-spam a livello del server.

Scegliere il corretto software anti-spam

Sul mercato sono disponibili molti pacchetti software che aiutano a combattere lo spam, ma non tutti sono abbastanza incisivi nella gestione dello spam. Di seguito vengono trattati alcuni argomenti e funzionalità da richiedere.

Basato sul server oppure basato sul client?

Per combattere lo spam a livello di client è necessario molto più tempo rispetto ad eseguire la stessa operazione a livello di server. Richiede l'impiego di software anti-spam su tutte le stazioni di lavoro della propria rete e di recarsi spesso presso questi computer per aggiornare le regole anti-spam su ciascuno di loro. Inoltre, l'infrastruttura email sarebbe gravata dallo spam, poiché gli archivi dei messaggi del server si riempirebbero di email inutili in attesa di cancellazione. In più, verrebbe sprecato anche il tempo degli utenti, che dovrebbero identificare lo spam oppure aggiornare il proprio set di regole: esattamente quello che si cerca di evitare in questo tentativo di bloccare lo spam!

Inoltre, con un software anti-spam a livello di client, non si dispone delle informazioni e delle risorse offerte da quello basato sul server, come la possibilità di eseguire controlli sul server mittente, ad esempio. Per bloccare lo spam in maniera efficace, è necessario un prodotto anti-spam basato sul server in quanto offre i seguenti vantaggi:

1. L'installazione a livello del gateway elimina le seccature d'impiego e amministrazione tipiche dei prodotti basati sul desktop.
2. È molto più economico da acquistare.
3. Impedisce allo spam perfino di entrare nella propria infrastruttura di posta elettronica, perciò gli archivi email non risultano più sommersi di spam.
4. Il server anti-spam basato sul server dispone di un numero maggiore di informazioni e può quindi fare di più per rilevare lo spam in modo efficace.

Tecnologia basata sul filtraggio Bayesiano

Alcuni anni fa, la maggior parte dei prodotti anti-spam utilizzava semplicemente un elenco di parole chiave per identificare lo spam. L'uso di un valido insieme di parole chiave era in grado di catturare molto spam. Tuttavia, oggigiorno la cattura dello spam basata su parole chiave genera troppi falsi positivi e richiede troppi aggiornamenti manuali.

Il filtro Bayesiano è oggi largamente riconosciuto dai migliori esperti e dalle principali pubblicazioni come il metodo più efficace per catturare lo spam. Un filtro Bayesiano utilizza un approccio matematico basato sullo spam conosciuto e sulla posta valida (ham). Ciò costituisce un enorme vantaggio rispetto alla vecchia tecnologia anti-spam che, invece, cerca parole chiave o conta sulla capacità di scaricare le firme dello spam conosciuto. Ulteriori informazioni sul filtraggio Bayesiano sono disponibili nella white paper intitolata *Why Bayesian filtering is the most effective anti-spam technology*, all'indirizzo web: http://www.gfi-

italia.com/italia/whitepapers/why-bayesian-filtering.pdf.

Ecco una sintesi dei vantaggi offerti dal filtraggio Bayesiano:

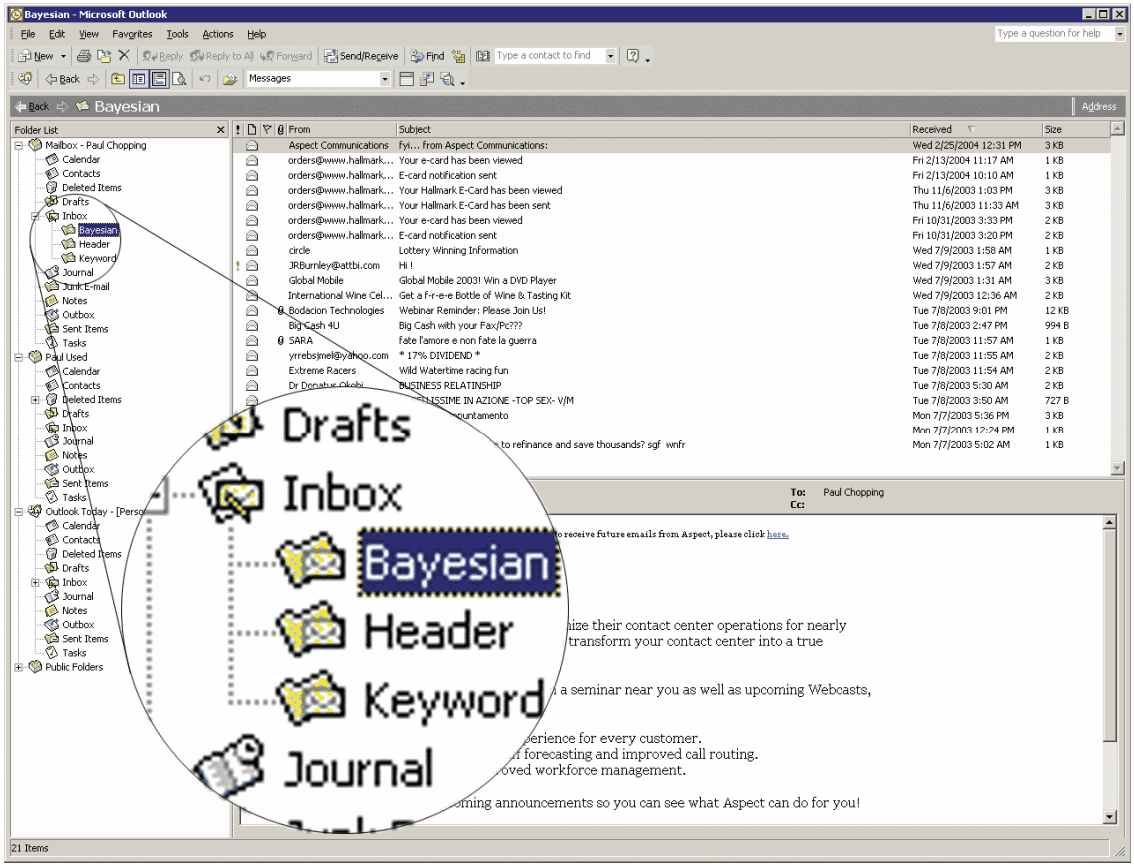
1. controllo del messaggio di spam completo e non solo delle parole chiave o delle firme di spam conosciute
2. apprendimento dalla posta in uscita (ham) con forte riduzione dei falsi positivi
3. adattamento costante automatico grazie all'apprendimento del nuovo spam e della nuova posta valida
4. dataset unico per ogni azienda, tale da non poter essere superato
5. multilingue ed internazionale.

Un file di dati ham su misura per il filtro Bayesiano

È fondamentale che il filtro Bayesiano utilizzi un dataset personalizzato in base alla propria installazione: i dati ham DEVONO essere raccolti dalla posta in uscita (in questo modo, il filtro Bayesiano è adattato alle esigenze dell'aziende grazie ad un periodo di addestramento iniziale). Alcuni software anti-spam utilizzano un file generico di dati ham fornito insieme al prodotto. Un esempio è il filtro anti-spam di Outlook o quello di Exchange Server Internet Message. Benché tale tecnologia non richieda il periodo iniziale di apprendimento, presenta 2 grossi difetti:

1. Il file di dati ham è disponibile pubblicamente e può quindi essere "piratato" da spammer professionisti e superato. Se il file di dati ham è esclusivo della propria azienda, allora piratare il file di dati ham risulta inutile. Ad esempio, esistono hack disponibili a superare il filtro anti-spam di Microsoft Outlook 2003.

2. In secondo luogo, il file di dati ham è generico e, in quanto non adattato alle esigenze di una data azienda, non può essere efficace quanto uno personalizzato. Si riscontrerà una notevole percentuale di falsi positivi. Per esempio, un istituto finanziario può utilizzare il termine "mutuo" molte volte, pertanto l'utilizzo di un file di dati ham generico può comportare molti falsi positivi.



La revisione dello spam diventa facile se viene archiviato in una sottocartella della casella postale di un utente

Un file di dati spam per il filtro Bayesiano aggiornato automaticamente

Il software anti-spam deve aggiornare costantemente il file di dati spam del filtro Bayesiano con lo spam più recente. Questo assicura che il filtro Bayesiano sia a conoscenza dei trucchi di spam più recenti, producendo un'elevata percentuale di individuazione dello spam (nota: tale livello si raggiunge al termine dell'iniziale periodo di apprendimento di due settimane richiesto). Scegliete un prodotto anti-spam che raccolga i dati spam per voi e vi consenta di scaricare automaticamente questi aggiornamenti!

Gestione dello spam per una revisione efficace dello stesso

Connessa alla tecnologia anti-spam vi è la possibilità di incorrere in falsi positivi, ossia, la posta viene etichettata come spam anche quando non lo è veramente. Pertanto, un buon software anti-spam deve offrire agli utenti un metodo semplice per rivedere la posta contrassegnata come spam in modo veloce ed efficace.

Per evitare all'amministratore perdite di tempo e seccature, un software anti-spam deve comprendere un'opzione che consenta di indirizzare la posta identificata come spam in cartelle

di posta indesiderata degli utenti individuali. Inoltre, il software deve ordinare lo spam in cartelle diverse in base allo strumento che l'ha individuato come tale. Il rapido accesso a posta contrassegnata come spam aiuta notevolmente l'utente a rivedere il proprio spam in maniera efficace. Alcuni prodotti anti-spam richiedono all'utente di collegarsi ad un sistema basato sul web e rivedere i messaggi praticamente uno per uno; questo metodo risulta molto macchinoso per l'utente e conduce alla rara utilizzazione della funzione in futuro.

Whitelist flessibili per ridurre i falsi positivi

Il software anti-spam dovrebbe disporre di un modo efficace per creare ampie whitelist in modo automatico. Le whitelist dovrebbero identificare tutti i partner commerciali validi, affinché la loro posta non sia mai etichettata come spam. Un buon software anti-spam dovrebbe includere la possibilità di creare e aggiornare automaticamente tali whitelist.

Come GFI MailEssentials affronta lo spam

L'approccio di GFI MailEssentials all'individuazione dello spam si basa sui seguenti metodi e tecnologie:

1. **Affronta lo spam a livello di server** - GFI MailEssentials si installa sul vostro Exchange 2000/2003 Server oppure davanti al vostro server di posta (se si utilizza Exchange 5.5 o un altro server di posta). Individua lo spam PRIMA che raggiunga il server di posta. In questo modo, lo spam non influisce sull'infrastruttura di posta elettronica e gli eventuali aggiornamenti di regole di individuazione dello spam vanno impiegati solo sulla macchina GFI MailEssentials. Le whitelist (domini/indirizzi email dai quali si desidera sempre ricevere posta) e le blacklist (domini/indirizzi email dai quali non si desidera ricevere posta) possono essere utilizzate a livello di server.

2. Analizza il contenuto della posta utilizzando il **filtro Bayesiano** i dati ham specifici della propria azienda. I dati spam sono aggiornati automaticamente scaricando i dati spam più recenti dal sito web di GFI. Per ulteriori informazioni sul filtraggio Bayesiano, si legga la white paper al seguente indirizzo: http://www.gfi-italia.com/italia/whitepapers/why-bayesian-filtering.pdf.

3. **Riduce i falsi positivi tramite una whitelist automatica** - GFI MailEssentials contiene uno strumento per la gestione automatica della whitelist in attesa di brevetto. Questa tecnologia esclusiva comporta che tutti i partner commerciali sono aggiunti automaticamente alla propria whitelist, senza la necessità di un'eventuale amministrazione, e la loro posta non passerà nel filtro anti-spam, riducendo fortemente i falsi positivi.

4. **Gestione flessibile dello spam** – Dopo che un messaggio email è stato riconosciuto come spam, può essere inoltrato ad una sottocartella della casella di posta dell'utente. Se trovano qualche email valida (ad esempio, una newsletter che desiderano ricevere), gli

utenti possono aggiungere il mittente alla whitelist.

5. GFI MailEssentials comprende **capacità di ricerca per parola chiave**; in questo modo gli amministratori possono adeguare ulteriormente i propri filtri anti-spam.

6. Per un'ulteriore protezione, il filtraggio Bayesiano è aiutato da un certo numero di **altre tecnologie anti-spam**, compresi l'analisi intelligente dell'intestazione della posta e il controllo dei mittenti rispetto a blacklist personali e pubbliche, quali ORDB o SpamHaus.

Informazioni su GFI

GFI è produttore leader di software per la sicurezza della rete, del contenuto e per la messaggistica. I suoi prodotti principali comprendono: GFI FAXmaker, connettore fax per Exchange e server di posta SMTP; GFI MailSecurity, software per il controllo di contenuto ed exploit della posta elettronica e antivirus; GFI MailEssentials, software anti-spam basato sul server; GFI MailArchiver, soluzione per l'archiviazione della posta elettronica; GFI LANguard Network Security Scanner (N.S.S.), software per la scansione della sicurezza e la gestione delle patch; GFI Network Server Monitor, con il suo invio automatico di avvisi e la correzione di problemi della rete e del server, GFI LANguard Security Event Log Monitor (S.E.L.M.), con la sua scoperta d'intrusione basata sui log degli eventi e la gestione dei log degli eventi di tutta la rete; GFI EndPointSecurity, con il suo controllo di supporti rimovibili su tutta la rete e, infine, GFI WebMonitor, software per il monitoraggio HTTP ed FTP e antivirus per ISA Server. GFI vanta clienti come Microsoft, Telstra, Time Warner Cable, NASA, DHL, Caterpillar, BMW, l'IRS e l'USAF statunitensi. GFI ha uffici negli Stati Uniti, nel Regno Unito, in Germania, Cipro, Romania, Australia e Malta ed opera attraverso una rete mondiale di distribuzione. GFI è Microsoft Gold Certified Partner e ha vinto il premio Partner of the Year di Microsoft Fusion (GEM) Packaged Application. Per ulteriori informazioni su GFI, visitare il sito http://www.gfi-italia.com.