Progettare un'Architettura di Posta Elettronica

Nel mondo internet l'importanza del servizio di posta elettronica è forse seconda al solo servizio Web. In questo articolo illustreremo una architettura che premette di offrire un servizio di posta elettronica con vari elementi che offrano una maggiore sicurezza e fruibilità agli utenti.

Ci occupiamo di disegnare il servizio offerto da un (piccolo) ISP o da una media o grande azienda con un proprio sistema di posta elettronica. In altre parole abbiamo a disposizione:

- alcune macchine da dedicare al servizio di spedizione e ricezione della posta
- un servizio DNS
- un accesso (permanente) ad internet.

In questo articolo non ci occuperemo di disegnare un sistema di sicurezza all'interno del quale installare il sistema di posta, assumeremo che ci sia in una DMZ adeguatamente protetta, ma ci occuperemo solo degli aspetti relativi al servizio di posta elettronica in se.

Dividiamo il servizio di posta elettronica in due fasi, la ricezione della posta e la spedizione della posta. Il diagramma 1 riporta una schema logico del servizio di ricezione della posta.

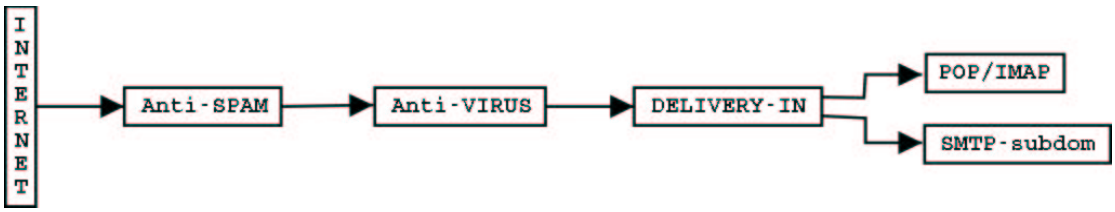

Diagramma 1

Per semplicità assumiamo che ogni step sia svolto da un host indipendente, anche se per sistemi piccoli è possibile implementare tutto il sistema su di un'unica macchina. Avremo perciò

- una prima macchina **Anti-Spam** con l'MX Principale (record DNS che indica che per una lista di domini la posta deve essere inviata a questo indirizzo IP) il cui compito è di filtrare dallo SPAM, o messaggi bulk non richiesti, tutti i messaggi in arrivo; i filtri principali applicati sono di 3 tipi
    1. **DNS-based Block List:** liste di indirizzi IP di host che inviano messaggi SPAM, queste liste sono aggiornate in tempo reale e consultate via un lookup DNS, questo server

rifiuta di ricevere messaggi da questi host

2. **Local Black List:** liste di indirizzi email o IP di host che inviano SPAM, queste liste sono di solito manutenute manualmente
3. **Filtri:** filtri che rifiutano messaggi sulla base di parole chiave contenute nel messaggio stesso (header e/o body), a differenza dei due casi precedenti il messaggio deve essere prima ricevuto e poi applicato il filtro (spesso il filtro viene applicato prima di inviare al server mittente l'OK per la ricezione del messaggio inviando invece "`550 Error: Message content rejected`") questo step può richiedere parecchi cicli di CPU per ogni messaggio

- una seconda macchina che si occupa di applicare i filtri Anti-Virus a tutti i messaggi che hanno passato l'**Anti-Spam;** le firme dei Virus sono mantenute in tempo reale da alcune aziende specializzate; l'apertura di tutti gli attachment e la ricerca in ognuno di esso delle firme dei virus può richiedere molte risorse, a seconda della quantità e della velocità del flusso di messaggi; qualora venga trovato un virus, questo dovrebbe essere parcheggiato in un area apposita del server ed inviato un messaggio al destinatario che nel caso può prelevare ugualmente il messaggio
- una terza macchina che distribuisce e consegna la posta, questa può andare ad altri server **Smtp** che ricevono la posta per sottodomini, o direttamente a caselle **Pop/Imap**; ovviamente gli indirizzi devono essere risolti, ovvero tutti gli alias devono prima essere tradotti nel nome della casella o dell'indirizzo di posta finale.

Gli utenti finali scaricano la posta dalla propria casella **Pop/Imap** (se non locale preferibilmente via SSL) i messaggi sul proprio PC oppure la consultano tramite un'interfaccia WebMail. In ogni caso sul proprio PC vi deve essere installato un Anti-Virus che deve anche essere aggiornato almeno quotidianamente sia per ridondanza ma anche perché la posta non è l'unico veicolo di infezioni. Inoltre agli utenti con un minimo di esperienza è suggerito anche di adottare dei filtri di selezione e anti-spam sui singoli PC, ad esempio i nuovi filtri Bayesiani.

La spedizione della posta è descritta nel diagramma 2 che è più semplice.

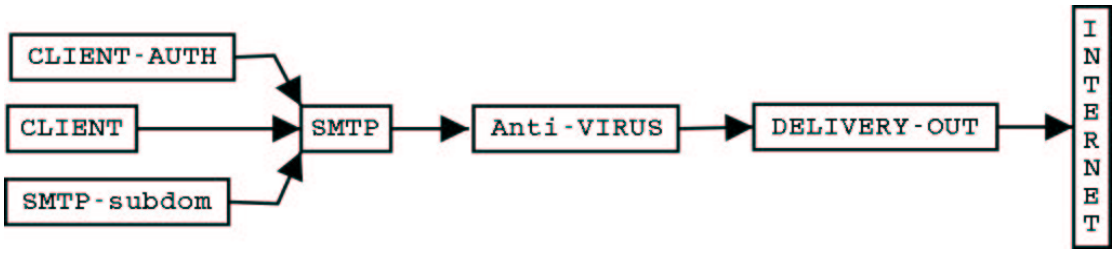

Diagramma 2

In questo diagramma i **Client-Auth** sono degli utenti, di solito con PC portatili in mobilità, autorizzati da un protocollo di autenticazione ad inviare la posta tramite il server **Smtp** anche se l'host da cui si connettono è su di una rete remota con un indirizzo IP non riconosciuto. Infatti il server **Smtp** ha una lista di indirizzi IP (quelli dei **Client**) per i quali accetta di fare `relay`, ovvero di inviare al destinatario esterno i messaggi. Questa White List più la lista dei **Client-Auth** sostituisce logicamente la funzionalità **Anti-Spam**. L'**Anti-Virus** non è obbligatorio, e molti non lo mettono, ma è sicuramente ben visto dalla comunità poiché da buone garanzie che la posta in uscita dal proprio network sia priva di Virus. La macchina che si occupa del **Delivery-Out** è direttamente connessa ad internet, e deve consegnare i messaggi in uscita ad i server che ricevono la posta (DNS MX record) per i destinatari.

I due diagrammi possono essere messi insieme nel diagramma 3.

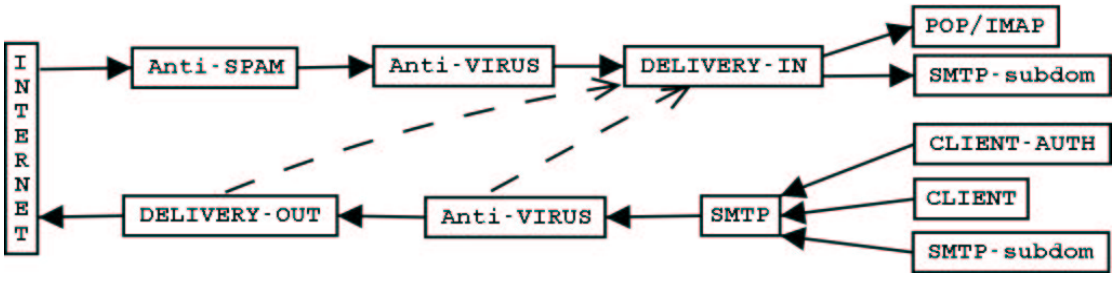

Diagramma 3

Per soluzioni non troppo grandi e ove gli utenti siano ragionevolmente sotto controllo, vista la posizione centrale dell'**Anti-Virus,** questo può essere anche comune ad entrambe le direzioni. In questo caso è anche ovvia la soluzione per la consegna della posta interna, che dall'**Anti-Virus** andrà direttamente al **Delivery-In** verso l'interno invece che verso **Internet**. Se si tengono due

Anti-Virus ed il sistema è piccolo, il **Delivery-Out** può consegnare la posta interna direttamente al **Delivery-In**, visto che in questo caso l'**Anti-Spam** e l'**Anti-Virus** della posta in entrata non sono di fondamentale importanza.

A seconda della quantità di utenti e del tipo di infrastruttura nella quale si implementa il servizio di posta, gli elementi qui descritti possono essere implementati ognuno su di una macchina, nel caso anche con più macchine per servizio in load-balance, od all'estremo opposto tutti sulla stessa macchina.

Un altro aspetto da considerare è l'accesso da/ad internet del servizio di posta elettronica. E' fortemente consigliato limitare l'accesso alle porta 25 TCP sia in entrata che in uscita dal proprio network lungo tutto il perimetro. Si dovrebbe permettere l'accesso da internet verso la porta 25 TCP solo verso il server **Anti-Spam**, e permettere l'uscita verso internet porta 25 TCP solo al server **Delivery-Out**. A parte proteggere host interni i cui servizi di posta non devono essere accessibili all'esterno, questo previene che host interni possano essere utilizzati dall'esterno per effettuare `relay` non autorizzati di messaggi di posta, di solito ai fini di SPAM. Inoltre bloccando la porta 25 TCP in uscita, si obbligano tutti i propri utenti a passare attraverso l'**Anti-Virus,** limitando la possibilità che macchine infette o compromesse nella propria rete possano diventare causa di attacchi verso terzi, ridistribuendo SPAM od agendo quali proxy. Nelle reti odierne è di fondamentale importanza per la sicurezza che tutto il traffico di posta elettronica in entrata ed uscita dalla propria rete passi solo attraverso i sistemi centrali. Inoltre spesso vengono configurate macchine di riserva con MX Secondari per backup o load-balancing del server principale. Purtroppo in molte configurazioni queste macchine di riserva non hanno le stesse difese (Anti-Virus, Anti-Spam ecc.) di quelle principali, e vengono spesso utilizzate per l'invio di SPAM, virus ecc. Nella progettazione del servizio va perciò assicurato che qualunque sia il percorso dei messaggi di posta, la sicurezza sia sempre la stessa.

L'implementazione pratica di tale architettura richiede comunque un approfondimento dell'argomento, la scelta delle tecnologie, un corretto dimensionamento delle macchine e del software, e l'inserimento del progetto all'interno delle più generali politiche di sicurezza dell'organizzazione, sia tecniche che procedurali.

L'autore desidera ringraziare Furio Ercolessi (Coordinatore dei Servizi di Messaggistica di Spin Srl) per la collaborazione data alla realizzazione dell'articolo.

Andrea Pasquinucci
Consulente di Sicurezza Informatica
pasquinucci@ucci.it

Riferimenti Bibliografici:

[1] Informazioni su SPAM: http://www.mail-abuse.org/, http://www.spamhaus.org/ ed altre risorse on-line

[2] Filtri Bayesiani: http://www.paulgraham.com/spam.html (anche in http://www.pacificavc.com/blog/2003/02/10.html)

[3] RFC: 2821, 876, 1651, 1652, 1869, 1870, 1891, 1939, 1957, 1985, 2505, 2554, 2595, 2654, 2683, 2852, 3207.