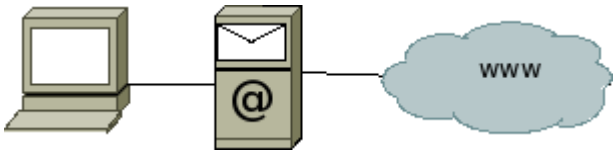
Una implementazione sicura per il mailing

Il servizio di mailing è oggi una parte irrinunciabile del web come lo conosciamo ed è parte strutturale del processo di comunicazione sia interpersonale sia aziendale. Ma il servizio porta con se una serie di problematiche di sicurezza che gli amministratori di sistema devono conoscere ed affrontare. Qui si proporrà una modalità di implementazione sicura per una struttura di mailing.

Nella sua forma di base un sistema di posta è costituito da un client collegato ad un server che a sua volta è collegato con il web e può attraverso di esso scambiare messaggi con altri server di posta.



Già in questa forma è possibile evidenziare un certo numero di possibili problemi di sicurezza in quanto il server, essendo connesso ad internet, è suscettibile di vari tipi di intrusioni e manomissioni in quantità inversamente proporzionale alla qualità del lavoro del sistemista che lo ha configurato.

Nella realtà le cose sono peggiori in quanto il client, nel caso più comune, non comunica direttamente con il server ma vi accede attraverso il web esponendosi a sua volta a vari rischi di sicurezza.

A peggiorare la cosa le mail sono spesso portatrici di virus in allegato; virus che utenti distratti e programmi di posta mal configurati (o mal costruiti) diffondono a velocità impressionante.

Vedremo quindi come è possibile tramite strumenti open source realizzare una struttura per il mailing e come è possibile migliorare il progetto per minimizzare i vari problemi che si possono incontrare.

Corretta configurazione del mail server

Si ritiene superfluo in questo contesto spiegare se, e perché, è opportuno scegliere software Open Source, ormai su questo argomento sono stati scritti interi volumi sia pro che contro. Ci si limiterà a riportare che esistono dei programmi Open Source che oramai sono degli standard consolidati e che, data la modalità di sviluppo, rendono disponibili le patch di sicurezza in tempi brevi.

Per abitudine l'autore di questo articolo utilizza sendmail ma un programma ancora più sicuro potrebbe essere postfix che a detta di molti è un po più snello e facile da configurare.

A differenza di quanto ci si poteva aspettare dal titolo del capitolo, qui non verrà illustrata alcuna specifica configurazione. E' corretto ritenere che chi ha sviluppato il software e ne ha scritto le istruzioni di installazione siano le persone più competenti per esporre queste procedure. Per cui l'invito è di investire del tempo nella lettura dei manuali del programma scelto. Ci si limiterà quindi ad esporre dei punti procedurali evidenziando attività che troppo spesso vengono trascurate od omesse.

Le attività minime consigliate per la messa in sicurezza della macchina sono:

1. L'attivazione del firewall locale alla macchina in modo da lasciare aperte solo le porte strettamente necessarie. Questa attività è indispensabile se non vi è alcun altro firewall presente ma potrebbe sembrare inutile qualora esista già un firewall. In realtà la piccola precauzione di avere un firewall aggiuntivo potrebbe darvi il tempo necessario a prevenire un intrusione sul server quando il firewall principale venisse compromesso. Questo, ovviamente, a patto di avere installato un sistema di intrusion detection che vi avvisi istantaneamente della compromissione (a questo proposito si veda il punto successivo).
2. L'utilizzo fin dall'inizio un tool di data integrity come ad esempio tripwire, SNORT oppure OSSEC per poter monitorare e individuare modifiche esterne al sistema. La marcatura del sistema, in particolare, è attività da fare subito dopo l'installazione in quanto perde senso se non avete la totale certezza che il sistema non sia già stato compromesso.
3. Qualora sia possibile, limitare al massimo il numero di macchine che possono avere accesso al server in particolare per le modalità di amministrazione. Questo vi permetterò di monitorare più facilmente alcuni tipi di attività/traffico in quanto dovranno provenire solo dalle macchine autorizzate.
4. Eliminare qualsiasi password di default per i vari programmi, eliminare i banner standard dei vari programmi (per rendere più difficile la loro identificazione), etc. Per avere nozioni di base su questo tipo di attività si consiglia la lettura di "Securing and Optimizing Linux-The Ultimate Solution v2.0" di Gerhard Mourani disponibile presso il Linux Documentation Project. Il documento per quanto datato contiene nozioni e informazioni di indubbia utilità e validità.
5. Una volta terminata la configurazione di base testare il sistema con qualche tool di scanning come OpenVAS e/o nmap in modo da determinare che non vi siano vulnerabilità residue. Strumenti come questi sono i primi tool (in ordine di sequenza) utilizzati dai cracker per analizzare un sistema da attaccare, quindi garantirsi che il sistema non sia scoperto a questi strumenti è un buon inizio.

Messo in sicurezza il server vediamo come proseguire...

Firewall

Questa indicazione può sembrare inutile dopo avere realizzato quanto descritto in precedenza ma si consiglia comunque di aggiungere un firewall fra il mail server e internet.

Il firewall non dovrà necessariamente essere un appliance con tale funzionalità, potrebbe essere tranquillamente sostituito con un PC e apposito software, ma, in ogni caso, dovrà essere una macchina dedicata solo a tale utilizzo.

Se desiderate realizzare un firewall software tramite un normale PC, l'Open Source può aiutare con strumenti come m0n0wall o IPCop

Il firewall avrà la funzione di lasciare aperte solo le porte strettamente necessarie per i nostri servizi, servirà per redirigere (NAT) le porte alle varie macchine server (e vedremo in seguito l'utilità di tale funzionalità), avrà la funzione di confondere gli strumenti di scanning rilasciando un fingerprinting non conforme con il servizio, ma soprattutto dovra avere funzioni di logging per poter identificare e verificare a posteriori eventuali tentativi di attacco.

Il log dovrebbe venire inviato ad una macchina remota in modo che non venga alterato in caso di compromissione del firewall. I fondamentalisti della security suggeriscono ancora oggi di riversare il log su una stampante ad aghi con carta in modulo continuo ma, al di là della facile ironia, si può osservare che è un sistema reso obsoleto dalla enorme mole di dati per secondo che viene gestita da un firewall al giorno d'oggi.

Importante potrebbe essere, l' avere a disposizione uno strumento come Logwatch o Logsurfer che permetta la facile comprensione dei log per l'individuazione dei problemi. Sarebbe infatti totalmente inutile raccogliere enormi moli di dati in un log e non avere poi la capacità e gli strumenti per analizzarlo correttamente e facilmente.

antivirus / antispam / greylisting

Si passa quindi a mettere (indirettamente) in sicurezza i client partendo dal presupposto che il mailserver sia pubblico e che l'amministratore potrebbe non sapere nulla dei client che si collegano (è il caso più comune).

Si farà quindi il possibile per eliminare i virus dalle mail in transito, sia in partenza sia in arrivo, dotando la macchina di un buon antivirus capace di frequenti aggiornamenti e di buone prestazioni. In questo caso la spesa è da considerare un investimento quindi mani al portafoglio e si scelga il meglio che ci si può permettere. Uno strumento scadente, infatti, potrebbe penalizzare notevolmente le prestazioni dei sistemi a scapito della loro usabilità.

Lo spam è l'altra grande croce del mailing. Una percentuale enorme delle mail che girano al mondo è spam (ogni cifra citabile può essere messa in discussione ma tutti concordano sul fatto che le spam mail sono decisamente troppe ed in numero superiore alle mail utili). Lo spam può essere ridotto di molto con l'adozione di opportuni filtri antispam.

La soluzione più semplice può essere quella di installare nel server smtp (verrà spiegato più oltre perchè si è scritto server smtp e non mail server) un programma come spamassassin in coppia con MIMEDefang. Questi sono programmi che per fare il loro lavoro generano un elevato carico computazionale quindi l'hardware, che in loro assenza potrebbe essere modesto, non deve essere obsoleto. Inoltre bisogna tenere in considerazione che necessitano di una manutenzione e di una messa a punto sià immediatamente dopo l'installazione, sia (seppure in misura minore) successivamente. Infatti l'analisi di spamassasin si basa sui contenuti delle mail e gli spammer tendono a variare spesso il contenuto per bypassare questi filtri che vanno quindi ritarati. Inoltre potrebbe essere necessario, nella messa a punto iniziale, tenere conto della specificità del mailserver. Se esso, infatti, fosse quello di una azienda farmaceutica le regole che contrassegnano come spam le mail contenenti la parola 'drugs' o similari dovrebbero venire rimosse o perlomeno essere depenalizzate.

Come alternativa il greylisting è un metodo che ha maggiore efficacia, rispetto alla marcatura dello spam effettuata da spamassassin, in quanto rifiuta le mail in ingresso al primo tentativo. Esso si basa sul concetto che le mail "regolari", il cui identificativo viene posto in un elenco detto greylist, verranno reinviate automativamente dal server del mittente (e saranno quindi in seconda battuta accettate dopo averne verificato la presenza in greylist) mentre l'invio dello spam solitamente non viene ripetuto e quindi decade in maniera automatica. Quasi tutti i mailserver più usati implementano funzionalità di greylisting ma non sono attive di default. Si può consultare in merito la pagina con l'elenco delle implementazioni.

Questo metodo, per quanto efficace soffre di un paio di difetti di fondo in quanto

- Introduce un ritardo, dovuto al primo tentativo di invio respinto, che è spesso mal tollerato dagli utenti, soprattutto quando stanno aspettando una determinata mail.
- è sufficiente che lo spam server venga programmato per effettuare almeno due tentativi di invio e la maggior parte dei sistemi di greylist lascerà passare la mail...

queste considerazioni non vogliono scoraggiare dall'utilizzo di questo sistema, che è sicuramente il più efficace, ma semplicemente porre l'accento sui suoi possibili limiti.

Evitare la perdita dei dati

Quanto fin qui illustrato non risolve la possibile perdita di dati che può avvenire a conseguenza di un crash del programma di posta

elettronica (o del disco del client se essa viene scaricata tramite protocollo pop3 sul client stesso). E' vero che il backup di un client è a carico dell'utente ma se siete un amministratore di sistema interno ad un'azienda le problematiche degli utenti (per misteriosi motivi) diventano vostre problematiche.

Questo tipo di problema può essere del tutto eliminato se avete la possibilità di imporre agli utenti l'uso del solo protocollo IMAP, che prevede che la posta rimanga depositata sul server, rimuovendo il servizio POP3 dal server. Ovviamente ciò rappresenta una soluzione solo se il server verrà dotato di adeguato sistema di backup altrimenti avremo solo spostato il problema dal client al server.

Il lato negativo di tale soluzione è dato dal fatto che se la posta risiede sul server gli utenti non potranno consultare le vecchie mail in caso di mancanza di connessione. Ho specificato le vecchie mail in quanto per le mail non ancora visualizzate sia imap che pop3 sono ugualmente inutili in assenza di conessione.

Alcuni client per risolvere la cosa implementano la modalità off-line di IMAP con la quale si ha la possibilità di visualizzare le mail anche se non si è più connessi in quanto le stesse vengono "replicate" sul client ad ogni connessione. Questa soluzione rappresenta probabilmente il compromesso ideale fra le due modalità di funzionamento.

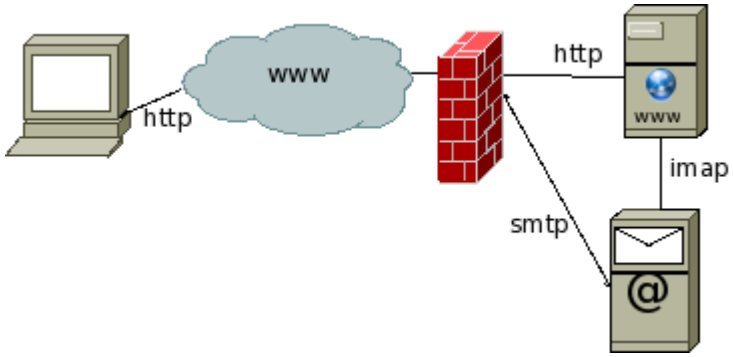
Aumentare la sicurezza

L'utilizzo della webmail

A questo punto, viste le considerazioni di cui sopra, potrebbe essere utile un buon salto di qualità per aumentare la sicurezza introducendo l'utilizzo della webmail.

I programmi di webmail sono di fatto dei siti internet strutturati in modo da replicare le funzionalità dei programmi client di posta elettronica. Possono implementare le sole funzionalità di base come Round Cube o essere integrati con funzionalità di groupware come Horde, giusto per citarne un paio.

Il vantaggio nell'utilizzare una webmail (e solo quella) congiuntamente con un server imap, è dato dal fatto che la macchina che fornisce il servizio di webmail sarà l'unica a collegarsi con il server IMAP (ci si riallaccia a quanto espresso in precedenza sull'opportunita di limitare le macchine connesse al server) permettendo di fatto di aumentare il livello di sicurezza della macchina in cui è stato installato il server imap ed in cui, di fatto, giace la posta.

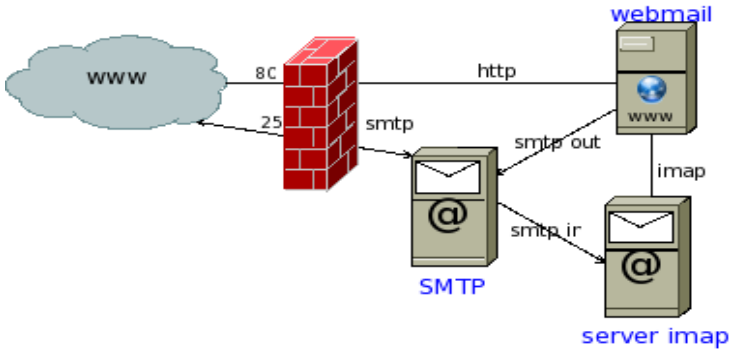


Oltre a ciò risulta evidente l'indubbio vantaggio di poter consultare la propria posta da una qualsiasi postazione connessa a internet.

Tale soluzione non è però adottabile in tutte le aziende in quanto richiede un atto di forza da parte dellìamministratore per imporre a tutti gli utenti l'utilizzo della webmail. Anche una sola eccezione farebbe decadere il vantaggio (in termini di sicurezza) acquisito con tale soluzione.

Separazione del mail-gateway

Un ulteriore passo potrà essere quello di separare tramite un mail-gateway il servizio di invio/ricezione da quello di lettura/gestione della posta.



A questo punto, come da schema ili servizio di posta viene fornito da tre diverse macchine (4 se si separa l'invio dalla ricezione):

- una incaricata alla sola spedizione/ricezione e pulizia (antispam - antivirus) delle mail e che fornirà il servizio SMTP.

- una che fornisce l'interfaccia all'utente per la lettura/scrittura tramite il servizio web HTTP.
- una che fornisce il servizio di deposito delle mail tramite IMAP

Questa separazione netta permette di aumentare le difese anche a livello di firewall e di gestione degli hosts in quanto.

- Dall'esterno saranno visibili solo le porte SMTP e HTTP ma non l'IMAP e questo renderà di fatto invisibile il server IMAP.
- I due servizi visibili dall'esterno punteranno a macchine differenti creando una maggiore confusione in chi effettua un port-scanning e creando un'ulteriore barriera nel caso di compromissione di una delle macchine.
- Si può applicare ai server HTTPD e SMTP una politica di backup separata e molto più blanda di quella applicata al server IMAP in quanto i dati risiedono solo nell'ultima macchina e delle altre dovremo salvare solo la configurazione iniziale e le successive (piccole - in dimensione) modifiche alla stessa.

Risulta ora chiaro il perchè in precedenza si era parlato di SMTP server, in luogo di mail server, in vari punti del testo, volendo evidenziare, in tali contesti, che alcuni accorgimenti sono legati alla specifica macchina deputata al servizio SMTP che non necessariamente è la stessa in cui risiede la posta.

Ulteriori test/attività

Per completare l'opera si possono (devono) effettuare una serie di attività di test che andrebbero poi ripetute periodicamente per valutare le condizioni dei sistemi.

Per prima cosa si verifichi di non avere lasciato aperta la possibilità di effettuare relaying non autorizzato sul mail-gateway. Il relaying è di fatto la capacità di inoltro della posta da parte di un mail server. Se viene lasciata aperta a tutti chiunque può sfruttare il nostro server per un bell'invio massivo di spam. Per verificare se abbiamo lasciato aperta questa condizione è sufficiente sfruttare un servizio on-line come quello messo a disposizione da abuse.net. Per effettuare il test inserire nella pagina web l'indirizzo IP pubblico del server SMTP (normalmente sarà un determinato indirizzo del firewall) e attivare il pulsante "Test for relay".

Come seconda attività sarà bene effettuare un port scanning sull'interfaccia esterna del firewall per capire come vengono "visti" dall'esterno i servizi attivi. Un port scanner serio vi indicherà se sono da coprire delle falle riscontrate come presenti.

La terza attività da fare è di controllare frequentemente nei siti ufficiali l'esistenza di bug nei programmi utilizzati e applicare prontamente le relative patch o eventuali workaround proposti.

Conclusioni

La struttura proposta non è impenetrabile (secondo un vecchio adagio l'unico computer sicuro è quello spento e scollegato dalla rete) ma rafforza notevolmente una installazione ben fatta permettendo di isolare i vari servizi.

La manutenzione di tre macchine al posto di una sola può sembrare inizialmente un notevole aggravio ma in strutture di una certa entità i vantaggi conseguiti andranno velocemente a superare questo problema. Si tenga inoltre presente che oggigiorno i server vengono sempre più spesso realizzati in architettura virtualizzata per cui di fatto si potrebbe avere a che fare con tre distinte macchine logiche risiedenti su un unico server fisico. A tali condizioni quindi non si avrebbe una maggior spesa hardware ma solo un leggero maggior onere di manutenzione di tre distinte macchine a fronte dei vantaggi espressi.

Riferimenti

- Simple Mail Transfer Protocol - RFC 2821
- Sendmail: Installation and operation guide
- Securing and Optimizing Linux-The Ultimate Solution v2.0" di Gerhard Mourani
- The Next Step in the Spam Control War: Greylisting; by Evan Harris
- Open mail relay (su Wikipedia)
- Il punto di vista di John Gilmore sull' open relaying

di Rudi Giacomini Pilon