



SecurityPlus e la scansione antivirus inline

Oltre ai danni diretti, virus e malware sono causa anche di un altro tipo di danno: lo **spreco di tempo e risorse**. Questo avviene perché la maggior parte delle soluzioni per la sicurezza dei contenuti controlla i file dopo il loro arrivo sul mail server o sul PC.

Controllare i file dopo il loro arrivo è preferibile alla totale assenza di protezione, ma è un sistema paragonabile a chi, portatosi un ladro in casa, rimane in attesa di vedere se succede qualcosa! Una soluzione più efficace consiste **nel bloccare l'intruso fuori dall'ingresso**. Dopo tutto, il malware non riesce a creare problemi fino a quando rimane confinato all'esterno del sistema.



Caccia al malware risparmiando tempo ed energie

Rifiutare le email infette

SecurityPlus for MDAemon esegue il controllo antivirus/antimalware per il mail server MDAemon. A partire dalla versione 8 MDAemon può servirsi di SecurityPlus per effettuare scansioni inline dei messaggi, durante ciascuna sessione SMTP.

La scansione inline (cioè in tempo reale) è efficace nel **bloccare il malware** trasmesso via email **direttamente al punto di ingresso in rete**. Quando SecurityPlus rileva un messaggio che costituisce una minaccia alla sicurezza del sistema, MDAemon rifiuta l'email o i suoi allegati: in questo modo stronca il problema sul nascere.

Più sicurezza, meno rischi

Rifiutare l'ingresso ai messaggi infetti contribuisce a **rafforzare la sicurezza del sistema** ed elimina il lavoro e i rischi lega-

ti alla risoluzione dei problemi creati dall'ingresso di malware in rete.

Studiata appositamente per SecurityPlus for MDAemon, la scansione inline controlla il contenuto di ogni messaggio e tutti gli allegati alla ricerca di malware noto o dati sospetti.

La scansione inline protegge gli utenti e la rete **impedendo l'accesso ai messaggi infetti**. Tali messaggi non raggiungeranno mai le code dei messaggi del mail server.

La protezione inline sul mail server è la prima difesa contro i software che tentano di penetrare abusivamente nel sistema.

Risparmiare risorse con la scansione inline

Se un'azienda consente alle email infette di entrare nella rete, si assume anche la responsabilità di neutralizzarle e renderlo noto a eventuali altre parti coinvolte.

In passato MDAemon si serviva esclusivamente di tecniche antivirus implementate come processi offline. In quei casi l'antivirus offline riceveva tutti i messaggi dalle code locali e remote per analizzarli con un processo separato.

Terminata la scansione dei messaggi, il software li rimandava alle code originarie per continuare il processo. Alcuni messaggi potevano essere etichettati come minacce per la sicurezza. Generalmente, le email infette venivano ripulite, messe in quarantena, cancellate o recapitate. Inoltre, il mittente, il destinatario e il postmaster ricevevano un'email di notifica inerente l'eliminazione del virus.

Tutto questo lavoro richiedeva **impiego di risorse elettroniche e tempo delle persone coinvolte**. Vi era inoltre la possibilità che un'email infetta riuscisse ad arrivare, seppur accidentalmente, a destinazione.

Con la scansione inline (cioè in tempo reale) **questo spreco di tempo e risorse non esiste**. Utilizzando la scansione inline, che rifiuta i messaggi infetti, si può azzerare il numero di messaggi di notifica, il che permette di liberare la casella di posta del postmaster dalle centinaia di messaggi di avviso.

La scansione predefinita in MDAemon

La scansione inline è **una caratteristica di MDAemon** e si avvale di SecurityPlus for MDAemon. Sebbene in teoria possa abbassare le prestazioni del mail server, la scansione inline garantisce un notevole rendimento in MDAemon con un impatto limitato sulle prestazioni, tanto che Alt-N ha impostato la scansione inline come **metodo di scansione predefinito**.

La scansione offline è comunque ancora disponibile; ed è anche utilizzata per i messaggi che eccedono una dimensione specificata dall'utente, superata la quale non si applica la scansione inline.

L'aggiornamento delle firme

Come la scansione offline, anche quella inline riconosce il possibile malware ricercando le *firme* (o *segnature*) degli esem-

plari conosciuti.

Per facilitare il riconoscimento del malware più recente, SecurityPlus for MDAemon si avvale anche della tecnologia euristica che analizza i messaggi e gli allegati confrontandoli con regole basate su modelli costruiti analizzando email infette.

Aggiornare le segnature è l'aspetto più importante della manutenzione di SecurityPlus for MDAemon. Per impostazione predefinita, SecurityPlus **ricerca quotidianamente gli aggiornamenti**, ma questa opzione è modificabile secondo le proprie esigenze.

Inoltre, quando si possiede una licenza per SecurityPlus ci si può iscrivere gratuitamente al servizio di segnalazione di aggiornamenti urgenti. Quando compare un nuovo malware particolarmente pericoloso, Alt-N invia a SecurityPlus un messaggio che ne sollecita l'aggiornamento, e il software si aggiorna automaticamente.

Uno sviluppo continuo

La scansione inline rappresenta lo sviluppo più recente nella "lotta" che MDAemon porta instancabilmente avanti per ridurre la quantità di malware che raggiunge gli utenti attraverso la posta elettronica.

Il continuo sviluppo è indispensabile, in quanto chi crea malware escogita nuovi meccanismi di propagazione, difficili da intercettare. **La lotta al malware richiede una strategia continua e approfondita**: non è più sufficiente installare un antivirus e dimenticarsi per sempre del problema.

SecurityPlus for MDAemon aiuta a rilevare e bloccare le minacce diffuse attraverso la posta elettronica, ma deve essere considerato come una delle molte difese da implementare contro i programmi dannosi.

SecurityPlus for MDAemon non sostituisce ma affianca, rafforzandole, le applicazioni per la sicurezza installate sui singoli PC.

Achab S.r.l. - Piazza Cinque Giornate, 4 - 20129 Milano
Tel: 02 54108204 - Fax: 02 5461894 - <http://www.achab.it>
Informazioni commerciali: sales@achab.it
Informazioni tecniche: supporto@achab.it