

Symbolic, gestire i log in modo centralizzato e semplice

Con Security Threat Response Managers di Juniper Networks si superano le criticità nella gestione di log eterogenei.



L'appliance STRM5000 di Juniper Networks

I responsabili IT e i tecnici che si occupano di sicurezza di rete sono sicuramente a conoscenza del provvedimento emanato dal Garante della Privacy nel novembre del 2008 in materia di protezione dei dati personali. Ma al di là della normativa, si può affermare senza tema di smentita che la problematica è molto sentita e di particolare attualità. Tra i vari articoli che disciplinano le “misure minime di sicurezza e protezione dei dati”, il Garante si è pronunciato in materia di registrazione degli accessi.

In particolare, il paragrafo F dichiara: “Devono essere adottati sistemi idonei alla registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici da parte degli amministratori di sistema.”

Tre punti chiave sui log

In merito alla normativa appena citata, tre sono i punti chiave relativi ai log: inalterabilità, ovvero non sono consentite manomissioni o modifiche anche accidentali; completezza, nel senso che i log devono comprendere ogni riferimento dell'accesso (date, risorse utilizzate, durata, ecc.,...); i log devono essere conservati per un congruo periodo che viene indicato come non inferiore ai sei mesi.

La prima criticità per un amministratore di rete è dover gestire

log in ambienti eterogenei come ad esempio, server, device di rete, database e altro ancora. Ognuno di essi esporta e scrive i propri log con modalità differenti, senza un modello standard. Questo porta alla seconda criticità, ovvero rendere tutti i dati salvati inalterabili in modo certo.

La soluzione

Tra le varie soluzioni finalizzate a soddisfare i requisiti del Garante, Symbolic propone Security Threat Response Managers (STRM), l'appliance di Log Management e Network Behavior Analysis di Juniper Networks.

A differenza di molti altri prodotti presenti sul mercato, STRM è in grado di riconoscere e normalizzare log provenienti da piattaforme totalmente differenti e di vendor eterogenei (come firewall, database, server, applicazioni) permettendo agli amministratori di avere un unico punto di store.

Ogni informazione inoltre, può essere salvata in modo sicuro mediante la scrittura del loro hash su disco, garantendone l'inalterabilità. Infine, STRM può salvare i dati sia sui propri dischi sia su sistemi di archiviazione esterni come IPSAN con iSCSI e NAS con NFS.

L'appliance è totalmente configurabile attraverso un'interfaccia di amministrazione via web e consente di gestire eventi e flow

della rete, correlare i dati raccolti e permette agli amministratori di rete di rilevare attacchi e minacce.

Symbolic Gray Program

Oltre a ciò, Symbolic propone un programma di affiliazione ai VAR e System Integrator interessati all'acquisizione di competenze di alto profilo – sia di natura tecnica che commerciale – su tutta la gamma delle soluzioni Juniper Networks.

Il programma prevede una serie di percorsi formativi e attività di laboratorio, oltre che di supporto marketing e vendita, nell'obiettivo di fornire un know-how specifico sulle soluzioni SSG, SA, SRX e STRM. Per i partner che aderiranno sono previsti inoltre vantaggi commerciali, consulenza on-site e supporto tecnico di primo e secondo livello.

www.symbolic.it

A.C.R.