

Sicurezza fisica e logica gestita centralmente

RODOLFO FALCONE
Amministratore Delegato –
Communication Valley Reply



Parlando di sicurezza informatica o, per meglio dire, delle informazioni, è comune pensare a quella che, in realtà, è solo una singola faccia della medaglia: la *sicurezza logica*. Firewall, antivirus, sistemi IDS e IPS sono ormai concetti che ogni CSO o amministratore di sistema conosce ed utilizza quotidianamente. I dati raccolti da questi diversi sistemi, poi, sono spesso raccolti e analizzati tramite un sistema SIEM (*System Information and Event Management*), che consente di creare regole di correlazione che portino allo scatto di un allarme nel momento in cui si verificano determinate condizioni.

È però importante notare che, spesso e volentieri, la sicurezza logica non è sufficiente a garantire la sicurezza delle informazioni preziose per l'azienda: è quindi pratica comune adottare, al fianco delle tecnologie descritte in precedenza, anche misure di *sicurezza fisica*, come rilevatori di presenza, video-sorveglianza, sensori anti-intrusione e così via.

Se è vero che questi sistemi di sicurezza fisica sono quasi sempre gestiti in modalità remota, proprio come avviene per i corrispettivi dispositivi di sicurezza logica, è altresì vero che solo raramente si procede ad una corretta integrazione di questi sistemi, probabilmente perché si fatica a comprendere le potenzialità di una loro mutua correlazione.

Si pensi, per esempio, a un sistema in grado di correlare tra loro informazioni eterogenee quali l'utilizzo di un badge associato ad un determinato utente per l'ingresso in un'area critica dell'azienda, l'accesso da parte dello stesso utente ad un server e il successivo tentativo di acquisire il controllo del server, per esempio attraverso un *exploit*.

Un sistema di monitoraggio di questo tipo può essere visto come una macchina a stati, in cui ogni evento generato dallo stesso utente causa l'innalzamento di un *indice di pericolosità* dell'evento correlato: quando questo indice raggiunge una soglia prefissata, sarà generato un allarme che potrà portare all'identificazione dell'utente malintenzionato e al



blocco dell'attacco in corso.

Immagini raccolte dal sistema di videosorveglianza possono completare l'informazione, consentendo così di verificare la corrispondenza tra badge, utenza e immagine della persona che ha tentato l'attacco.

Anche l'orario di accesso può dare informazioni utili, se molto lontano dai normali orari lavorativi dell'utente e magari in violazione di specifiche policy aziendali.

Naturalmente, per poter elaborare politiche di *alerting* efficaci, è necessario che lo sforzo del progettista si concentri sull'individuazione dell'insieme delle policy di sicurezza, secondo i parametri classici già noti: classificazione asset e loro valore, definizione delle restrizioni all'accesso (livelli di autorizzazione, orari di fruizione, ecc.) e individuazione delle misure di sicurezza accessorie.

Una volta fatto questo, sarà possibile progettare i meccanismi che consentano di individuare le anomalie e di assegnare a ciascuna un livello di pericolosità. La correlazione delle varie anomalie e la somma dei pesi parziali darà una misura efficace e - quel che più conta - in tempo reale della gravità di una minaccia, consentendo l'immediato innesco delle necessarie contromisure.

Dopo questo studio preliminare, l'implementazione degli allarmi all'interno del SIEM farà uso degli stessi meccanismi già in atto per i dispositivi di sicurezza logica: basterà realizzare il collegamento tra i dispositivi e il SIEM, eventualmente implementando o migliorando le interfacce di raccolta log dai vari dispositivi che dovessero risultare lacunose o assenti. Il passo successivo consiste nel correlare tra loro gli eventi di sicurezza fisica e logica secondo le modalità definite nello studio preliminare, ma questa operazione non comporta particolari studi, in quanto le tecnologie utilizzate sono di norma già familiari a chi si occupa di sicurezza logica.

I moderni sistemi di sicurezza fisica, soprattutto quelli inerenti il controllo degli accessi e la videosorve-

glianza, stanno infatti convergendo sempre di più verso l'utilizzo di protocolli di comunicazione standardizzati, basati quasi sempre su TCP/IP e su formati sempre più comuni, come XML o SOAP: questo fattore consente quindi una rapida ed efficace integrazione di questi dispositivi nei moderni SIEM.

Concludendo, per implementare un sistema per il controllo congiunto della sicurezza logica e fisica, si dovranno considerare i seguenti aspetti:

- Nel caso in cui un'azienda sia già dotata di un impianto per la sicurezza logica e di un SIEM, il costo di realizzazione del sistema integrato è composto esclusivamente dai costi di progettazione e realizzazione dell'impianto di sicurezza fisica e dai costi di realizzazione degli eventuali strumenti di comunicazione tra questo e il SIEM pre-esistente; i costi di setup degli allarmi sono invece limitati in quanto sfruttano competenze già acquisite e tecnologie già disponibili.
- Nel caso in cui un'azienda non sia dotata di alcun tipo di impianto di sicurezza, la progettazione congiunta dei due sistemi di sicurezza fisica e logica consente un abbattimento dei costi in quanto la fase di progettazione può e deve essere completamente integrata.
- I costi di gestione, manutenzione, tuning e ottimizzazione dell'impianto finale sono ridotti al minimo dal momento che il personale che si occupa dei due diversi settori è in realtà lo stesso, essendo questi fusi tra loro senza soluzione di continuità.

L'approccio integrato consente di raggiungere livelli di tuning molto raffinati; combinando differenti tecnologie, infatti, si riducono all'osso l'incidenza dei falsi positivi, che di per sé rappresentano l'onere maggiore per chi deve gestire e monitorare il sistema, oltre che dei falsi negativi, i quali rappresentano il maggior costo per l'azienda.

Ma soprattutto contribuisce ad innalzare in maniera sensibile il livello di controllo globale dell'azienda stessa e dei suoi beni di maggior valore, siano essi fisici o intellettuali. ■