

I VANTAGGI DI UNA VALIDA STRATEGIA DATI BASATA SU STORAGE AREA NETWORK

di Tino Prato- Country Manager Italia - Brocade

La centralità delle informazioni ai fini del business è oggi più che mai vitale. E così è la loro protezione dalle minacce, interne o esterne, alla sicurezza. Ma da dove cominciare? La sfida inizia nella Storage Area Network (SAN), dove risiede la maggior parte dei dati aziendali, e da dove chi si occupa di storage deve agire per implementare e gestire una robusta strategia di sicurezza dei dati basata su fabric. Se si parte dal cuore dell'organizzazione, mantenere l'integrità dei dati distribuiti lungo l'intera l'impresa diventa molto più fattibile. Nonostante ci siano molte disposizioni normative, sia governative sia di settore, su come gestire e proteggere le informazioni personali, le norme non dovrebbero essere la sola spinta alla sicurezza dei dati. Gli amministratori storage necessitano di lavorare con il dirigente dell'information security non solo per rispettare tali regolamenti, ma soprattutto per mantenere protetti i clienti, le aziende, i dipendenti e le informazioni (sia dalle minacce interne che esterne), minimizzando il rischio di non-compliance dell'organizzazione stessa.

La SAN, dove la maggior parte dei dati aziendali risiede, è già un ambiente sicuro in se stesso. È gestita in modo centralizzato e supporta praticamente ogni aspetto del data center (server, workstation, ambiente di backup) rendendolo l'ambiente ideale per standardizzare e consolidare una strategia di sicurezza globale. Tuttavia, bisogna chiedersi se una strategia di sicurezza basata su fabric può avere riflessi negativi sulla produttività, anche se non è facile rispondere a questa domanda. Si prenda per esempio l'enigma di come permettere ai dipendenti di lavorare da remoto (utilizzando laptop, PDA oppure di archiviazione mobili), garantendo, però, la sicurezza delle informazioni. I livelli di servizio impongono che l'IT consenta alle persone di svolgere il proprio lavoro nel modo più efficiente possibile, ma chi si occupa di storage ha anche la responsabilità di proteggere l'organizzazione e le informazioni dalle minacce alla sicurezza. Ma spesso, in nome del "qualsiasi cosa pur di avere il lavoro fatto", la sicurezza finisce trascurata.

Spetta all'IT lavorare con le persone di business per sviluppare, applicare e aggiornare policy di sicurezza in grado di proteggere i dati senza impatti negativi sulla produttività degli utenti. La strategia deve inglobare una soluzione completa che protegga i dati aziendali in tutto la storage area network. In passato, molti hanno implementato soluzioni software di sicurezza con diversi livelli di efficacia nell'individuare e arrestare le violazioni alla sicurezza nello storage fabric, ma si trattava di soluzioni molto esigenti in termini di spazio storage, di utilizzo della Cpu e di banda di rete. Oggi è generalmente accettato che l'intelligence layer debba risiedere direttamente nell'infrastruttura di rete, liberando i server per farli concentrare esclusivamente sulle loro funzioni primarie.

Costruire la strategia di sicurezza

Quindi, una robusta strategia di sicurezza basata su fabric deve cominciare a livello hardware nello storage fabric dove gran parte dello schema necessario per questo intelligence layer esiste già. Questa strategia di sicurezza dovrebbe essere:

- olistica, estendendo questo strato protettivo in tutta l'organizzazione;
- in grado di sostenere la crescita esplosiva dei dati e la loro natura sempre più distribuita;
- non pericolosa, eliminando inutili politiche e procedure che potrebbero ostacolare la produttività degli utenti o di processi IT, come il backup e le migrazioni dei dati;

- vantaggiosa in termini di costo, scalabile e interoperabile;
- facile da implementare, gestire e aggiornare, garantendo che le policy e le procedure vengano applicate costantemente.

Ma questo cosa significa in concreto? Considerando gli attuali livelli di concorrenza, le aziende non possono permettersi di implementare una strategia di sicurezza che diminuisca le prestazioni dei sistemi aziendali. Bisogna essere sempre più in grado di reagire rapidamente alle mutevoli condizioni del mercato, rendendo la veloce e accurata accessibilità dei dati una componente essenziale per garantire la flessibilità del business. La chiave di questo equilibrio non è solo un potente storage fabric che fornisca prestazioni e flessibilità necessari, ma uno che consenta e gestisca rigorose politiche senza che questo abbia impatti negativi gli utenti. Inoltre, una soluzione di sicurezza basata su fabric deve semplificare la gestione per risparmiare preziose risorse di personale IT. Una strategia di sicurezza proattiva gestita attraverso un'unica console di amministrazione basata su fabric può aiutare a prevenire potenziali violazioni prima che si verifichino, risparmiando il tempo necessario per risanare i sistemi infetti ed evitare l'imbarazzo di dover rendere nota ai clienti la violazione della sicurezza.

Oggi che gli attacchi ai sistemi diventano sempre più sofisticati e le minacce alla sicurezza interna più comuni, le aziende si trovano ad affrontare sfide sempre maggiori: fortunatamente, i vendor stanno trovando soluzioni a queste sfide, per consentire alle aziende di avere una integrità a tutta prova del loro storage fabric.