

# M Magazine III.08



## ATTUALITÀ

"Storage e Security vanno a braccetto?"  
di Dario Forte

# Storage e Security vanno a braccetto?

Lo storage e la sicurezza stanno ormai consolidando una simbiosi. Ma con qualche potenziale pericolo per tutti gli attori coinvolti. Vediamo come.

Il momento storico in cui ci troviamo rappresenta, per molti, un ritorno alla visione "information centric" dove i CIO vengono chiamati a tutelare l'informazione, con attenzione sia alla sua posizione ma non esclusivamente. È comunque molto importante conoscere dove l'informazione si trovi, sia per ragioni di compliance sia per motivazioni di tipo strategico.

Le informazioni vengono, inoltre, memorizzate in maniera "statica", cioè con riferimento al loro immagazzinamento. Lo storage, quindi, continua, da un lato, a ricoprire una sempre maggiore importanza mentre, dall'altro, si inizia a guardare alla convergenza tra questo ramo della tecnologia e la gestione della sicurezza.

Gli analisti come IDC parlano di questa convergenza già da tempo, e guardano al cosiddetto processo di adozione delle 3S (Security, Storage, System Management), asserendo che, in questo momento, la convergenza tra sicurezza e storage è, almeno dal lato tecnologico, un importante spunto di riflessione.

Lo è sia per gli utenti finali sia per coloro che gestiscono l'offerta. Nel primo caso, IDC dichiara che, in base a studi da lei fatti in Italia, i clienti sono disponibili a spendere una media del venti per cento in più per affiancare allo storage delle soluzioni appropriate di sicurezza. A questa indagine ci sentiamo di affiancare una serie di considerazioni basate sull'esperienza diretta verso i clienti finali:

- L'investimento ulteriore "on top" delle soluzioni di storage con finalità di sicurezza viene visto come una scelta prettamente tecnologica. In questo caso viene favorito (almeno inizialmente) lo stesso fornitore di storage, il quale viene invitato a proporre anche il layer di security.
- Il livello superiore non deve costituire un overhead o, peggio ancora, un fattore di limitazione del flusso informativo e/o peggiorare ancora delle performance. Questo è un rischio molto palpabile che si comprende soprattutto durante la fase di predisposizione delle RFP (Request for Proposals) dal cui testo è possibile percepire queste possibili preoccupazioni.



## SECURITY

- Detto livello di sicurezza viene chiesto dal Cliente non solo al fornitore di tecnologia ma anche all'eventuale outsourcer. In molti casi, infatti, la memorizzazione delle informazioni viene fornita come servizio e, al contempo, la sicurezza viene interpretata come un plus o come un obbligo implicito nella fornitura. Questo apre una parentesi di una certa importanza nella gestione dei rapporti tra clienti e fornitori di servizi in outsourcing. L'esperienza diretta sul campo ci dice che è in aumento il numero dei clienti che richiede features di security all'interno dei progetti di storage ma è in aumento anche il numero di quelli che ritengono che un layer robusto di protezione (non formale, ma reale) debba essere incluso, senza costi aggiuntivi. Non dello stesso avviso sono, evidentemente, i fornitori di servizi, che vedono in questo tipo di richieste il pericolo di un abbassamento dei margini che, evidentemente, è un rischio di impresa.

Non è dello stesso avviso, evidentemente, il settore dell'offerta tecnologica, cioè dei vendor, secondo il quale le tendenze citate nella prima parte di questo articolo siano fondamentalmente un'opportunità per tutti.

A sentire i vari keynotes delle conferenze destinate al canale di vendita, coloro che non colgono questa opportunità dovrebbero rivedere il loro modo di fare business. Dal canto loro, i vendor stanno proponendo numerose soluzioni consolidate, come le varie storage appliances che contengono, al loro interno delle features più o meno avanzate di sicurezza.



*Dario Forte, CFE, CISM, si occupa di sicurezza dal 1992 ed è Founder and CEO di DFLabs. Docente di Gestione degli Incidenti informatici all'Università di Milano, ha lavorato con NASA, Esercito Americano e Governo Italiano. Ha pubblicato nove libri e circa trecento articoli in Italia, Usa, Sudamerica e Asia. [www.dflabs.com](http://www.dflabs.com)*

za che vanno dalla crittografia, al controllo degli accessi al tracciamento delle operazioni di accesso, copia, scrittura e lettura.

Che si tratti di una tendenza per niente temporanea lo testimonia il numero decisamente alto (e in crescita) delle fusioni ed acquisizioni nel settore specifico, con particolare riferimento ai vendor più grandi che sono sempre disponibili a valutare l'acquisto di aziende che abbiano delle tecnologie in grado di poter allargare l'offerta.

Vi sono poi una serie di messaggi abbastanza chiari che provengono dai Top Manager di alcuni vendor, che incitano i partner a puntare la loro offerta in questa direzione.

Arthur Coviello, Ceo di RSA Security, ha recentemente ricordato che sono gli stessi clienti ad avere la necessità di rispondere ai requisiti di protezione di cui abbiamo parlato nella prima metà di questo articolo. In particolare Coviello ricorda che, per fronteggiare gli incidenti di sicurezza di questo momento storico sono necessarie tecnologie in grado, da un lato, di proteggere il patrimonio informativo dai security threats emergenti e dall'altro un superset di capabilities di backup per favorire il ripristino in tempi brevi.

Numerosi operatori di settore, inoltre, ritengono fondamentale includere, all'interno di queste soluzioni "aggregate", features di encryption, più o meno avanzate, al fine di proteggere le informazioni anche in caso di furto "materiale", cioè di asportazione fisica più o meno autorizzata e/o sofisticata.

La memorizzazione è sicuramente un fattore importante, ma non solo a livello centralizzato. Numerosi incidenti di sicurezza hanno dimostrato l'importanza anche del settore periferico, termine con il quale si intendono i punti di memorizzazione mobile quali laptop, smartphone e/o finanche le chiavi USB. Se i vendor sono concentrati sulla fascia high end, ne esistono comunque molti dedicati alla fornitura di oggetti simili in scala ridotta. Stiamo parlando di hard disk crittografati in maniera nativa, la cui robustezza è in molti casi superiore rispetto alle soluzioni software, molte delle quali sono anche gratuite.

In entrambi i casi è suggeribile effettuare una verifica sulle motivazioni che potrebbero portare il cliente ad orientarsi verso una serie di scelte di questo tipo. Di solito si parte da esigenze di pura compliance (cio' accade specialmente nel mondo finance e in quello sanitario, ove è necessario garantire una certa compliance). Negli Stati Uniti, per esempio, esistono delle normative che richiedono l'adozione di queste misure di sicurezza, con implementazioni tecnologiche effettuate su più livelli. Normative quali HIPPA, Sarbanes Oxley e standard come PCI sono ormai cogenti e non possono essere trascurate. Esse hanno inoltre degli impatti anche al di fuori dei meri confini americani, in quanto numerose aziende locali intrattengono rapporti formali di business con gli Stati Uniti e ad esse viene richiesta una compliance de facto che si affianca necessariamente alla gestione della normativa locale.

Ma quanto costa tutto ciò? Evidentemente non è possibile parlare di prezzi in questo articolo. Tuttavia riteniamo utile scomporre le classi di spesa, ancora una volta in base al posizionamento di queste ultime.

I Clienti finali devono per forza di cose valutare un impatto in termini di costi non esclusivamente legato all'acquisto delle tecnologie ma anche (e soprattutto) al lato consulenziale. È da ritenersi infatti che l'acquisto delle tecnologie sia l'ultimo atto di una catena ben più complessa, che inizia con un attento lavoro di valutazione preventivo, il cui esito dovrebbe essere poi quello della scelta del vendor. Molti clienti finali (in questo caso intendiamo anche gli outsourcer) seguono il percorso inverso e ottengono risultati criticabili.

Dal punto di vista dell'offerta, infine, mentre i vendor conoscono bene le potenzialità dei loro prodotti, i partner corrono il rischio di vedersi scaricare le responsabilità (o gli onori) di una implementazione. Per questo, ancora una volta, gli operatori di canale dovranno seguire le strategie dei vendor con la massima attenzione, e investire non solo in termini di acquisto dei pezzi ma anche in termini di know how. Lo studio di fattibilità e l'attività di progettazione, infatti, saranno sicuramente a carico loro. La buona notizia è che questi fattori potenzialmente di rischio, se ben compresi, possono tramutarsi in reali opportunità di business.