

## STORAGE E SECURITY: UN'UNIONE DA PERFEZIONARE

La recente approvazione del "*Codice in materia di protezione dei dati personali*" ha imposto ad enti ed aziende di adottare un insieme di misure minime per la protezione dei dati, misure la cui declinazione nell'ambito dell'Information Technology assume connotazione diversa in funzione della natura dei dati trattati, così come recitano lo stesso codice ed i relativi allegati tecnici.

Gli obblighi descritti hanno avuto, quale diretta conseguenza, una maggiore concentrazione dell'attenzione di enti ed aziende alla sicurezza dei propri ambienti e sistemi di storage, attenzione che è ulteriormente maturata vista la crescente informatizzazione del business e dei servizi e la conseguente pressante necessità di rispondere alle esigenze di disponibilità immediata dei dati in qualunque condizione operativa.

Sino ad oggi, ambienti di storage caratterizzati da stringenti requisiti di disponibilità del dato si sono contraddistinti per complessità e costi tali da renderli appannaggio di pochi soggetti. Di recente, però, l'evoluzione tecnologica e la maggiore attenzione dei vendor al segmento medium business – soprattutto nel mercato italiano – hanno modificato questo atteggiamento, dando una forte spinta alla diffusione degli strumenti di storage anche nella media impresa.

La contropartita che numerosi enti ed aziende si trovano oggi a pagare è legata, così come è accaduto in passato al crescere della diffusione delle tecnologie Internet, alla necessità di fronteggiare e risolvere al meglio le problematiche di sicurezza correlate alla realizzazione degli ambienti di storage.

Spesso, infatti, le *storage area network* (SAN) sono state realizzate con la massima cura rispetto ai requisiti di capacità di memorizzazione, resilienza e prestazioni, ma non con altrettanta attenzione alla sicurezza. La convinzione di molti è sempre stata quella che una protezione perimetrale (come, ad esempio, una linea firewall dedicata che controlli l'accesso alla SAN) e un minimo di conformità ad un approccio di tipo "*defense in depth*" fossero sufficienti ad assicurare la tutela della SAN e del patrimonio informativo che la stessa custodisce.

Poche riflessioni permettono, al contrario, di accorgersi che la questione non è così semplicistica. Più che altri sistemi, infatti, una SAN è vulnerabile ad attacchi interni e spesso le tradizionali misure di protezione adottate sino ad oggi non sono del tutto adeguate ad un simile contesto, soprattutto se si considera che tali misure tengono frequentemente conto delle lacune di infrastruttura, ma non del valore intrinseco dell'informazione da proteggere. In questo senso, le misure di protezione sovente non arrivano ad interessare l'ambito dell'autenticazione di sistemi, utenti ed amministratori, né si rivolgono alla protezione dagli attacchi che possano sfruttare le vulnerabilità tipiche dei protocolli e/o degli applicativi dei contesti SAN.

Non va dimenticato, poi, che la tendenza alla distribuzione degli ambienti di storage, l'outsourcing, la varietà di protocolli in uso (iSCSI, FC-IP), la varietà dei sistemi ai quali si devono rendere disponibili i dati (spesso lo spazio di memorizzazione è condiviso tra applicazioni e sistemi operativi eterogenei, con caratteristiche di security del tutto peculiari), sono tutti elementi che possono creare complicazioni nella gestione dell'ambiente e nella definizione di una politica di sicurezza armonica, a scapito delle garanzie di confidenzialità, disponibilità ed integrità dei dati.

Quando si parla di sicurezza degli ambienti di storage, pertanto, non si deve fare riferimento alla sola protezione perimetrale, ma anche e soprattutto alla tutela dei dati custoditi dai sistemi di storage e alla necessità di definire delle vere e proprie politiche di *storage security*, proprio nell'ottica della massima tutela e della massima disponibilità e fruibilità dell'informazione.

Una efficace politica di sicurezza dovrebbe rispettare, anche per un ambiente di storage, il criterio cosiddetto di "*security by design*", in base al quale già dalla fase progettuale dovrebbero essere valutati tutti gli aspetti di sicurezza necessari a garantire un'ideale ed efficace protezione del patrimonio informativo, dalla possibilità di sottoporre a cifratura i dati in ingresso/uscita dalla SAN (incapsulando, ad esempio, il protocollo iSCSI in IPsec<sup>1</sup>), alla opportunità di adottare, per i dati più critici, sistemi di protezione che ne garantiscano la totale inalterabilità (sistemi *Write Once Read Many* - WORM - come, ad esempio EMC Centera).

E' recentissima la notizia diffusa dagli organi di informazione nazionali di un tentato attacco ai sistemi di Poste Italiane, avente la finalità di distogliere consistenti importi di danaro dai conti dell'ente, a vantaggio dei cyber-criminali. Poste Italiane, essendo preventivamente al corrente di quanto stava accadendo, è stata in grado di

---

<sup>1</sup> L'estensione di IPsec al protocollo iSCSI è in corso di studio da parte dell'Internet Engineering Task Force, che ha già formulato proposte per l'adozione del protocollo ESP (cfr. RFC 2406).

gestire e seguire l'evoluzione dell'attacco, che, come noto, è stato attuato con la complicità di personale dipendente dell'ente Poste.

Eventi come questo, uniti alle considerazioni sin qui operate, fanno riflettere sulla varietà di opportunità che un qualsiasi cracker ha a propria disposizione per introdursi in un ambiente di storage.

Gli attacchi a livello infrastrutturale, tipici degli ambienti SAN, vanno dall'hijacking delle sessioni in un ambiente Fibre Channel (mediante alterazione degli identificatori di sessione contenuti nell'intestazione della frame FC), allo spoofing del World Wide Name di un host per tentare l'accesso ad una diversa zona (ZONE); per non parlare poi dei numerosi attacchi *IP-like* che possono essere tentati all'indirizzo di ambienti iSCSI.

Se si concentra l'attenzione sugli attacchi legati all'accesso non autorizzato alle risorse, poi, ci si rende conto che le opportunità sono ancor più numerose, favorite sia dall'assenza di efficaci meccanismi di autenticazione, autorizzazione ed accounting (AAA), sia dal trattamento e dalla memorizzazione in chiaro dei dati.

Una recente indagine di Yankee Group (2003) afferma che, nel prossimo futuro, l'attenzione del mercato si concentrerà proprio su questi ultimi due aspetti, orientandosi alla realizzazione di apparati e sistemi capaci di proteggere i dati memorizzati da tentativi di accesso illecito, attraverso meccanismi di cifratura e controllo di accesso combinati (*storage security appliance*).

Molti produttori, già oggi, sono in grado di offrire soluzioni di questo genere: basti pensare ai sistemi Centera – [www.emc.com/centera](http://www.emc.com/centera) – commercializzati dall'americana EMC<sup>2</sup>, la cui finalità primaria è quella di assicurare l'integrità dei dati memorizzati (non alterabilità) mediante l'impiego di una tecnica basata sull'associazione tra il dato originario ed un hash (metadato) che lo identifica univocamente, o agli apparati Datafort di DECRU (Figura 1) – [www.decru.com](http://www.decru.com) – in grado di offrire una interessante e versatile soluzione di crittografia e controllo degli accessi a dati residenti su supporti Storage (in ambienti SAN e NAS o Tape) per assicurarne la

confidenzialità, indipendentemente da architettura e caratteristiche dei sistemi di storage in uso.

Oggi è possibile fare molto per contrastare efficacemente i tentativi di attacco, già con la sola adozione di contromisure di base che sfruttino quanto intrinsecamente offerto dagli ambienti di storage: pensiamo all'*hardening* dei dispositivi, all'autenticazione e all'*auditing* degli accessi, al LUN masking<sup>2</sup>, al port zoning<sup>3</sup>, e ad altre misure analoghe. E' bene però, tenere conto del fatto che molte di queste contromisure offrono una protezione per i soli dati in transito (*data-in-flight*), ma nulla garantiscono in termini di protezione dei dati memorizzati (*data-at-rest*)

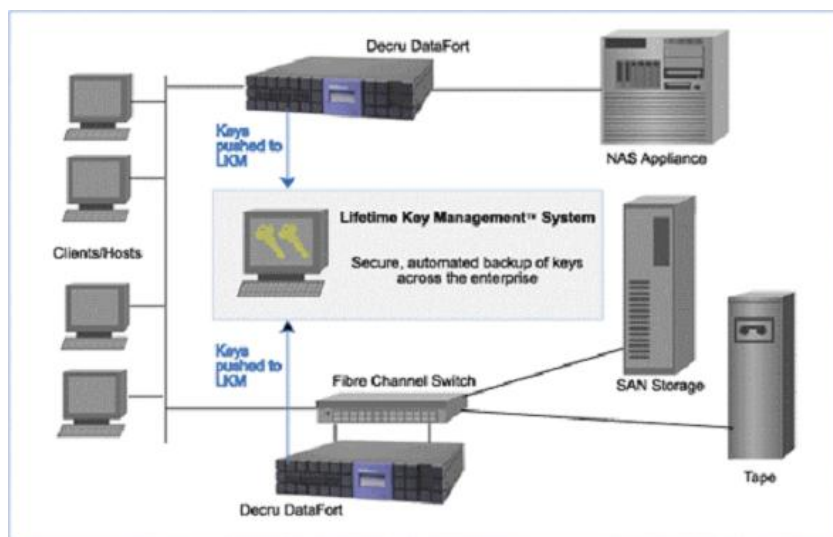


Figura 1

o dei supporti di memorizzazione (*storage media*). I meccanismi di protezione dei dati e dei supporti si configurano quindi come misure complementari alle tradizionali misure di difesa perimetrale, rappresentando la

<sup>2</sup> Il LUN (*Logical Unit Number*) Masking è un meccanismo di autorizzazione implementato a livello di HBA (*Host Bus Adapter*) che rende una LUN disponibile solo ad alcuni host della SAN.

<sup>3</sup> Il meccanismo del port zoning agisce sulla configurazione delle porte fisiche dell'infrastruttura per definire le cosiddette *security zone*, con il fine di condizionare l'accesso di ciascun utente ai dati sulla base della porta fisica alla quale l'utente stesso è collegato. Il port zoning si implementa solitamente mediante un meccanismo denominato *hard zoning*, il base al quale viene impedito l'accesso fisico ad una *security zone* a qualsiasi dispositivo che non sia stato dichiarato membro della *security zone* stessa.

sola possibilità di introdurre criteri di protezione che tengano conto, come si diceva in apertura, del valore intrinseco dal dato.

E' facile immaginare che cosa potrebbe accadere ad un qualsiasi ente o azienda qualora, identificata una nuova vulnerabilità e aggirati i controlli di infrastruttura, un cyber-terrorista si impossessasse o distruggesse il patrimonio informativo dell'ente stesso. Danni di immagine, danni finanziari e probabili imputazioni per la violazione del “*Codice in materia di protezione dei dati personali*” sono soltanto alcune delle dirette conseguenze di una simile evenienza.

Proprio sulla spinta di questa nuova consapevolezza del valore dell'informazione è lecito attendersi una reale crescita sul mercato di quei produttori di *storage security appliance* che sapranno rispondere adeguatamente alle necessità di tutela del patrimonio informativo di enti ed aziende, ponendo enfasi su quei meccanismi di cifratura dei dati e controllo di accesso a dati, applicativi e supporti di memorizzazione che rappresentano l'unica maniera per costruire una efficace barriera protettiva contro il furto, l'alterazione o l'intercettazione delle informazioni, e che possono garantire la conformità alle normative in materia. Gli unici, in sostanza, a costituire il vero tassello complementare in un approccio multi-livello alla sicurezza (*layered security model*).