Sicurezza delle Storage Area Networks

Giuseppe Paternò

Spesso in questi anni abbiamo notato una mancanza di attenzione in fase progettuale verso le problematiche della sicurezza. In generale, uno dei principali aspetti causa dei problemi di sicurezza sono le impostazioni di default: per facilitare gli utenti, molti prodotti sono impostati in modalita' "plug and play", ovvero preconfigurati con impostazioni generiche che vadano bene per tutti gli ambienti. Ad esempio, nell'ambito delle Wireless LAN, i produttori hanno privilegiato la facilità d'uso a discapito della sicurezza. Di conseguenza è stato necessario porre rimedio a posteriori su sistemi già installati e in produzione, intervenendo sia in ambito architetturale che di configurazione. Questi interventi tardivi richiedono maggiori investimenti di quanto richiesto dall'introduzione della sicurezza in fase progettuale.

Se una certa sensibilità verso la sicurezza è maturata in questi anni per le reti IP-based, questa non è ancora matura per le Storage Area Networks (SAN). Le SAN sono vere e proprie reti basate sul protocollo FC-SCSI. Analogamente alle reti IP, dovremmo preoccuparci della sicurezza delle nostre reti storage, proteggendole da eventuali usi impropri. Possiamo dividere l'uso improprio delle SAN in tre macro categorie: accesso non autorizzato, spoofing e sniffing.

Il concetto sui cui dobbiamo focalizzarci è che l'accesso non autorizzato prevede un rischio nettamente maggiore a quanto avvenga nelle reti IP, poichè un qualsiasi sistema compromesso potrà accedere a tutti nostri dati. Al contrario delle reti IP, dove esiste un "punto di accesso" su ogni scrivania, le reti storage possono essere confinate ad uno spazio ben determinato: il datacenter. Il fatto che fosse necessario risiedere nel datacenter per avere accesso alla SAN, induce a pensare che la sicurezza fisica coincida anche con una sicurezza dell'ambiente storage (la "security through obscurity"), ma non è così! Attraverso una compromissione di una qualsiasi macchina del nostro datacenter, un potenziale intruso potrebbe avere accesso ai dati del nostro database o dei nostri files condivisi, senza dover "forzare" nessun firewall. Non è sufficiente proteggere i server: se un attaccante ha accesso "legale" ad un solo sistema e riesce a forzare l'accesso allo switch SAN allora potrebbe ridirigere sulla propria macchina le LUN di proprio interesse. Esiste anche una forma più complessa di accesso non autorizzato: lo spoofing. Si tratta di impersonare una scheda Host Bus Adapter (HBA) di un altro sistema, cambiando il World Wide Name (WWN) associato all'HBA. In questo modo, l'attaccante potrà avere accesso allo storage della macchina a cui è associato normalmente il WWN, leggendo i dati. Un altro aspetto da tenere in considerazione è lo sniffing, ovvero l'intercettazione del traffico della rete SAN e la raccolta dei dati in transito dallo switch.

Dovremmo cominciare a pensare in un'ottica differente, la cosiddetta "*in-deep security*", ovvero il disegno di un'architettura intrinsecamente sicura: ogni singolo componente dell'architettura deve essere inserito e configurato in maniera sicura e la Storage Area Network non si può esimere da questo concetto. A tal scopo si consiglia di fare 'hardening' della propria infrastruttura storage, ad esempio:

- Proteggendo i sistemi di management della SAN
    - Usando SSH per accedere agli switch
    - Usando una rete di management separata dalla rete del traffico utente
    - Proteggendo la rete di management con un firewall
    - Criptando il traffico di management attraverso IPSec
- Usando port-based ACL per fissare un determinato WWN ad una determinata porta;
- Usando il LUN Masking sullo storage;
- Cercando di non implementare Host-based zoning (chiamato anche persistent binding) o zoning in base agli OS/applicativi;
- Usando soft zoning, o (meglio) hard zoning;
- Implementando sui sistemi sensibili:
    - La crittografia del filesystem;
    - HBA capaci di criptare il traffico FC-SCSI in transito.
- Proteggendo i gateway FOIP/iSCSI attraverso IPSec e firewall.