

Per una Fluida Circolazione dei Dati

«Maggiore sicurezza equivale a maggiore fluidità della circolazione dei dati. Occorre garantire una linea pulita». Intervista a Gino Bettoni, Regional Director Radware.

Si assiste a una moltiplicazione dei device, dei terminali da cui si può accedere ai dati, il tutto richiede una nuova architettura del flusso di informazioni...

“In primis” il terminale era un Pc, l’evoluzione della comunicazione ha fatto poi in modo che entrassero in gioco diversi device: palmare, telefonino, televisore, l’Umts... e la demotica è alle porte. Il baricentro si è spostato dalle applicazioni all’utenza. Lo sviluppo va verso la comunicazione e la flessibilità su differenti device. Questo ha portato a una nuova filosofia del prodotto: da una filosofia *application centric*, a una attenzione al *profiling dell’utenza*. Lo stesso utente può collegarsi nello stesso giorno con sistemi diversi, dall’ufficio, da casa, in movimento.

Gli attacchi informatici sono sempre più sofisticati, in alcuni casi vi sono intrusioni silenti e perciò ancora più pericolose: è come ospitare il ladro in casa, libero di scegliere cosa rubare...

Oggi i mafiosi chiedono il pizzo in modo elettronico, pensiamo al diffondersi di attacchi dimostrativi, avvertimenti mafiosi a siti di e-commerce. Cambia il modo e la metodologia con cui il crimine mette le mani sul web. La nostra piattaforma si chiama Apsolute: *availability, performance e security absolute*. Tre elementi indispensabili per un accesso professionale al web. L’*availability* per il web corrisponde all’apertura o chiusura della vetrina di un negozio. L’e-commerce non tollera interruzioni nella continuità del servizio. L’e-commerce oggi è sempre più legato a portali multimediali, non ci si può permettere una navigazione ridotta, una usabilità scarsamente funzionale e non immediata.

Cosa significa garantire la “performance”?

Garantire la *performance* significa mantenere l’accessibilità a tutti i servizi di un sito senza privilegiarne alcuni a discapito di altri. Occorre garantire un quantum di capacità trasmissiva a tutta la banda. Se chi vive al primo piano di un palazzo riceve tutta l’acqua, all’inquilino del terzo piano non rimangono che poche gocce. La sicurezza implica la capacità di gestione degli attacchi. Quando si è sotto attacco in realtà si perde contemporaneamente l’*availability* e la *performance* complessiva della connessione. Più computer in mano agli *hacker* e maggiore è la capacità di fuoco a disposizione per portare gli attacchi. La direzione di provenienza del fuoco diventa disorientante. Si fa saltare il sistema grazie all’intensità dell’attacco, come una invasione di cavallette. Milioni di richieste su un sito. La strozzatura, il collo di bottiglia è la connettività. Contro gli attacchi posso avere sofisticate barriere di protezione, ma questo non impedisce di ritrovarmi il canale di trasmissione saturato da una tempesta di richieste che bloccano la connettività. Il firewall può bloccare l’accesso ma in ogni caso il sistema non riesce a mantenere la connessione e diventa incapace di *performance*.

Cosa è una rete “application aware”?

Le Telco devono affrontare il fatto che il “premium” sulla connettività oggi è bassissimo, occorre garantire servizi a valore aggiunto, certamente uno fra questi è quello di mantenere una linea pulita. Sistemi di firewall centralizzati piuttosto *managed security service platform* che *content filter* per controllare l’accesso a Internet. Proprio per la grande apertura dei sistemi, le aziende corrono costantemente il rischio di ricevere “worm” o quant’altro, che come minimo rallentano l’intero sistema che viene messo in quarantena. Le tre componenti *availability*, *performance* e *security* sono concatenate da un sistema di interdipendenze. Absolute classifica e gestisce il traffico dati ottimizzando la connessione. Bisogna rendere le reti “application-aware”. Le reti devono capire le applicazioni che sono utilizzate in un determinato momento. La filosofia è quella di portare tutto sul web. L’evoluzione dell’informatica va verso il web. L’informatica è passata dalla logica mainframe con una architettura centric-based strutturata con terminali ‘stupidi’ e un centro ‘intelligente’, alla logica Lan dove tutti possono far tutto, non c’è un controllore che dirime la circolazione dei dati. L’ulteriore evoluzione è andata verso una architettura di client-server con i dati in centro e le applicazioni in periferia. Con la logica client-server le applicazioni devono tutte essere aggiornate in periferia. L’informatica di oggi è un ritorno a una certa logica del mainframe dove però non ho più un solo calcolatore, ma posso averne cento che lavorano in parallelo. Il futuro è una rete che si sappia autocontrollare: una sicurezza a monte del collo di bottiglia. Maggiore sicurezza equivale a maggiore fluidità della circolazione dei dati.

Intervista a cura di Vittorio Raschetti