

Il Processo Dinamico del Rischio

Per Gianfranco Severino, Channel Manager SEMEA Micromuse «la sicurezza deve essere gestita in “real time”, e richiede una attenzione e una prontezza non solo reattive ma proattive».

Dalle Telco al “finance”, il “real time” al centro del business...

Micromuse è nata in Inghilterra nel 1994 operando inizialmente nel settore delle telecomunicazioni, si è quotata al Nasdaq nel 1997, ed è oggi una multinazionale a tutti gli effetti. In Italia siamo presenti dal 1999 con un forte radicamento nel mondo delle Telco. Oggi stiamo penetrando anche su altri mercati, come quello del “finance”. Siamo nati come azienda che gestisce l'intera infrastruttura IT – Sistemi, Reti e Applicazioni – in tempo reale, nell'ottica di assicurare il “Servizio” con continuità. Un “fault” dei sistemi informatici può provocare un gravissimo danno sia in termini economici sia in termini di immagine. La prevenzione e la gestione delle discontinuità operative che da sempre costituiscono il “core business” delle telecomunicazioni è oggi esportabile al settore bancario.

Le banche sono sempre più simili per certi aspetti a un network di comunicazione...

Oggi l'imperativo è sempre più quello dell'allineare il business all'infrastruttura IT. Il nostro impegno è focalizzato nel tradurre il nostro consolidato *know-how* sulle soluzioni di Assurance in “real time” in soluzioni per il mondo “finance”. Nel mondo abbiamo già consolidati clienti come JPMorgan/Chase, Deutsche Bank, Bank of America, UBS, ABN AMRO, HSBC, ecc. vogliamo trasferire il nostro *know-how* maturato in grandi gruppi finanziari mondiali anche in Italia. Strategicamente abbiamo acquisito recentemente anche un'azienda che si occupa di gestione della sicurezza. La sicurezza richiede una dedizione tutta particolare, un approccio specifico. La sicurezza è un processo dinamico, non basta installare i sistemi di protezione, gli accessi via user/password e le barriere (i “firewalls”) per sentirsi a posto, la sicurezza deve essere gestita in “real time”, richiede una attenzione e una prontezza non solo reattive ma proattive. I ritmi sono spinti. Nella sicurezza il tempo è determinante: occorre individuare il problema con una visione anticipante, altrimenti è quasi sempre troppo tardi.

Come è strutturata la piattaforma Netcool per gestire la sicurezza?

Innanzitutto come uno strumento che a trecentosessanta gradi raccoglie e correla eventi da reti, sistemi, applicazioni e da prodotti di gestione di terze parti, e in particolare nello specifico mondo della sicurezza, Netcool/neuSECURE (questo è il nome del prodotto della suite Netcool specifico per la Sicurezza) gestisce i “firewalls”, “gli antivirus”, i “routers”, gli “IDS/IPS”, le “VPN”, i “log di accesso ai sistemi”, ecc. Si tratta di più di mille ambienti differenti che rappresentano anche un ampio spettro di soluzioni tecnologiche: si può dire che raccoglie lo stato dell'arte nel campo della sicurezza logica. Netcool/neuSECURE inoltre può essere integrato con i sistemi di monitoraggio della sicurezza fisica, quali videocamere, accessi fisici, ecc.

E soprattutto la sincronizzazione in tempo reale degli strumenti di prevenzione tra loro...

Innanzitutto Netcool/neuSECURE dispone di una funzione di gestione dell'incidente. Una volta identificata e analizzata la minaccia, viene generata una risposta e viene effettuata una

procedura automatica di escalation con cui si informa il Security Team di quello che è accaduto: nella sicurezza infatti è difficile automatizzare sempre l'intervento di risoluzione, il margine interpretativo umano è molto importante; si può fornire una risposta automatica solo quando non vi sono particolari problemi interpretativi e in occasione di azioni ripetitive (es. nella gestione dei falsi positivi). A valle dell'Incident Management, la funzione di Risk Mitigation consente di automatizzare la risposta in casi già analizzati, evitando di subire l'attacco di un elemento simile – un clone di discontinuità operativa – e riducendo i tempi di disservizio. Grazie a questa procedura il tempo di analisi e risposta a un attacco può passare da trenta a tre minuti: tutto questo si traduce in una grande riduzione del danno operato da una discontinuità del servizio. Un risparmio di danaro enorme. L'azienda non si può più permettere una discontinuità: il disservizio è di per sé causa di insuccesso e danno all'immagine. Il processo di ottimizzazione dei tempi di risposta alle minacce si fonda su un complesso database di memoria che costituisce una sorta di "Security Intelligence" che si aggiorna in modo automatico e in "real time".

Una reattività sempre più approssimata al tempo reale...

Certamente, la nostra parola chiave è "real time". Per questo è importante ridefinire le *policy* di sicurezza in funzione del quadro dinamico e mutante del rischio. Catturare le minacce grazie alla proattività, alzando la barriera di protezione, abbattendo i tempi di reazione. La multicanilità e la multimedialità dei servizi, le reti di accesso ai servizi online che sono enormemente ampliate (Voip, "mobile", WiFi, ecc.): un grande sforzo è stato sin qui fatto per aprire la banca all'esterno. Adesso si tratta di chiudere al meglio il circuito virtuoso della sicurezza. Gestione e sicurezza rappresentano lo strumento fondamentale perché nuovi business si possano effettivamente concretizzare. Si tratta di aiutare le aziende ad assicurare nuovi servizi e nuovo mercato. Il nostro rapporto con le aziende non è più riferibile solo a un dialogo con il Dipartimento IT, ma si tratta di una nuova forma di servizio a metà strada tra il business e l'ICT. Trasferire la tecnologia per una implementazione non misurata solo sulle caratteristiche strutturali dell'ICT ma anche sulla base dell'impatto effettivo sul "business model": «It's a hard job, it's a real time job».

Intervista a cura di Vittorio Raschetti