

Unify & Simplify

«Ridurre la complessità per un maggior supporto al business aziendale. Questo è il messaggio di CA». Intervista a Bruno Degradi, Responsabile della Divisione Sicurezza di CA Italia.

La sicurezza è sempre stata vista come pericolo esterno, ma il tipo di attacco si è evoluto assumendo forme sempre più sofisticate...

Rispetto a qualche anno fa, quando il principale obiettivo degli attacchi dall'esterno era il sistema informatico stesso (pensiamo ad attacchi come il "Denial of Services" o ai classici "virus", "worm"), stiamo assistendo a un cambiamento piuttosto consistente. Oggi (si veda per esempio il fenomeno del "phishing": azione fraudolenta per impossessarsi dei dati personali di un utente per uso illecito) l'obiettivo degli attacchi non è più e solo il sistema informatico, bensì il furto delle identità. Tutto questo per arrivare (in forma elettronica) a dei veri e propri furti di danaro danneggiando innanzi tutto l'immagine della banca vittima. In pratica, i sistemi informatici (sempre più sofisticati), da obiettivi finali degli attacchi sono divenuti il mezzo stesso per perpetrarli.

La complessità della gestione della sicurezza rischia di elevare il grado di complessità delle piattaforme di controllo. Cosa fare per semplificare il processo?

La tecnologia, se non è accompagnata dal "razionale", rischia effettivamente di aumentare anziché diminuire la complessità gestionale. L'Information Technology è nata proprio per automatizzare i processi (un tempo manuali), al fine di semplificarne la gestione e ridurre i costi. In questi ultimi anni l'aumentata complessità degli ambienti informatici ha richiesto la presenza, nell'infrastruttura IT, di ulteriori tecnologie di sicurezza proprio per garantire la protezione del patrimonio informativo delle aziende, banche incluse ovviamente. Per coniugare maggior sicurezza e maggior produttività (vale a dire riduzione della complessità), è assolutamente necessario che le tecnologie di sicurezza siano fortemente integrate in modo da fornire al Security Manager un efficace strumento di controllo e al gestore della sicurezza un efficiente strumento di amministrazione. CA (ex Computer Associates) sta seguendo da anni questa strada dell'integrazione e della semplificazione; al recente CA-World (il più grande evento mondiale di Information Technology con oltre 6000 partecipanti fra clienti, partner e fornitori), il messaggio forte è stato proprio "Unify & Simplify", cioè ridurre la complessità per un maggior supporto al business aziendale, caratteristica appunto delle nostre soluzioni tecnologiche.

Cosa fare per controllare dall'interno aziende complesse con un grande numero di dipendenti e un continuo flusso di comunicazione con l'esterno?

La soluzione a questo problema può essere raggiunta attraverso l'Identity and Access Management (IAM) e il Security Information Management (SIM). L'IAM permette, attraverso moduli specifici, di automatizzare la gestione delle identità (utenti e processi) e degli accessi alle applicazioni informatiche. Grazie all'IAM, ogni utente/processo esterno o interno alla banca viene identificato, autenticato e autorizzato ad accedere solo e unicamente

alle applicazioni/risorse necessarie per svolgere il proprio ruolo (vedasi principi quali “need to know”, “least privilege” e “segregation of duty”). Una volta definiti i ruoli e le autorizzazioni di accesso previsti, la semplice associazione dell’utente al rispettivo ruolo (o ruoli) abilita l’utente a operare in un contesto di massima sicurezza e produttività. Grazie alla tecnologia SIM, è poi possibile controllare chi ha acceduto alle applicazioni, ma anche cosa è successo all’infrastruttura informatica in termini di sicurezza. Per esempio, è possibile rilevare, filtrare, correlare eventi ed emettere segnalazioni o allarmi, a seguito di situazioni anomale (per es. un attacco da “virus”, “spam” o quant’altro). È inoltre possibile operare in modo proattivo, grazie alle caratteristiche offerte dalla soluzione stessa. Entrambe le suite (IAM e SIM) devono però offrire la massima integrazione, elemento indispensabile per perseguire gli obiettivi di unificazione e semplificazione. CA è leader di mercato in entrambe le aree (IAM e SIM) proprio grazie alle caratteristiche delle proprie soluzioni: completezza, “best of breed”, integrazione, semplicità d’uso.

Qual è il ruolo del dettato normativo nel guidare il processo di implementazione della sicurezza nelle organizzazioni?

La normativa sulla privacy (D.Lgs 196/2003) che tutela il cittadino e la normativa di Basilea 2 che tutela il modello di business della banca, impongono uno *standard di sicurezza* imprescindibile per le organizzazioni, che si traduce in un’esigenza di automazione del sistema organizzativo. Gestire modelli di sicurezza per singole aree, senza dotarsi di un’infrastruttura completa e integrata significa aumento della complessità e un conseguente dispendio di energie. Non bisogna poi dimenticare che il livello complessivo di un sistema di sicurezza è dato dal suo anello più debole. Di conseguenza, c’è una forte necessità tecnologica (oltre che organizzativa ovviamente) di dotarsi di un sistema globalmente efficiente e strutturato in modo organico. Nell’ottica di una “security governance”, chi non si è dotato di una infrastruttura organica si ritroverà quindi in grandi difficoltà: ne trarranno vantaggio quelle banche che avranno realizzato quanto richiesto dalle normative in tempo utile. Va inoltre segnalato che il legislatore (riferendoci in particolare alla legge sulla privacy) non si è limitato a scattare una foto istantanea rilevando lo stato dell’arte (la tecnologia del momento), ma ha anche previsto il futuro e l’evolversi del contesto tecnologico stesso. La legge dunque è stata non solo reattiva ma proattiva e preveggente. Assisteremo probabilmente anche a una futura integrazione delle legislazioni, visto che molti punti sono in comune.

Intervista a cura di Vittorio Raschetti