

L'ASPETTO TRASCURATO DELLA SOA SECURITY

LE ARCHITETTURE SOA DANNO LA POSSIBILITÀ DI POTER SFRUTTARE UN ECOSISTEMA DI SERVIZI ELEMENTARI CHE, COMBINATI TRA LORO, CONSENTONO DI COMPORRE APPLICAZIONI E DI IMPLEMENTARE PROCESSI AZIENDALI CON LA FLESSIBILITÀ NECESSARIA PER AFFRONTARE RAPIDAMENTE I CAMBIAMENTI DI BUSINESS.

Ma cosa possiamo dire circa l'approccio corretto da perseguire nel disegnare un'architettura SOA sicura? Un approccio rigido e verticale che prevede l'adozione o il riadattamento delle misure di sicurezza 'classiche' è spesso l'errore che viene commesso quando si vuole proteggere una infrastruttura SOA. Infatti è importante partire dal presupposto fondamentale che una SOA seguendo regole e meccanismi a servizi, dovrà adottare metodologie di sicurezza studiate appositamente per tali caratteristiche. Partendo da questo approccio si potrà avere la certezza di garantire i vantaggi di flessibilità e protezione specifici dell'architettura interessata. Infatti, nello sviluppo di un progetto, la sicurezza deve essere considerata come un servizio di supporto, in

grado di adattarsi velocemente ai mutamenti architetture e di business e che può essere riutilizzato indi-

pendentemente dalle piattaforme applicative e dalle loro evoluzioni nel tempo. Quest'obiettivo può essere raggiunto considerando l'introduzione di strumenti di sicurezza dedicati come XML Gateway e Agent che consentono di predisporre un 'layer' di sicurezza comune, flessibile e riutilizzabile, in grado di evolvere nel tempo seguendo i cambiamenti della piattaforma e dei re-



quisiti di sicurezza aziendali. La predisposizione di una 'SOA Security Infrastructure' basata su XML Gateway e Agent, infatti, con spiccate caratteristiche di flessibilità e riutilizzabilità, assicura un adeguato livello di sicurezza garantendo un costante e duraturo abbattimento dei tempi e dei costi di sviluppo.

**Senior consultant, Spike Reply*



© Sean Gladwell - Fotolia.com