

# OPEN SOURCE e sicurezza

Un dibattito aperto quello che coinvolge i software open relativamente alla loro sicurezza.  
Con esperti del settore cerchiamo di fare un po' di chiarezza

di Giuseppe Badalucco

**L'**open source ha occupato il centro del palcoscenico. Anche se a dire il vero la luce dei riflettori accompagna il software libero sin dagli albori di Internet come ci rammenta Manuel Castells che, nel suo *Galassia Internet* (Feltrinelli, Milano, 2001), definisce il movimento open source l'espressione culturale fondante nello sviluppo tecnologico della Grande rete.

L'adozione da parte delle aziende è il risultato di un lungo processo durante il quale il software aperto ha ampiamente dimostrato l'efficacia del proprio modello di sviluppo basato sul contributo di lavoro, know-how e collaborazione da parte della community globale.

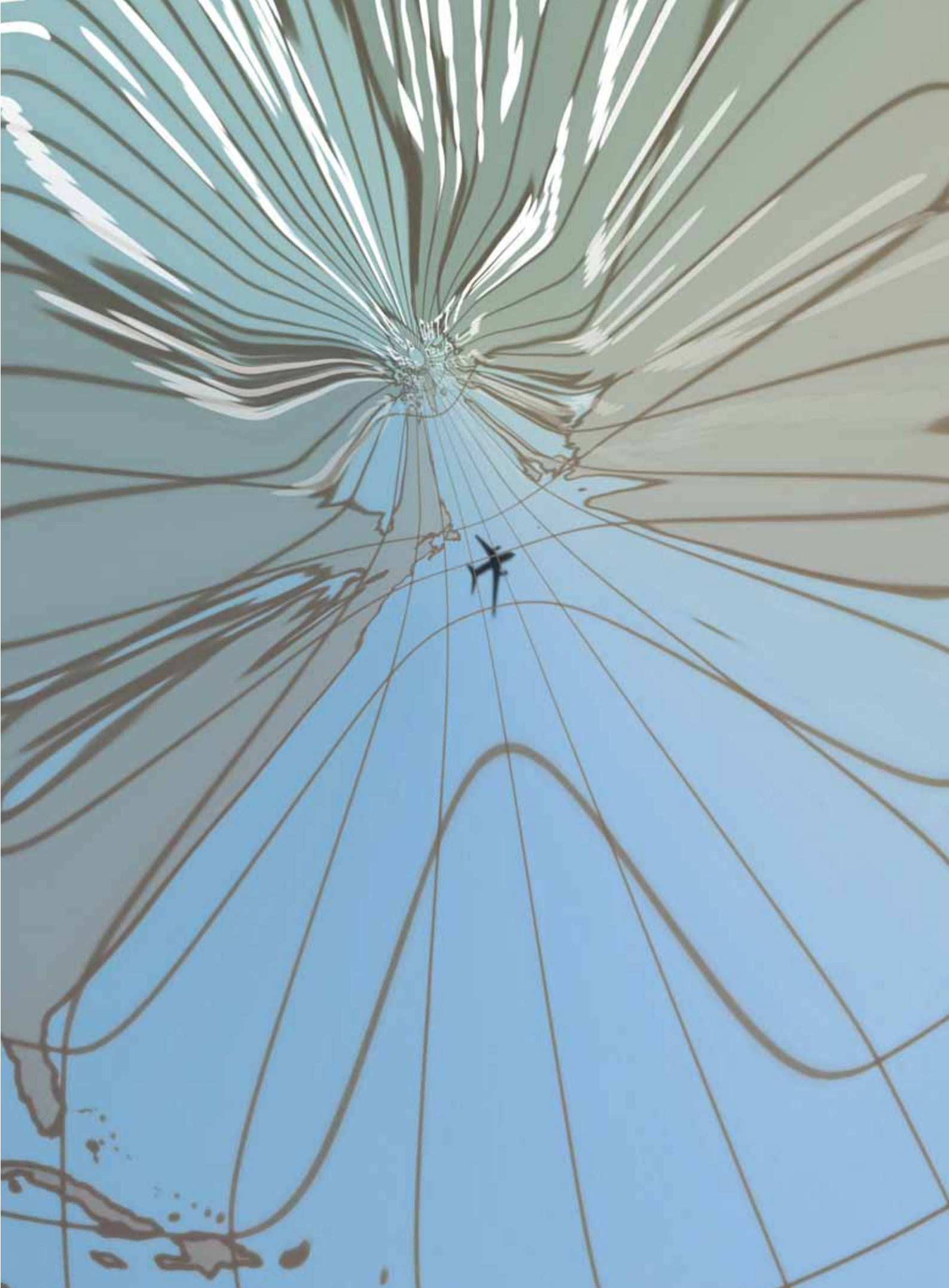
L'efficacia del modello ha migliorato la

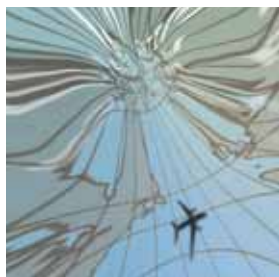
tecnologia influenzando positivamente l'intero comparto industriale del software. Oggi sempre più soluzioni "closed" beneficiano del patrimonio di conoscenze e relazioni sviluppate dalle comunità open; ciò si è tradotto in una maggiore efficienza e, per quel che ci consta, maggiore sicurezza del software.

L'onda lunga ha interessato anche l'offerta dei vendor la cui attenzione nei confronti del mondo open non è mai venuta meno; così essi hanno dapprima integrato i contributi provenienti dalle comunità open; poi chi ha potuto permetterselo ha stanziato risorse per creare o irrobustire al proprio interno team dedicati; infine hanno iniziato ad "aprire" il proprio software commerciale.

Prendiamo l'esempio di **Symantec** ([www.symantec.com](http://www.symantec.com)). Come ci conferma **Andrea Del Miglio, practice manager, operational services**, in Symantec Corporation, negli anni, la comunità open al proprio interno è cresciuta in modo significativo tanto che dal 2005 è stata creata una funzione chiamata "open source review board" deputata a guidare la presenza di Symantec all'interno della comunità internazionale.

Ovviamente la scelta di alcuni vendor di mettere a disposizione il codice dei propri software non può non essere dettata da ragioni di opportunità legate al business; così per esempio qualora non si preveda di continuare a innovare un prodotto, sia esso o





Per gli analisti di IDC il mercato del software open source standalone è entrato in una fase di forte espansione che dovrebbe protrarsi sino al 2011 raggiungendo un valore di circa 5,8 miliardi, con un tasso di crescita annuo nell'ordine del 26%

meno core rispetto alla propria offerta, si potrebbe scegliere di lasciarlo nelle mani di una community di sviluppatori e quindi non abbandonare lo zoccolo duro di utilizzatori che continua a richiederne supporto; oppure, ed è forse lo scenario più comune, una soluzione che non ha raggiunto il livello di successo che si sperava potrebbe essere rilasciato confidando nella possibilità che riesca ad attrarre nuovi utenti dal momento in cui diventa liberamente disponibile.

## LO SCENARIO

Questi fattori, in molti Paesi, hanno incoraggiato la nascita e il consolidamento di nuove imprese che, incentivate dai successi conseguiti dal mondo open, tentano il grande salto nel mare magnum dell'industria del software, debitore di una salutare ventata di competizione e innovazione.

Anche l'Italia beneficia dell'onda lunga di questa situazione, ostacolata però nel proprio cammino da alcuni impedimenti strutturali. L'industria italiana del software è composta da circa 58.000 imprese<sup>2</sup>; l'estrema polverizzazione dell'offerta del comparto è ben sintetizzata dal dato relativo al numero di addetti per azienda con meno dell'1% che supera i 50 addetti; e altrettanto anomalo, ma perfettamente in linea con il nanismo delle nostre imprese, è il fatturato medio per azienda del settore che in Italia è stimato in circa 260.000 euro (dato del 2003) contro i 335.000 euro della Spagna e il milione di euro della Germania.

Tuttavia è nel ruolo ricoperto dalle Pmi italiane che si svela l'estrema debolezza del comparto. In sostanza le piccole imprese It

svolgono il ruolo di subappaltatrici di grandi committenti che esternalizzano a basso costo produzioni It approfittando della maggiore flessibilità del lavoro delle imprese terziste; oppure il loro è quello, altrettanto limitato in termini di innovazione e tecnologia, di distributrici di prodotti sviluppati da altri soggetti.

Questa situazione influenza negativamente la propensione a investire in formazione e innovazione/ricerca limitando lo sviluppo e la competitività del settore e accentuando il ritardo del Paese in questo campo rispetto a nazioni come gli USA, l'India e la Cina; e neppure favorisce lo sviluppo della produttività, pietra angolare del nostro sistema economico; si legge infatti nel rapporto Assintel 2006 che la nostra competitività a livello internazionale è in grado di mantenere le proprie posizioni solo a fronte di un costante aumento della capacità produttiva, che cresce in media un punto in meno rispetto a quella dei Paesi Ocse.

## DIBATTITO SULLE POTENZIALITÀ DELL'OPEN SOURCE

Su questo terreno si sviluppa da qualche anno il dibattito sulle potenzialità del software open per il nostro sistema industriale e per la Pubblica amministrazione.

Il superamento dell'attuale assetto produttivo passa secondo molti osservatori attraverso l'adozione dei modelli di produzione propri delle comunità open, il più adatto a valorizzare il lavoro distribuito di un network di aziende cooperanti in autonomia e creatività. Il modello in tal senso è rappresentato da Paesi come Finlandia e Svezia dove nel giro di un decennio la produzione di softwa-

re open ha condotto a un sensibile affrancamento dalle software house multinazionali.

L'esperienza positiva di questi Paesi dovrebbe rendere più agevole affrontare alcuni nodi irrisolti che ostacolano la diffusione di imprenditorialità open source; da tempo infatti queste tecnologie hanno varcato il confine angusto dei circuiti alternativi e delle istituzioni accademiche, come dimostra la presenza di nuovi soggetti economici; la spinta allo sviluppo di una nuova leva di imprenditori oltre che dall'accumulazione di competenze e dalla possibilità di avvalersi e progettare autonomamente e in cooperazione con la community internazionale il software open, beneficerebbe del progressivo consolidarsi di un mercato di servizi It basati su tecnologie open alimentato da una crescente domanda proveniente dai settori pubblico e privato.

Per gli analisti di IDC il mercato del software open source *standalone* è entrato in una fase di forte espansione che dovrebbe protrarsi sino al 2011. Per il 2006 IDC stima in 1,8 miliardi di dollari il giro d'affari complessivo del segmento che potrebbe raggiungere alla fine del 2011 un valore di circa 5,8 miliardi, con un tasso di crescita annuo nell'ordine del 26%.

## OPEN SOURCE E SECURITY

I riscontri nella realtà sono altrettanto positivi; sebbene sia difficile stimare con precisione il numero di progetti open attivi sul Web i due portali di accesso alle soluzioni open source più conosciuti, **Sourceforge** (<http://web.sourceforge.com>) e **Freshmeat** ([www.freshmeat.com](http://www.freshmeat.com)), censiscono rispettivamente 97.000 e 43.000 progetti in fase di sviluppo<sup>3</sup>.

**NOTE:** 1 Lo ha fatto persino Microsoft con due programmi specifici, lo Shared Source Program e specificatamente per il Governo USA con il Government Security Program. 2 Fonte: Infoimprese ([www.infoimprese.it](http://www.infoimprese.it)). 3 Rilevazione effettuata il 12/06/07.



**Andrea Del Miglio**  
Symantec



**Rodolfo Sacchi**  
SysNet



**Enrico Campagna**  
I.Net



**Giuseppe Paternò**  
Red Hat



**Elio Molteni**  
CA

Per quanto riguarda il nostro Paese secondo una ricerca condotta da Berlecon Research nel 2004 l'Italia, con più di 30.000 programmatori si colloca al quarto posto nel mondo tra i Paesi maggiormente impegnati nello sviluppo di software open source dopo Francia, Germania e Stati Uniti; anche se i risultati nel frattempo potrebbero essere cambiati non dovrebbe scandalizzare nessuno affermare che il nostro Paese si trova ancora nel gruppo delle prime con più di un centinaio di comunità attive impegnate in altrettanti progetti software, di cui almeno una buona metà sviluppati anche fuori dai nostri confini.

Quale ruolo occupa la sicurezza nei progetti di sviluppo della comunità open source in Italia? Prima di affrontare questo aspetto approfondiamo alcune considerazioni preliminari chiedendoci anzitutto quali fattori orientano le scelte delle comunità che sviluppano progetti open source. E' noto che dietro alle quinte di alcuni dei progetti open più famosi vi sia il supporto a 360° dei grandi vendor; il loro contributo non si limita al mero finanziamento della comunità, ma pur con gradi diversi di coinvolgimento arriva in alcuni casi a dettarne fattivamente lo sviluppo; ciò non dovrebbe sorprendere nessuno e anzi sarebbe oltremodo *naïf* negare l'importanza della spinta economica anche in questo ambito.

Un secondo fattore da considerare attentamente, quale è quello della continuità del progetto, può aiutarci ad apprezzare le implicazioni legate a una scelta di sponsorizzazione. Quando un progetto viene abbracciato l'apporto di tutta quanta la comunità non si limita ai soli campi della programmazione e al limite della localizzazione del software. «Il coinvolgimento è totale anche

per le funzioni correlate, legate all'architettura, alla gestione del software, agli aspetti legali, alla documentazione, al training», ci conferma **Rodolfo Sacchi, amministratore delegato di SysNet**, ([www.sys-net.it](http://www.sys-net.it)). Ecco allora che la presenza interessata del vendor contribuisce a scongiurare la possibilità che il progetto open source si interrompa in maniera repentina sebbene esista il pericolo sempre reale del fork, del distacco cioè di qualcuno dal gruppo originario, fenomeno questo abbastanza comune tra le comunità open che può ingenerare confusione nel mercato, dispersione di energie, e un impatto negativo verso l'utenza finale.

In questo quadro, aspetti quali la proprietà del software, controllo del codice e accountability non sono più condizioni irrinunciabili nello sfruttamento commerciale dei programmi. «E' difficile dire quanto questo modello sarà sostenibile in futuro. I clienti sono sempre più alla ricerca di collaborazione, desiderano assumere un ruolo attivo sia nella fase di sviluppo che in quella di produzione», afferma **Giuseppe Paternò, solution architect & Emea security product expert di Red Hat** ([www.redhat.com](http://www.redhat.com)). Certo su questi temi le posizioni possono essere ancora discordanti, come dimostra il parere di **Augusto Berti, country manager di Quest Software Italia** ([www.quest.com/it](http://www.quest.com/it)), secondo il quale individuate le quattro priorità di business (capacità di migliorare i processi di business, aumentare la penetrazione sul mercato, migliorare la produttività e avere a livello di impresa il controllo dei costi operativi) «i fattori citati (proprietà del software, controllo del codice e accountability) risultano assolutamente necessari a supportare l'attività commercia-

le dei programmi e quindi il business delle aziende». Staremo a vedere; è ancora vero però che a fronte di una domanda consolidata e di un offerta già matura l'open source non sempre riesce a mietere successi: «Pensiamo solo alla gestione e manutenzione di un database di impronte virali di un server antivirus, oppure alla realizzazione di sistemi per il riconoscimento dello spam», rileva **Enrico Campagna, direttore marketing I.Net** ([www.inet.it](http://www.inet.it)). Oppure nell'area dell'identity & access management «segmento in cui le soluzioni open source non occupano posizioni di particolare rilievo», rileva **Elio Molteni, senior executive advisory di CA** ([www.ca.com](http://www.ca.com)). Ad attenuare in futuro questo solco potrebbe contribuire la tendenza già in corso di ricorrere per alcune problematiche a sistemi misti open/proprietario. «Nel segmento strumenti di gestione che comprende gli applicativi per la sicurezza, l'identity management e la collaborazione tra gruppi di lavoro, assistiamo al prevalere di soluzioni miste come alternativa alle soluzioni proprietarie esistenti», argomenta **Carlo Baffè, solution architect Novell Italy & Greece** ([www.novell.com/it-it/](http://www.novell.com/it-it/)).

D'altra parte è un fatto acclarato che il binomio open source-sicurezza incontra tuttora il favore del pubblico, soprattutto tra gli utenti che esprimono esigenze specifiche di sicurezza e magari frustrate in passato da vendor impreparati a rispondere in maniera adeguata, e sollecitati altresì dal grado di maturità raggiunto da alcuni applicativi di sicurezza diventati autentici standard di mercato nel loro ambito anche per i software commerciali.

Prendiamo per esempio la possibilità di poter modificare il codice; anche a fronte di una mancanza di una reale necessità



**Carlo Baffè**  
Novell Italy & Greece



**Mauro Batini**  
Sistemi Informativi



**Fabio Panada**  
Internet Security Systems

d'intervenire sullo stesso in modo diretto, potrebbe comunque essere utile ispezionarlo per comprenderne il funzionamento.

Naturalmente uno dei punti di forza delle architetture open è quello di poter analizzare il codice al fine di individuare potenziali problemi di sicurezza; con qualche qualificazione d'obbligo però: limitando l'analisi alla sicurezza del codice il problema non è solo di carattere quantitativo, con un numero potenzialmente illimitato di revisioni possibili su sorgenti aperti quanto, come argomenta **Mauro Batini, open source consultant di Sistemi Informativi** ([www.sistinf.it](http://www.sistinf.it)), «di ottenere revisioni di qualità in un contesto generale in cui la sicurezza sia organica alle procedure e alla cultura degli individui».

Anche il fattore personalizzazione presenta, a nostro parere, un certo grado di ambiguità di cui tenere conto. E' superfluo rilevare che una delle ragioni che spinge all'adozione di soluzioni open è la possibilità di gestire senza particolari vincoli le personalizzazioni che si ritengono più opportune.

Per questo molti system integrator consigliano ai propri clienti di ricorrere a questa opzione solo a fronte di una necessità concreta, come errori o problemi bloccanti che potrebbero pregiudicare il funzionamento complessivo del sistema; il ricorso a pesanti personalizzazioni potrebbe infatti pregiudicare la possibilità di effettuare l'upgrade del prodotto, come per altro avviene per le soluzioni proprietarie, personalizzate, in genere dallo stesso vendor, su richiesta del cliente. Si tende poi a sconsigliare una personalizzazione eccessiva anche in ragione dei costi che una o più risorse aggiuntive dedite alla manutenzione evolutiva del prodotto finirebbero per far lievitare.

Ancora sul versante strettamente tecnico un punto critico del software open è rappresentato dalla sempre perfettibile capacità delle soluzioni open source di integrarsi con le piattaforme esistenti. «Tale sfida passa attraverso lo sviluppo dell'offerta di software e, soprattutto, di servizi», puntualizza Batini. Inoltre occorre rilevare che i tool capaci di evidenziare in maniera automatica i problemi di sicurezza sviluppati per fare fronte al bisogno largamente diffuso di testare le applicazioni prima della loro messa in produzione sono ancora pochi e qualitativamente migliorabili.

Sul piano delle argomentazioni di tipo culturale un punto di vista discutibile è, a nostro parere, quello secondo cui i vendor consolidati avrebbero un patrimonio di credibilità di cui non disporrebbero invece la maggior parte delle aziende che sviluppano soluzioni open. E' vero che in qualche caso sporadico il software aperto si è rivelato una vera e propria backdoor realizzata per rendere vulnerabili sistemi che di per sé non lo sarebbero stati; ma è altrettanto vero che un'analisi meno conformista del livello di qualità di alcuni applicativi proprietari molto diffusi, pratica particolarmente in voga in questo periodo, ha portato a risultati ben poco lusinghieri sulla qualità complessiva del software.

Altrettanto radicato rimane il pregiudizio di alcuni rispetto all'utilizzo di applicativi open quali Erp, Crm, Ecm, BI in ambito aziendale. «In particolare le medie e grandi aziende non sono molto propense a ricorrere all'utilizzo dell'open source per queste tipologie di progetti», sottolinea **Marco Masarin, open source solutions manager di Unisys Italia** ([www.unisys.it](http://www.unisys.it)).

## LA QUALITÀ DELL'INVESTIMENTO

Come più volte sottolineato non è nei risparmi economici nel breve termine che risiede il vantaggio di una scelta open source quanto piuttosto nell'opportunità di migliorare la qualità degli investimenti riassumibile con la formula "meno licenze, più competenze"; la scelta dell'open source richiede però di affidarsi a un supporto tecnico più specializzato per lo svolgimento delle operazioni di installazione, configurazione e manutenzione; questo significa, giocoforza, dover fare i conti con alcuni indicatori tipici delle performance in azienda quali Sla; livello del servizio, efficacia delle soluzioni; per tutte queste ragioni spesso i critici dell'approccio open spostano l'accento sui rischi tipici della programmazione. «In particolare, le aziende dovrebbero considerare l'adozione di specifiche procedure, come per esempio, la revisione dei license agreement o una valutazione specifica costi-benefici da seguire riguardo il licensing del software open source», mette in guardia **Fabio Panada, technical manager Internet Security Systems Italia** ([www.iss.net](http://www.iss.net)).

Tuttavia anche in questo campo le cose stanno mutando. Per esempio sino a qualche anno fa solo con le soluzioni proprietarie era possibile acquistare direttamente dal vendor o da fornitori specializzati servizi di manutenzione, gestione e assistenza (la cosiddetta managed security) con garanzie contrattuali dei livelli di servizio; oggi la scelta è maggiore sebbene è indubbio che per potere effettuare alcune scelte occorra disporre al proprio interno della necessaria competenza per mantenere in efficienza e sviluppare la propria soluzione o architettura open source.

Per concludere anche se l'offerta di soluzioni software sviluppate in Italia è ancora in una fase di avvio e, di conseguenza, la sudditanza dalle importazioni in questo settore sia ancora molto pronunciata, è auspicabile che anche in questo ambito si ripercorran le esperienze di successo che si sono registrate nei progetti open. **DM**