

Le aziende italiane e la sicurezza: costo o opportunità



ROSSELLA MACINANTE
PRACTICE LEADER,
NETCONSULTING

LA SICUREZZA DEI SISTEMI INFORMATIVI È UN TEMA DI ELEVATA CRITICITÀ PER MOLTE AZIENDE, SEBBENE L'APPROCCIO ADOTTATO NELL'AFFRONTARLO SIA MOLTO DIFFERENTE.

Questo dato emerge con chiarezza dalla survey condotta annualmente da NetConsulting e promossa da CA, che per il 2007 si è focalizzata su un campione di 40 aziende italiane di grandi dimensioni (65% delle aziende intervistate hanno più di 3.000 dipendenti)

appartenenti a diversi settori (PA Centrale e Locale, Retail, Finance, Industria, TLC e Media). Tra i settori analizzati, Finance e TLC/media sono, analogamente a quanto riscontrato nella scorsa rivelazione, quelli che con maggior anticipo hanno affrontato la tematica a 360 gradi, e si trovano ad un livello più avanzato nella curva di adozione delle soluzioni di Information Security.

La dotazione delle aziende è stata analizzata nelle tre diverse tipologie di soluzioni in cui si suddivide la Security:

- threat management, ovvero l'insieme di soluzioni relative alla gestione delle minacce dall'esterno;
- la gestione delle autenticazioni e degli accessi;
- Security Information Management.

La prima area è quella su cui le aziende sono partite prima, tanto che ha raggiunto un livello di copertura

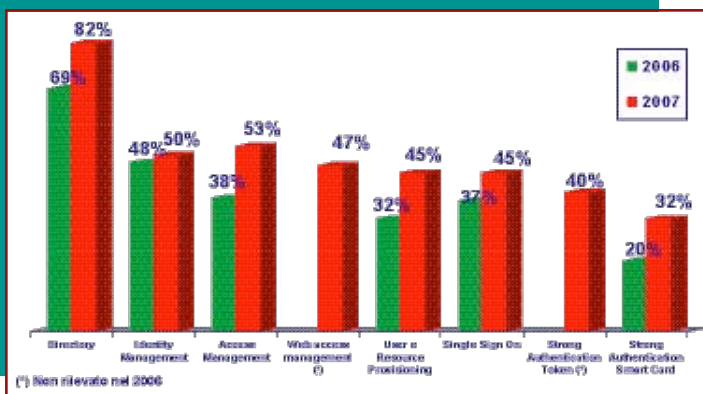
molto elevato, che arriva al 100% per antivirus e firewall. Sempre in quest'area è in forte crescita l'adozione di soluzioni di Intrusion Prevention, fondamentali per intraprendere un monitoraggio costante della rete al fine di individuare eventuali anomalie prima che si trasformino in minacce. L'area della gestione delle autenticazioni e degli accessi è quella su cui si registrano i miglioramenti più consistenti rispetto alla scorsa edizione della survey e su cui, anche nel 2008, si prevede si concentrerà il maggior numero di progetti da parte delle aziende intervistate. In particolare, cresce in misura considerevole sia l'Access Management (dal 38% al 53%), sia lo User e Resource Provisioning (dal 32% al 45%) e il Single Sign On (dal 37% al 45%). **Fig. 1**

Anche in questo caso sono i due settori più avanzati (Telco/Media e Finance) ad avere una migliore dotazione da questo punto di vista, contro settori come la PAL e il Retail in cui la Directory, ovvero il repository di dati relativi alle utenze aziendali su cui far poggiare le soluzioni di Identity e Access Management, rappresenta in molti casi l'unica soluzione di Identity Management adottata. Ancora da sviluppare l'area della Security Governance, in particolare per quanto riguarda i cruscotti per il monitoraggio degli eventi legati alla sicurezza, adottati dal 26% delle aziende. Nel 2008 i progetti si concentreranno su Identity & Access Management, che rappresentano una priorità di investimento per oltre l'81% delle aziende intervistate. Gli investimenti riguarderanno in particolare le soluzioni di single sign on. Nell'area del Threat management gli sviluppi previsti sono volti all'introduzione di soluzioni di Intrusion Prevention e Detection e all'aggiornamento di alcune soluzioni base già esistenti. Infine, si rileva un forte interesse sull'area del Security Information management, costituita dagli strumenti di governance per il monitoraggio degli eventi legati alla sicurezza. Quest'area rientra nei piani di investimento del 50% delle aziende, che stanno cominciando a comprendere l'importanza di soluzioni per monitorare e gestire la sicurezza. **Fig. 2**

Tra i fattori che frenano l'investimento in security la

FIGURA 1

L'ADOZIONE DEGLI STRUMENTI DI IDENTITY E ACCESS MANAGEMENT PRESSO LE PRINCIPALI AZIENDE ITALIANE



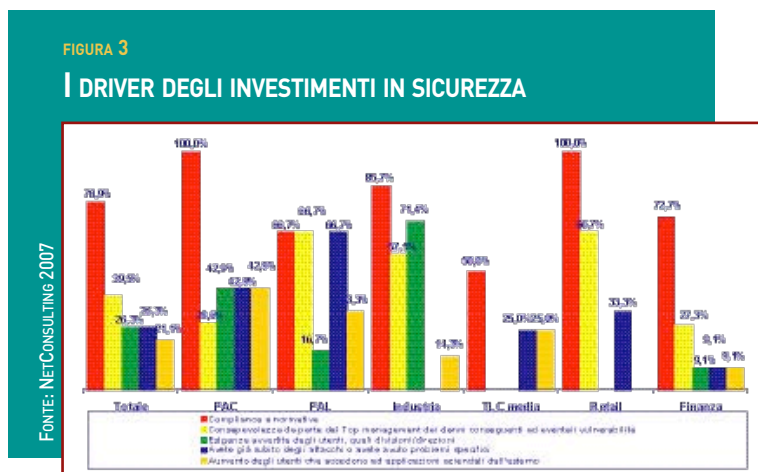
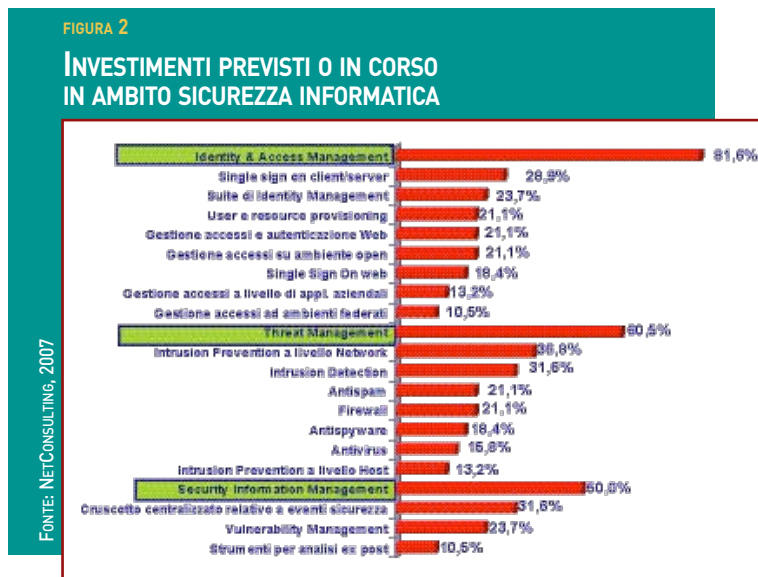
FONTE: NETCONSULTING

difficoltà a mappare tutti i processi è al primo posto, anche se il budget rappresenta ancora un ostacolo, soprattutto nel Retail e nella PAL. Il principale driver all'investimento sarà rappresentato, anche per il 2008, dall'adeguamento alle normative, citato dal 79% delle aziende intervistate, anche se in crescita rispetto allo scorso anno (39,5%) la consapevolezza da parte del Top Management che eventuali danni legati alla sicurezza comporterebbero per il business. **Fig. 3**

In questo scenario i fornitori hanno un ruolo fondamentale, dovendo supportare le aziende nel percorso evolutivo verso un approccio più completo alla security. Le caratteristiche che secondo le aziende intervistate devono possedere i fornitori sono rappresentate innanzitutto dalle competenze tecnologiche in tema di sicurezza, seguita dall'affidabilità e dalla capacità del fornitore di erogare un supporto post vendita adeguato e continuativo nel tempo. Questo si collega al rapporto di partnership che viene ad instaurarsi tra cliente e fornitore, considerata anche la forte specializzazione che caratterizza questo mercato e la tendenza da parte delle aziende ad adottare soluzioni best of breed su ciascuna delle aree precedentemente analizzate. In sintesi, è importante che il fornitore sia in grado di supportare l'azienda, fornendo quel valore aggiunto indispensabile per intraprendere un processo evolutivo già avviato ma non ancora completato.

Il punto di vista di CA

Correlando i dati della survey con le quotidiane esperienze presso i clienti, è possibile confermare il buon momento in Italia delle soluzioni di Identity and Access Management ove CA continua a mantenere la sua posizione di leadership tecnologica e consulenziale. Importanti progetti in quest'area sono stati realizzati da CA nel corso del 2007 presso alcune delle maggiori organizzazioni italiane, con ottime previsioni anche per il 2008. La crescita dell'IAM e della sicurezza in generale è dovuta anche al mutato ruolo dell'IT. Di pari passo, anche l'Identity and Access Management ha modificato il proprio scopo primario, passando da mera soluzione per "controllare chi fa cosa" ad un vero e proprio strumento per il Risk Management. Inoltre, le aziende sono sempre più soggette alle regole imposte dalle numerose ed articolate normative nazionali ed internazionali e l'IT risulta essere un elemento fondamentale nel processo ancora più ampio di Governance, Risk and Compliance (GRC). Anche l'ufficio legale, l'amministrazione e controllo, il dipartimento HR, il finance, e le altre principali funzioni aziendali sono coinvolte nel processo di "compliance". Infine, integrando i dati della ricerca con quanto ap-



preso dall'esperienza sui clienti, si delinea un panorama in cui la Security sarà probabilmente sempre più in totale simbiosi con il concetto di Risk Management. CA sta investendo molto nell'area del Risk Management con l'obiettivo di offrire ai propri clienti, ed in particolare a coloro che hanno scelto la tecnologia di Identity and Access Management (ma non solo), una continuità in linea con le aspettative delle organizzazioni che pongono l'accento sul Business. Per garantire continuità al business (lato azienda) e nel contempo un servizio efficiente, efficace, sicuro e duraturo (lato utente), è ormai essenziale un approccio rivolto al Risk Management. Sempre in ambito Identity and Access Management, CA, con la collaborazione dei partner certificati, ha applicato l'approccio del Risk Management anche nella conduzione dei grandi progetti e il fatturato di security, cresciuto nel 2007 più del 100%, è il risultato di questo modo di operare.