

DOSSIER

La digitalizzazione del business in Italia è proseguita nel corso del 2002, ma a passo ridotto. Il rallentamento dell'economia ha portato ad un ridimensionamento o a un rinvio dei progetti IT delle aziende. Investimenti di natura strategica come quelli ICT sono spesso rimasti nel cassetto pronti per essere estratti ai primi segnali di ripresa, mentre si è speso solo per l'indispensabile.

Ma quante sono le imprese che vorrebbero investire per progredire nell'e-business? A quali applicazioni pensano? Che valore assegnano ad Internet e al business in rete?

Due ricerche condotte fra maggio e luglio descrivono una situazione di considerevole ritardo della nostra imprenditoria su questi temi, ma anche di crescente interesse. Secondo il Net Impact Study Italia, una ricerca condotta dall'Università Bocconi per misurare l'impatto della rete sul sistema produttivo, le imprese che utilizzano soluzioni di business basate su Internet sono ancora

la vendita. Interpretando poi i risultati della ricerca più come la fotografia di una realtà desiderata che non effettiva, come suggeriscono gli analisti di Sirmi per spiegare le incongruenze delle risposte degli intervistati, è allora di un certo interesse apprendere che il 19,6% delle imprese da 20 a 49 addetti ha affermato di avere un ERP completo e il 15% un CRM. Il 24% di tutti gli intervistati ha detto anche di avere un accesso alle applicazioni aziendali condiviso tra clienti, fornitori e partners, il 60% di possedere una Intranet, mentre poi solo il 19,4% ha reso disponibili sulla stessa informazione per i dipendenti. Insomma c'è ancora molta confusione e sicuramente si pongono quanto meno problemi di chiarezza nella comunicazione e di semplicità di approccio e di utilizzo dei sistemi, se si vuole che l'universo delle imprese italiane benefici delle efficienze dell'e-business.

Peraltro a partire dall'esperienza di quelle imprese, per lo più grandi, che si sono dotate di soluzioni

L'attenzione che comunque dimostrano per le nuove tecnologie si tradurrà quanto prima in progetti se i fornitori sapranno utilizzare linguaggi comprensibili, offrire soluzioni con obiettivi e costi ben precisi, capaci di essere operative in tempi brevissimi e di generare ritorni quantificabili nell'entità e nei tempi.

"E le grandi sfide fra fornitori ICT non sono più sull'hardware -ha affermato Francesco Caio, CEO di Netscalibur, nel corso del convegno Eito sulla banda larga a Smau 2002- di switch e PC sono pieni i magazzini. La sfida oggi è sui servizi per rispondere alla grande crescita della domanda di e-business delle PMI".

L'E-BUSINESS HA BISOGNO DI SICUREZZA

Nel corso del 2002 le aziende italiane hanno speso molto per servizi e applicazioni relativi alla sicurezza. Secondo Federcomin, è questo il mercato che ha tirato maggiormente, tanto da riuscire

deve avere un concetto di sistema sicurezza con una sorta di centrale di riferimento. Ad esempio si potrebbe definire un'organizzazione di accreditamento delle figure che si occupano della sicurezza.

Ma tornando al comportamento delle aziende, in generale non si può ancora parlare di un approccio strutturato al problema della sicurezza, vale a dire che si spende, ma in modo piuttosto sconsiderato, magari senza produrre regolamenti interni che evitino comportamenti che possono esporre l'impresa a dei rischi. Si pensi banalmente a quali danni può produrre un'inconveniente navigazione in Internet in una pausa di lavoro. Non si tratta perciò solo di adottare contromisure tecniche, che sulla carta possono essere valide per tutte le realtà, bensì di collocarle all'interno di una struttura che ha le sue caratteristiche logistiche, tecniche e amministrative. Ogni contromisura deve trovare posto in un quadro complessivo, in una politica azienda-

Francesca Prandi

TENDENZE NELL'E-BUSINESS

molto poche, soprattutto fra le PMI. Si parla di un 11,4% contro il 47% di tasso medio tra Gran Bretagna, Germania e Francia, e il 61% degli Usa. Limitando l'analisi alle organizzazioni medio grandi, con più di 250 dipendenti, la penetrazione è invece pari al 50% ed è avvenuta fra il 1998 e il 2000, con tre anni di ritardo rispetto agli Usa e due nei confronti dei maggiori paesi europei. Il freno principale alle decisioni di investimento è dato dalla percezione di inutilità delle soluzioni basate su Internet, diffusa nel 69% degli intervistati dalla Bocconi.

Inutilità e non conoscenza trapassano anche nel campione di aziende intervistate da Sirmi: piccole imprese, con un numero di addetti fra 10 e 199, tutte informatizzate, la cui spesa annuale in IT è variata nel 2001 da 8.000 a 250.000 euro. Ebbene, il 15% ha dichiarato di non sapere a cosa possa servire un sito aziendale e il 73%, pur avendo un sito, non capisce cosa farne. Ciononostante, secondo Sirmi, rispetto al 2001 si rileva una crescita di attenzione per Internet e in generale è previsto un aumento dell'erogazione di servizi al cliente e di attività di e-commerce, ed in particolare la gestione on line dell'ordine e del-

business basate su Internet, si dimostra che gli investimenti effettuati hanno prodotto significativi ritorni in termini di efficienza. Secondo i risultati del Net Impact Study Italia, dal 1996 al 2001, le aziende interessate hanno realizzato un risparmio di costi pari a 9,17 miliardi di euro e un aumento dei ricavi pari a 6,69 miliardi di euro. E dato che le applicazioni sono sviluppate solo per il 70%, si attendono risultati ancora migliori per il futuro. Entro il 2006 la Bocconi stima un totale di 15,78 miliardi di euro, come risparmio di costi, e di 18,53 miliardi di euro di maggiori ricavi. L'impatto sul tasso di crescita della produttività annuale è molto elevato (0,14%) nel periodo 1996-2000, soprattutto rispetto a Germania, Francia e Gran Bretagna, e poi si allinea con quello dei partner europei. Le maggiori efficienze si sono riscontrate nelle imprese che sono passate all'adozione completa delle soluzioni basate su Internet mentre chi ha mantenuto elementi di organizzazione del business tradizionali è andato incontro a maggiori costi di gestione che hanno depresso la redditività dell'investimento. Un'ampia diffusione dell'e-business in Italia dipende quindi dalle scelte delle PMI.

a compensare gli andamenti negativi di hardware e telefonia. La spesa per la sicurezza è ormai indispensabile e inevitabile. Le aggressioni da virus e hacker sono molto cresciute. Secondo le stime di Federcomin gli attacchi degli hacker sono passati da 31.000 nel 2001 a 70.000 nel 2002. E del resto più sono sofisticate le tecnologie utilizzate, più si fa dell'e-business always on e più si è soggetti a rischi. Soprattutto nelle aziende aperte verso l'esterno (quelle meno aperte devono comunque fare i conti con gli attacchi dall'interno che secondo gli analisti sono altrettanto consistenti) è in gioco non solo la preservazione dei sistemi ICT ma anche la difesa dello stesso business. Come caso estremo si pensi a cosa significherebbe per un'istituzione finanziaria il blocco, anche solo temporaneo, della possibilità di contrattare in Borsa. Per questo nelle organizzazioni più avanzate si sta diffondendo la figura dell'ICT Security Manager, che si occupa di sicurezza del business seguendo un approccio integrato. La rilevanza del problema è tale che secondo Pietro Varaldo, Direttore Generale Federcomin, la sicurezza informatica deve diventare in qualche modo un servizio di pubblica utilità, si

le di sicurezza il cui obiettivo finale deve essere, secondo la definizione ISO, "garantire la disponibilità, l'integrità e la riservatezza delle informazioni gestite".

Su questi temi e in particolare sulla percezione che ne hanno le imprese italiane, la società di ricerca Sirmi ha condotto nel settembre 2002 una ricerca qualitativa basata su un campione di oltre 300 imprese, rappresentativo di 20.000 aziende italiane, appartenenti alla pubblica amministrazione e ai settori finanza, industria, commercio e servizi, con un numero di dipendenti non inferiore a 50. Il 100% delle aziende intervistate dispone di un accesso a Internet e la quasi totalità utilizza la posta elettronica e ha implementato una rete locale. Parlando della politica di sicurezza, solo il 20% dichiara di avere una politica scritta che indica tutte le procedure, circa il 30% pone per iscritto solo gli obiettivi e il 50% non ce l'ha o la giudica informale. Come elemento della politica di sicurezza quasi tutti utilizzano password, l'83% adotta sistemi di amministrazione della rete e di protezione e detenzione dei dati, l'82% ha un'amministrazione del sistema informativo, il 70% un'architettura sicura e il 62% ha stabi-

lito regole per l'uso delle e-mail. Gli strumenti più utilizzati sono il backup dei dati (96,4% degli intervistati), antivirus (93,4%), password (81,5%) firewall (74,5%). Sono invece poco diffusi gli strumenti più complessi come le smart card (5%), sistemi di sicurezza dei pagamenti (10,3%), firme digitali e crittografia (11-12%). Quanto all'origine degli attacchi subiti, secondo la maggior parte delle imprese sono arrivati dall'esterno sotto forma di virus (88% degli intervistati). Le aziende ritengono che, per lo più, ciò sia la conseguenza di comportamenti non intenzionali degli utenti, che quindi hanno prestato poca attenzione o non conoscono le procedure di sicurezza elementari. Quanto alle altre tipologie di attacco, hacker esterni o attacchi interni di pirateria, vandalismo e sabotaggio, ne vengono denunciati pochi, troppo pochi secondo i ricercatori. In questo caso infatti è in gioco l'immagine aziendale.

Per quanto concerne i costi connessi alle falle nella sicurezza dei sistemi informativi, le imprese non sembrano essere in grado di valutare i danni subiti. In caso di perdita dei dati aziendali e di arresto dei sistemi dovrebbero infatti valutare il costo per i dati perduti, l'hardware e il software danneggiati, il tempo speso per il ripristino del sistema e quello di mancato lavoro del personale, ma non sono in grado di farlo. Infatti il 32% delle aziende dichiara di non avere mai subito danni in seguito agli attacchi ai sistemi informativi, e il 74% afferma di non essere in grado di stimarli e il 19% li valuta in meno di un migliaio di euro. Fa riflettere che invece il 36% parli di inutilizzabilità dei sistemi e il 16% di perdita dei dati, conseguenze non da poco.

In generale quindi non si valutano i danni, ma neanche si predispongono budget specifici. Per contro, le aziende ammettono di avere speso molto per la sicurezza negli ultimi 12 mesi specialmente per interventi sulle procedure di backup dei dati e per l'acquisto di firewall. Volendo tentare delle conclusioni, si può dire che il problema della sicurezza non inibisce certo i programmi di e-business delle aziende, che al contrario spendono per proteggere le proprie attività in rete. Manca tuttavia una cultura della sicurezza che consenta di passare a schemi di protezione più efficienti, che implicano una politica aziendale ad hoc.

Ma se la crescita dell'e-business è inarrestabile, questo sarà inevitabilmente il percorso da seguire.

UNA FIRMA DIGITALE PER ESSERE SICURI

La mole di documenti e informazioni che vengono scambiati nel

business in rete è in continuo aumento. Anche chi non utilizza applicazioni evolute di e-business, usa quanto meno la posta elettronica affidando al web messaggi di una certa importanza.

Fin dagli inizi dell'e-business si è quindi posto il problema del valore legale dei documenti scambiati e della loro gestione, vale a dire conservazione degli stessi, identificazione e autenticazione dei firmatari.

Con varie leggi succedutesi dal 1997 il legislatore ha dato pieno valore legale ai documenti elettronici purché firmati secondo le regole della firma digitale. Nata nella pubblica amministrazione per consentire la dematerializzazione dell'atto cartaceo, la firma digitale oggi viene anche utilizzata per i pagamenti nell'ambito statale, dove consente di avere la situazione del bilancio in tempo reale.

La firma digitale si sta ora estendendo allo scambio di documenti e informazioni tra privati. A breve tutte le aziende dovranno munirsi di questo strumento perché è la stessa pubblica amministrazione a richiederne l'utilizzo. Ad esempio dal 9 dicembre tutte le società devono presentare alle Camere di commercio moduli e documenti informativi con firma digitale. Concettualmente la firma digitale è l'analogo elettronico di una firma apposta sulla carta. E quindi garantisce l'identità di chi firma, l'integrità del documento, cioè che non è stato manomesso dopo la sottoscrizione, e la paternità dello stesso, per cui non è consentito il ripudio del documento firmato. Utilizzando la tecnologia della firma digitale si è anche certi della segretezza dei contenuti, e ci si può assicurare sulla provenienza e la ricezione di un documento. Si può trattare di una lettera, un messaggio, un atto e qualunque file di dati: testo, immagini, musica o altro.

La firma digitale ripone la sua totale sicurezza sulla crittografia a chiavi asimmetriche, una pubblica e una privata. Si tratta di una tecnologia di cifratura che prevede l'utilizzo di chiavi fra loro correlate. Conoscendo un elemento della coppia, non è tuttavia possibile dedurre l'elemento corrispondente. Con questa tecnologia si possono cifrare e firmare documenti. Il titolare della coppia di chiavi è l'unico soggetto a conoscenza della chiave privata e quindi è il solo in grado di decifrare un documento a lui destinato o di firmarlo. Tutti gli altri possono liberamente venire a conoscenza della chiave pubblica del titolare della coppia e quindi sono in grado di verificarne la firma o di inviargli documenti confidenziali. L'Ente Certificatore (CA: certification authority) certifica la chiave pubblica del titolare della coppia di chiavi di crittografia.

Detto questo vediamo in che cosa consiste questa firma informatica e come ottenerla. Si firma attraverso un certificato digitale di sottoscrizione che è un file generato dall'Ente Certificatore InfoCamere seguendo precise indicazioni e standard stabiliti per legge. Il file contiene informazioni che riguardano l'identità del titolare, la chiave pubblica che gli viene attribuita, il periodo di validità del certificato stesso e i dati dell'Ente Certificatore Infocamere. Per poter firmare occorre un supporto di memorizzazione della chiave privata del titolare del certificato. In genere si tratta di una smart card, ma potrebbero essere anche un dischetto o un altro dispositivo hardware.

Utilizzando la smart card e attraverso appositi strumenti hardware e software, l'utente appone la firma che rimane indissolubilmente legata al testo sottoscritto. Si devono dotare di dispositivo di firma tutti coloro che intendono firmare una pratica telematica e i suoi allegati. Nel caso di un professionista che assuma il ruolo di firmatario per i suoi clienti, egli avrà una propria smart card, una per tutti i clienti.

La smart card può essere richiesta presso le Camere di Commercio oppure presso intermediari convenzionati con le stesse. Si tratta generalmente di associazioni di categoria, studi professionali, società o agenzie di servizi.

Sul territorio nazionale i punti di distribuzione delle smart card, che si chiamano Uffici di Registrazione, sono più di 400. Entro fine anno, secondo un dato riferito allo Smau da Giovanni Manca, responsabile della firma digitale presso l'Autorità per l'Informatica nella Pubblica Amministrazione (AIPA), saranno state distribuite 30.000 firme digitali, con una forte accelerazione negli ultimi due mesi. L'obiettivo è quello di arrivare a 500.000 firme.

Le possibilità offerte dalla firma digitale sono varie. Il certificato di autenticazione ad esempio può essere utilizzato per accedere a un indirizzo web. In questo caso non solo il browser si accerta dell'identità del server, ma consente anche al server di accertare l'identità della persona che utilizza il browser. Così facendo il server consente l'accesso ad aree di informazione riservate piuttosto che ad altre. E in più i dati scambiati sono cifrati. Tutto questo è di massima utilità nell'e-business. Si pensi a tutti i casi nei quali clienti e fornitori interagiscono nei siti web del partner d'affari. Sempre tramite il certificato di autenticazione e utilizzando soluzioni di gestione e archiviazione dei documenti informatici è possibile ad esempio definire gruppi o persone abilitati alla consultazione.

Si possono poi firmare messaggi di posta elettronica, che risultano così arricchiti di informazioni certe sulla provenienza.

Attraverso un software di firma/verifica fornito da InfoCamere è anche possibile ottenere la marcatura temporale di un documento informatico. Attraverso questo servizio si genera un file che contiene il documento e la marca temporale di InfoCamere.

E ancora, il certificato di autenticazione consente l'utilizzo delle soluzioni di posta sicura e certificata, offerti ormai da vari operatori (come ad esempio InfoCamere stessa e Telecom). Si tratta di sistemi che garantiscono l'identità del mittente, l'integrità e la confidenzialità del messaggio e anche la certificazione del recapito. Tale è la sicurezza, che in alcuni casi consentiti dalla legge, i messaggi di posta certificata equivalgono alla notificazione per mezzo della posta (art. 14, comma 3 DPR 445/2000).

Vediamo quindi che, grazie alla firma digitale, già oggi si possono fare molte cose e sicuramente altre ne verranno. In definitiva siamo di fronte a uno strumento indispensabile per lo sviluppo dell'e-business, in quanto accresce la sicurezza dei rapporti e nel contempo realizza efficienza, riducendo i costi di gestione documentale.

ASP, UN MERCATO IN CRESCITA. MA PER QUALI AZIENDE CLIENTI?

ASP ovvero Application Service Provider e cioè fornitura in rete di servizi informatici e applicativi. Più in dettaglio, un ASP può offrire: software standard, ad esempio applicativi verticali, ERP, CRM, Business Intelligence, Office, collaborativi, e-commerce, e-procurement; servizi abilitanti e di supporto come possono essere un'assistenza applicativa e tecnica, la formazione, customer care; servizi di connettività e reti e servizi di Data Center: hosting e housing.

Ebbene, secondo recenti stime Sismi, la domanda di servizi ASP in Italia è cresciuta del 168% nel corso del 2002 raggiungendo un valore di mercato pari a 7,70 milioni di euro. Utilizzando gli ASP le imprese si avvantaggiano di risorse IT molto competenti che diventano complementari a quelle interne all'impresa e trasformano i costi di investimento in informatica in costi di servizio. Tutto questo a patto che siano consapevoli di dover adeguare i propri processi aziendali alla implementazione di applicazioni standardizzate, che possono essere parametriche, ma in genere non personalizzate.

Ma quali sono quindi le organizzazioni che possono essere maggiormente interessate ai servizi ASP?

Vengono descritte nelle conclusioni di una ricerca condotta dalla Scuola di Direzione Aziendale dell'Università Bocconi e da Sismi su un campione di 650 imprese informatizzate appartenenti ai settori industria, commercio, finanza, servizi, pubblica amministrazione locale e sanità.

Anzitutto sono imprese capaci di gestire in termini manageriali il servizio IT. Ciò significa che hanno obiettivi di riduzione dei costi, di efficienza operativa e di aggiornamento tecnologico, che perseguono anche valutando l'efficacia del sistema informativo attuale e gli obiettivi a questo assegnati.

Concretamente impiegano metodi per misurare il valore dell'ICT in azienda, e sono quindi in grado di valutare il valore differenziale della scelta ASP: sanno intrattenere un rapporto di partnership con l'ASP al quale delegano solo le decisioni di routine. Non tutte le aziende hanno queste caratteristiche. E quindi, anche fra quelle del campione che si dicono interessate ai servizi ASP, non tutte potrebbero trarre grandi benefici da questa opzione.

Vediamo quindi cosa pensano potenziali utenti che sono interessati al servizio e contemporaneamente hanno già una struttura adatta a dialogare con l'outsourcer. Si tratta generalmente di aziende medio-grandi, appartenenti un po' a tutti i settori considerati, ma in misura minore a quello industriale. Si dicono particolarmente interessate ai servizi ASP attraverso i quali confidano di ottenere una riduzione dei costi di gestione, di infrastruttura e del software e di poter utilizzare dotazioni software sempre aggiornate, nonché di semplificarne l'adozione.

I temi che ritengono più critici nel passaggio ai servizi ASP riguardano la perdita di controllo su applicazioni e informazioni, l'eventuale rallentamento dei tempi di risposta per eccesso di traffico e le difficoltà nella definizione degli SLA, cioè i service level agreement.

I servizi a cui sono maggiormente interessate sono: ERP parziale, business intelligence, e-mail e messaging, software di produttività industriale, software grafico, marketplace, portali e e-commerce.

Per quanto riguarda invece gli aspetti contrattuali, queste imprese sono orientate ad avere una pluralità di interlocutori e a stipulare un contratto con ciascuno di essi, da redarre integrando lo schema contrattuale proposto dal provider.

Richiedono preferibilmente un canone variabile e desiderano che il contratto con l'ASP contenga la clausola risolutiva espressa e definisca chiaramente le modalità di riscatto delle licenze software e il costo di migrazione dei dati da effettuarsi alla scadenza del contratto.