

L'ICT nelle banche: cosa cambia

Dal CRM alla sicurezza passando per l'integrazione applicativa fino ai processi. Scenari e opinioni sull'uso di tali tecnologie attraverso la voce di esperti e operatori del settore.

Il mondo delle Banche è storicamente uno dei più assidui a investire - su diversi fronti applicativi - nelle tecnologie informatiche e di telecomunicazione. Una panoramica sui vari aspetti di questa particolare tematica è stata tracciata, da esperti e operatori del settore, nel corso di un convegno organizzato da IDG Communications Italia e intitolato "L'ICT al centro della banca".

"Le banche si sono avvicinate al CRM prima dal punto di vista analitico, dotandosi di 'occhi e orecchie', e successivamente 'delle braccia' per interagire con i clienti", ha spiegato **Daniele Vanzanelli**, docente dell'Università Cattolica di Milano, CETIF, andando successivamente ad analizzare l'impatto che le direttive di Basilea 2 hanno avuto sul CRM bancario. "Per quanto riguarda la tematica del rischio di credito, ossia il rischio di perdite risultanti dal default di una controparte debitrice, l'accordo di Basilea può concretizzare un vantaggio competitivo e può generare una domanda di servizi collaterali. Soprattutto per quanto concerne il rischio operativo ha invece forti impatti sui sistemi e i processi di CRM". Per rischio operativo si intende, in breve, "il rischio di perdite di valore generate da errori o malfunzionamenti di processi o sistemi, da comportamenti non corretti di persone o da eventi esterni. Include i rischi legali ma esclude i rischi di strategia e reputazione".

La continuità operativa

Una delle tematiche più calde, in questo senso, è quella della continuità operativa sulla quale **Massimo Messina**, Responsabile Facility Management di Banca Intesa, ha sottolineato come nei progetti di business continuity sia necessario avere una infrastruttura di comunicazione solida e gestita per passare, in caso di problemi, da un centro operativo all'altro: "E' come cambiare i pneumatici della macchina mentre questa è in corsa.... far sì che anche se un aereo si rompe questo non cada ... insomma far sì che il servizio non si fermi. E la BC non è comunque solo un progetto tecnologico (la cui componente è comunque forte) ma deve esserci dietro un grande supporto organizzativo". Proprio in tema di Business Continuity e Disaster Recovery, **Dario Cosentino**, Technical Manager Italia di Avocent, ha dal canto suo spiegato che tramite tecnologie di controllo remoto è possibile posizionare i server strategici in data center sicuri, "monitorando lo stato dell'hardware, controllando il tutto in modo non intrusivo, collegandosi direttamente alle interfacce. Ad esempio è possibile andare a monitorare la temperatura dei processori, la velocità delle ventole, e agire di conseguenza. L'utente vede solo le risorse sui cui è abilitato a intervenire, sfruttando sistemi di autenticazione".

Un altro aspetto affrontato nel corso del convegno è stato quello dell'utilizzo della multicanalità in ambito bancario, che ha visto **Michele Borgonovi**, Lead Solution Specialist Financial Services di Siebel Systems illustrare i risultati di una ricerca commissionata dalla stessa Siebel e da IBM a Datamonitor (basata su 300 banche retail) per valutare lo stato dell'arte del CRM bancario, ponendosi nei panni del cliente: "In molti casi chi ha risposto non si è preoccupato di chiedere chi fosse il suo interlocutore e il perché della chiamata, proponendo magari qualcosa di extra, perdendo quindi opportunità in termini di cross e up selling. Infine manca (totalmente, in Italia) l'integrazione tra i diversi canali, come telefono e posta elettronica".

Vedere le leggi

Tornando alle tematiche legate alla protezione degli ambienti informativi, l'intervento di **Luigi Neirotti**, avvocato, Partner Studio Legale Tributario Ernst&Young, si è focalizzato sulle varie normative che entrano in gioco in particolare per quanto riguarda il cosiddetto "Codice privacy" per la tutela dei dati personali, facendo una distinzione tra misure minime di sicurezza (la cui mancata adozione prevede sanzioni penali) e misure più ampie (che devono essere individuate dall'imprenditore stesso in base alla sua attività e ai relativi rischi, con sanzioni civili). Tutto si sintetizza poi nel Documento Programmatico sulla Sicurezza: "Il codice non fa sconti, parla di tutte le misure idonee ad evitare danno ad altri". Nel particolare caso delle banche bisogna poi anche tenere conto, ha aggiunto Neirotti, delle Norme di Vigilanza della Banca d'Italia e dei Sistemi di Informazioni Creditizie (con coinvolgimento del Garante).

Le banche possono anche affidare all'esterno alcuni processi. E' il caso di quelli relativi alla gestione documentale che, ha spiegato **Silvano Curri**, Direttore Commerciale di Anacom Italia, permette di seguire le varie fasi che la riguardano, come emissione, trasmissione, archiviazione, conservazione e consultazione: "Si parla quindi di stampa, postalizzazione, scansione, elaborazione elettronica, stoccaggio degli archivi in varie forme, compreso l'archivio ottico sostitutivo. In quest'ultimo ambito un vantaggio per le banche è ad esempio quello per la spesa dei bolli, oltre che del costo della carta, della stampa e così via".

Attenzione al phishing

Una delle minacce più recenti per quanto riguarda i fornitori di servizi finanziari è quello del phishing: "Cresce velocemente - ha detto in tal senso, **Davide Camusso**, Key Account Manager Sophos Italia - Sono stati 3.000 i siti attivi di tale tipo evidenziati nell'aprile 2005. Inoltre i furti di identità hanno colpito oltre 9,3 milioni di persone nel 2004 e il valore della perdita stimata è pari a 40 miliardi di euro. E' quindi importante identificare in modo rapido questi messaggi notificandone prontamente l'esistenza ai propri clienti, mantenendone viva l'attenzione".

Sulle problematiche di integrazione di sistemi e applicazioni in occasioni di fusioni e acquisizioni si è infine soffermato **Daniele Bonfanti**, Financial Insight, IDC Italia. "Trattandosi di attività poco frequenti non ci sono best practice su cui basarsi e possono essere coinvolti sistemi molto complessi e stratificati, con poca documentazione. La metodologia vede una strategia di integrazione decisa secondo logiche indicate dal CIO e dal management (deve essere legata alla strategia di business) e tenendo conto anche del feedback del mercato. All'atto pratico, si passa alle fasi di implementazione e change management, prevedendo che comunque si è sotto il controllo degli organi di vigilanza che possono eventualmente creare dei ritardi".